



Gesellschaft für
Reaktorsicherheit (GRS) mbH

INTERNATIONAL
ATOMIC ENERGY AGENCY

GRS-Bericht

Procedures and Systems for
Assisting an Operator During Normal
and Anomalous Nuclear Power Plant
Operation Situations

IAEA/NPPCI Specialists' Meeting
Munich
Federal Republic of Germany
December 5 - 7, 1979

GRS-19 (August 1980)



Gesellschaft für Reaktorsicherheit (GRS) mbH

**INTERNATIONAL
ATOMIC ENERGY AGENCY**

GRS-Bericht

**Procedures and Systems for
Assisting an Operator During Normal
and Anomalous Nuclear Power Plant
Operation Situations**

**IAEA/NPPCI Specialists' Meeting
Munich
Federal Republic of Germany
December 5 – 7, 1979**

**Organized and Hosted by
Gesellschaft für
Reaktorsicherheit (GRS) mbH**

GRS-19 (August 1980)

The proceedings are obtainable by:
Gesellschaft für Reaktorsicherheit (GRS) mbH
Glockengasse 2, D-5000 Köln 1
Federal Republic of Germany

CONTENTS

Session I

SURVEILLANCE SYSTEMS, DESIGN AND OPERATIONAL EXPERIENCE

Chairperson: M.W. Jervis

Secretary: D. Beraha

M.W. Jervis, D. Beraha

SUMMARY OF SESSION I

3

H.M. Wilkinson

EVOLUTION OF COMPUTER-BASED SURVEILLANCE, CONTROL AND
MAN-MACHINE COMMUNICATION SYSTEMS IN NUCLEAR POWER
STATIONS

11

C. Hermant, G. Guesnier

DATA PROCESSING AND DATA DISPLAY IN ELECTRICITE DE
FRANCE PWR 1300 MW NUCLEAR POWER PLANTS

27

J. Helske, B. Wahlström

ON THE DETECTION OF PLANT ABNORMALITIES BY SUITABLE
CONTROL ROOM LAY-OUT, EQUIPMENT AND POSSIBILITIES FOR
COMPUTERIZED OPERATOR SUPPORT SYSTEMS

43

K.P. Ojha

AUGMENTING OPERATOR GUIDE FOR ROUTINE AND EMERGENCY
OPERATIONS

57

K. Kaneto, S. Ohteru, H. Natori

DEMONSTRATION AND VERIFICATION OF ON-LINE CORE EVALU-
ATION SYSTEM IN THE STARTUP TEST OF HEAVY WATER RE-
ACTOR FUGEN

69

B. Eales, I.C. Smith

FIVE YEARS OPERATIONAL EXPERIENCE OF A MINI-COMPUTER
BASED AUTO-CONTROL SYSTEM ON THE WINDSCALE ADVANCED
GAS COOLED REACTOR

85

H. Kawahara, K. Monta, M. Itoh

ON-LINE PROCESS COMPUTER APPLICATION FOR OPERATOR'S
AID IN TOSHIBA BWR

99

Written Contribution

R.J. Conte

A MODEL SURVEILLANCE PROGRAM BASED ON REGULATORY EX-
PERIENCE

113

C

CONTENTS

Session II

TRAINING / SIMULATORS

Chairperson: R. Espefält

Secretary: D. Beraha

R. Espefält, D. Beraha SUMMARY OF SESSION II	131
G. Vaccarino ON THE DESIGN OF THE PEC REACTOR TRAINING SIMULATOR	137
A. Kameda, M. Sato, T. Sato, M. Sakuragi EVALUATION OF LIQUID METAL FAST BREEDER REACTOR OPERA- TOR TRAINING SIMULATOR	151
C.F. Gnospelius, P.E. Persson, R.I. Carlsson TRAINING OF POWER PLANT OPERATORS BY THE USE OF A SIMULATOR CLOSELY REPRODUCING ANOTHER PLANT	167
S. Kawashima BWR OPERATORS TRAINING EXPERIENCE USING SIMULATOR	179
J.F. Green, S. Birnie OPERATOR TRAINING FACILITIES FOR CEGB ADVANCED GAS COOLED REACTORS	197

CONTENTS

Session III

DISTURBANCE ANALYSIS

Chairperson: Ph. Freymeyer

Secretary: W. Ehrenberger

Ph. Freymeyer, W. Ehrenberger	
SUMMARY OF SESSION III	207
C.H. Meijer, B. Frogner, A.B. Long	
A DISTURBANCE ANALYSIS SYSTEM FOR ON-LINE POWER PLANT SURVEILLANCE AND DIAGNOSIS	213
K. Yamazaki et al.	
DEVELOPMENT OF PLANT OPERATION MONITORING SYSTEM FOR NUCLEAR POWER PLANTS	233
L. Bürger, E. Végh	
MAN-MACHINE COMMUNICATION IN EXPERIMENTAL REACTOR CONTROL SYSTEM	247
W.E. Büttner, L. Felkel, R. Grumbach, F. Øwre, B. Thomassen	
FUNCTIONS AND DESIGN CHARACTERISTICS OF THE STAR DISTURBANCE ANALYSIS SYSTEM	261
L. Felkel, R. Grumbach, A. Zapp, F. Øwre, J.K. Trengereid	
ANALYTICAL METHODS AND PERFORMANCE EVALUATION OF THE STAR APPLICATION IN THE GRAFENRHEINFELD NUCLEAR POWER PLANT	283

F. Baldeweg

CONTENTS

ON-LINE ALARM ANALYSIS USING DECISION TABLE TECH-
NIQUE

301

Version III

Written Contribution

DISTURBANCE ANALYSIS

L. Felkel, A. Zapp

Chapman, H. Friedberg

THEORETICAL ASPECTS OF DISTURBANCE ANALYSIS

321

305

H. Friedberg, W. Friedberg

STARTUP OF VERSION III

315

C.R. Weller, H. Friedberg, A.R. Long

A DISTURBANCE ANALYSIS SYSTEM FOR ON-LINE POWER PLANT

DETECTION AND DIAGNOSIS

323

R. Yamamoto et al.

DEVELOPMENT OF PLANT OPERATION MONITORING SYSTEM FOR

NUCLEAR POWER PLANTS

347

D. Bégin, E. Végh

MAN-MACHINE COMMUNICATION IN EXPERIMENTAL REACTOR

CONTROL SYSTEM

361

K.E. Höffner, L. Felkel, A. Gombosi, F. Wenz

H. Gombosi

FUNCTIONING AND DESIGN CHARACTERISTICS OF THE STAR

DISTURBANCE ANALYSIS SYSTEM

381

L. Felkel, A. Gombosi, A. Zapp, E. Wenz

J.K. Friedberg

ANALYTICAL METHODS AND PERFORMANCE EVALUATION OF THE

STAR APPLICATION IN THE OPERATIONAL NUCLEAR

POWER PLANT

f

CONTENTS

Session IV

APPROACHES TO SPECIAL SURVEILLANCE PROBLEMS

Chairperson: J. Furet

Secretary: A. Zapp

J. Furet	
SUMMARY OF SESSION IV	343
A. Nedelik, H. Roggenbauer	
A COMPUTERIZED SYSTEM FOR EVALUATION OF THE STATUS OF A PROTECTION SYSTEM	349
R. Haubert, R. Stokke	
MONITORING READINESS OF SAFETY RELEVANT DEVICES IN NUCLEAR POWER PLANTS BY MEANS OF CRT-COLOUR DISPLAYS	363
P. Cormault	
SURVEILLANCE SYSTEMS UNDER DEVELOPMENT AT ELECTRICITE DE FRANCE	381
Y. Hashimoto, K. Kawai, M. Suzuki, S. Izumi, Y. Michiguchi, K. Yamada, T. Joge	
ACOUSTICAL SIGNAL PROCESSING FOR LIGHT WATER REACTOR DIAGNOSIS	393
R. Assedo, P. Bernard, J.C. Carre, J. Cloue, A. Epstein	
PWR NEUTRON NOISE SURVEILLANCE: NOISE SOURCES AND THEIR EFFECTS	407

G. Zwingelstein, M. Déat, Le Guillou APPLICATION OF PATTERN RECOGNITION TECHNIQUES TO THE DETECTION OF THE PHENIX REACTOR CONTROL RODS VIBRATIONS	439
M. Edelmann SIMULATION OF FUEL ELEMENT THERMAL HYDRAULICS FOR SENSITIVE MONITORING OF COOLANT FLOW	455
G. Weinkötz, H. Martin, L. Krebs DETECTION OF COOLANT DISTURBANCES IN THE FUEL ELEMENTS OF AN LMFBR BY TEMPERATURE FLUCTUATION ANALYSIS	483
P. Liewers, P. Schumann, F.P. Weiß USE OF NOISE DIAGNOSIS FOR SURVEILLANCE OF PARTI- CULAR DISTURBING PROCESSES IN A PRESSURIZED WATER REACTOR	497
<u>Written Contributions</u>	
M. Sato, T. Sato, A. Kameda, Y. Yoneda OPERATIONAL GUIDANCE EQUIPMENT FOR FUEL HANDLING SYSTEM	509
G.P. Beraud, A. Bonnemay, A. Le Dieu de Ville, J.C. Nimal ESTIMATION OF LOCAL POWER IN A PWR CORE FROM GAMMA RAYS MEASUREMENTS	525

h

CONTENTS

Session V

BASIC INVESTIGATIONS OF SURVEILLANCE

Chairperson: J. Wakabayashi

Secretary: L. Felkel

J. Wakabayashi	
SUMMARY OF SESSION V	555
J. Wakabayashi, A. Fukumoto	
SIMULATION STUDY ON THE DIAGNOSIS SYSTEM OF NUCLEAR POWER PLANT OPERATION	561
R. Černý	
THE DYNAMIC CLASSIFICATION AND REDUCTION OF ALARMS IN COMPUTER BASED INFORMATION SYSTEMS	575
M. Lind	
THE USE OF FLOW MODELS FOR DESIGN OF PLANT OPERATING PROCEDURES	583
T. Tamaoki, N. Naito, T. Tsunoda, M. Sato, A. Kameda	
VERIFICATION TEST FOR ON-LINE DIAGNOSIS ALGORITHM BASED ON NOISE ANALYSIS	605
R. Avenhaus, G. Spannagel	
ANALYSIS OF PROCESS SIGNALS IN NUCLEAR INSTALLATIONS	629
W. Ehrenberger	
SOFTWARE VERIFICATION IN ON-LINE SYSTEMS	645

Written Contribution

E. Holló

OPERATOR-INTERACTIVE SURVEILLANCE METHOD OF PERIODIC
INSPECTION OF ACTIVE ENGINEERED SAFETY SYSTEM OF
WWER 440 TYPE REACTORS

667

CONTENTS

Session VI

MAN-MACHINE COMMUNICATION

Chairperson: E.S. Patterson

Secretary: L. Felkel

E.S. Patterson, L. Felkel SUMMARY OF SESSION VI	689
E.S. Patterson COMMENTS MADE AT THE IAEA/NPPCI SPECIALISTS' MEETING, SESSION VI	695
D. Martin, D. Grensemann A MODERN APPROACH FOR THE REALISATION OF THE MAN- MACHINE INFORMATION SYSTEM	705
F. Frischenschlager ANALYSIS AND PRESENTATION OF ANNUNCIATIONS IN NUCLEAR POWER PLANTS	725
T.J. Bjørlo, J.K. Trengereid COORDINATION OF OPERATOR SUPPORTING SYSTEMS AND PROCEDURES	739
D.M. Hunns PSYCHOLOGY OF COMMUNICATIONS	757
K. Netland MEASUREMENT OF OPERATOR PERFORMANCE - AN EXPERIENCE SETUP	777

k

L.P. Goodstein

PROCEDURES FOR THE OPERATOR, THEIR ROLE AND SUPPORT

793

J. Decuyper, S. Reynaud, A. Hoepner, Rolland

A GOOD OPERATOR-PROCESS RELATION RESEARCH IN CREYS-
MALVILLE PROJECT

813

Written Contribution

E.S. Patterson

OUTLOOK FOR THE USE OF COMPUTERS FOR PROTECTION
SYSTEMS AND AUTOMATIC CONTROL IN NUCLEAR POWER
PLANTS

829

l

OPENING ADDRESS

W. Bastl

On behalf of the Director of GRS, who regrets not being able to be with you this morning, I would like to heartily welcome you in Munich, in the Penta Hotel, to our Specialists' Meeting on Procedures and Systems for Assisting an Operator during Normal and Anomalous Nuclear Power Plant Operation Situations. Especially I would like to welcome the representative of the International Atomic Agency, Dr. Raisić and the members of the International Working Group Nuclear Power Plant Control and Instrumentation. This meeting is one of a series of Specialists' Meetings, promoted by this Working Group and organized under the auspices of the IAEA, Vienna.

Being a member of the Working Group for years, I took the liberty to dig a bit in the past, in the history of these Specialists' Meetings, and I found out, that the present meeting can be taken as a kind of successor to the one we held in Munich in 1976. Its subject was the Use of Computers for Protection Systems and Automatic Control. When summarizing the session on Plant Supervision and Disturbance Analysis, the chairman Dr. E.S. Patterson made two statements

- I suggest noise analysis techniques hold the promise of important changes in future protection system concepts and design.
- We should remember that the plant must be successfully and safely operated and maintained for years.

For me these sentences are remarkable for the following reasons: They became very true when looking at the situation of nuclear power as it emerged in the last two years; and they remind us about the methods and techniques of all type of operator assisting systems, which basically existed already at that time. Therefore I believe, it is even in the light of our recent experiences, not at all correct to state, we have to start from the very beginning.

Nowadays, various systems for effectively improving the communication between the machine and the man are available. They can and have to be implemented in the reactor plant, in the control room. Others have reached a very advanced state from the theoretical point of view. They have to be sorted out and further developed for future practical application.

Therefore my suggestion: Let us not leave the solid base of the process instrumentation and control as used today in our nuclear power stations, let us rather promote the implementation of new signal analysis and signal condensation methods, of new signal presentation techniques, which have achieved a high state of maturity, and let us thus considerably improve the man-machine relationship.

I hope and I wish that this meeting will help to go along this path, and that it will become one of the milestones on our way to this goal. I wish all of you to benefit the maximum from the papers presented and from the discussions. Have a very pleasant stay in Munich, and hopefully some time to have a look around in this charming city.

Before actually beginning with the meeting let me say some words in memory of Rainer Grumbach, who suddenly died in September this year. Most of us knew him as a very engaged reactor engineer and scientist. For long years he was joining the OECD Halden Project; there he gave many important impulses for research work in process computer application. Since 1979 he was also with GRS, Munich, as the head of the Process Computer Department. During the last years he was heavily involved with the development of disturbance analysis methods. He is the father of the wellknown STAR system. Rainer Grumbach was for a long time the representative of the OECD Halden Reactor Project in the IAEA Working Group NPPCI, and he was also engaged in the operation and organisation of this Specialists' Meeting. Gentlemen, may I ask you to stand up and remain one minute in silence.

CONTENTS

Session I

SURVEILLANCE SYSTEMS, DESIGN AND OPERATIONAL EXPERIENCE

Chairperson: M.W. Jarvis

Secretary: D. Beraha

M.W. Jarvis, D. Beraha

SUMMARY OF SESSION I

3

H.M. Wilkinson

EVOLUTION OF COMPUTER-BASED SURVEILLANCE, CONTROL AND
MAN-MACHINE COMMUNICATION SYSTEMS IN NUCLEAR POWER
STATIONS

11

C. Hermant, G. Guesnier

DATA PROCESSING AND DATA DISPLAY IN ELECTRICITE DE
FRANCE PWR 1300 MW NUCLEAR POWER PLANTS

27

J. Helske, B. Wahlström

ON THE DETECTION OF PLANT ABNORMALITIES BY SUITABLE
CONTROL ROOM LAY-OUT, EQUIPMENT AND POSSIBILITIES FOR
COMPUTERIZED OPERATOR SUPPORT SYSTEMS

43

K.P. Ojha

AUGMENTING OPERATOR GUIDE FOR ROUTINE AND EMERGENCY
OPERATIONS

57

K. Kaneto, S. Ohteru, H. Natori

DEMONSTRATION AND VERIFICATION OF ON-LINE CORE EVALU-
ATION SYSTEM IN THE STARTUP TEST OF HEAVY WATER RE-
ACTOR FUGEN

69

B. Eales, I.C. Smith

FIVE YEARS OPERATIONAL EXPERIENCE OF A MINI-COMPUTER
BASED AUTO-CONTROL SYSTEM ON THE WINDSCALE ADVANCED
GAS COOLED REACTOR

85

H. Kawahara, K. Monta, M. Itoh

ON-LINE PROCESS COMPUTER APPLICATION FOR OPERATOR'S
AID IN TOSHIBA BWR

99

Written Contribution

R.J. Conte

A MODEL SURVEILLANCE PROGRAM BASED ON REGULATORY EX-
PERIENCE

113

M.W. Jervis, D. Beraha
SUMMARY OF SESSION I

M.W. Jarvis, D. Beraha

SUMMARY OF SESSION I

The contribution in the first session centered on the operational experience gained up to now with surveillance systems and on the design characteristics of such systems.

The paper by Wilkinson gives an overview on the evolution of surveillance systems in Ontario Hydro nuclear power stations, and describes in more detail the most recent computer-based control and man-machine communication systems. Considerable experience with digital monitoring, control and instrumentation systems is available, since the use of process computers in CANDU power stations dates back to 1962. The extensive surveillance systems of the units planned for Darlington are connected not only to operator interfaces (18 CRT's), but also to the digital control systems. Operator and surveillance thus complement each other w.r.t. the control functions. High reliability is achieved through the use of a dual computer configuration with self-checking features.

A question was posed concerning the large number of CRT's. The author pointed out that it is anticipated that CRT's will occasionally fail. Therefore, the same information display is available by more than one CRT. Furthermore, different parameters may be scanned at the same time on parallel displays.

A survey of the data processing and display in PWR nuclear power plants of Electricité de France is given in the paper by Hermant and Guesnier. Process computers are used in the reactor protection system (a multiprocessor structure with quadruple redundancy), in the automatic control system (modular distributed structure), and for monitoring the flux distribution in the core and the control rod positions (dedicated microprocessors). Communication between these three systems is achieved through multiplexed data links.

The processing and presentation of data is done in the Complementary Data Processing System (TCI), with the aim of providing operator assistance (surveillance of measurements, man-machine communication, control function simulation), post-incident analysis and core parameter calculations. The structure and the tasks performed by the TCI are described in more detail. These include comprehensive logging and history of state changes and analysis of plant performance, fast recording of turbogenerator data and a proposed disturbance analysis system. In reply to the question, if a conventional protection system is provided as back-up, the authors stated that only the system with four independent computers is employed.

In the next paper, the surveillance system of the Loviisa nuclear power station (Finland) is described. The computer-based system provides alarms to the control room, process status information, measurement values and information on present and past plant performance. The operating experience has indicated the necessity of improvements, especially towards reducing the large amount of information, the detection of leakages in the containment and the alarm presentation. While the last two items were solved satisfactorily (supervision of the sewerage pump operation by the operator; improved color code distinguishing between alarm and component status), the information reduction will require some more attention. A separate emergency panel is envisaged as a possible solution. The reasons and percentage of non-availability due to human errors are listed. Concluding, trends leading to future systems are discussed, emphasizing the need of disturbance analysis.

In the discussion, the authors were asked to comment on the selection of relevant alarms and on the number and function of the CTR's.

The first question was answered by stating that the alarm selection is designed based on the analysis of specific situations of the processes. The fundamental difficulty with the large information amount is thereby reduced, but not completely eliminated. As to

the second question, 6 CRT's are installed, 2 of them exclusively for alarm presentation. The other four may be used for display of functions called from the operator desk. The computer feeding the CRT's is separated from the instrumentation.

The paper presented by Ojha reviews the layout of the displays at Rajasthan Atomic Power Station (India). The display is distributed on six panels, each panel covering one subsystem. Parameters which are relevant to more than one subsystem are displayed on all relevant panels. Some additional displays and alarms are described. For disturbance analysis, pre-disturbance and post-disturbance memory is available. Data handling systems are used to detect failed fuel elements and to monitor the channel temperatures. It is stated that the display systems have been of much help to the operator.

As to the question posed regarding the tasks of the disturbance analysis, the author replied that the disturbance analyser keeps the plant parameters of the last 5 min updated until a disturbance occurs. After recognition of the disturbance, the plant state is recorded for further 5 min. Data are sampled every second.

Kaneto presented the Core Evaluation System ATROPOS for the Heavy Water Reactor FUGEN (Japan). ATROPOS is a simulator-based system which is adapted to the signals of the in-core instrumentation. This feature enables ATROPOS to estimate and furthermore to predict the power distribution in the core. In addition, the thermal operation limits are monitored.

ATROPOS has been verified at different power levels. Both estimation of the current core status and prediction yielded very satisfactory results: The estimation error of the power distribution was less than 3 % at any power level, while the prediction error stayed below 6 % excluding peripheral segments. Also, the errors in the core thermal power and the thermal operating limits were small.

The author was asked, if the system could fail in such a way as to create a dangerous situation, and if software errors might lead to dangerous conditions. He stated that the system was not designed for

use in protection systems. As to software errors, the system would fail by increasing the error margin. At about 6 % error, the operator would be alerted.

Smith reported on five years operational experience of a mini-computer based auto-control system on the Windscale Advanced Gas-Cooled Reactor. This reactor has two experimental loop facilities, each of the loop having an independent coolant system. The fuel cladding temperatures can be controlled by altering the coolant flow, which in turn is controlled by varying the circulator speed or a valve setting. The minicomputer controlling both loops is partly programmed in BASIC to provide enough flexibility under changed experimental conditions. The function of the control and the design features were explained. The procedure undergone for commissioning of the auto-control and the operating experience were described in detail.

The discussion centered on the auto-control performance under fault conditions. At failure of the control computer, all actuators are frozen, which the back-up system takes over and steers the plant to safe operating conditions and eventually shuts the plant down. As a precaution against software errors, the assembler language used for scanning routines and interfaces to the actuators was checked in the commissioning period. The routines written in BASIC were extensively tried out before going on-line; however, there are no safety implications involved.

The next paper delivered by Itoh dealt with on-line computer applications for operator's aid in Toshiba BWR nuclear power plants. Three process computer applications are surveyed: The PODIA system (Plant Operation by Displayed Information and Automation), Plant Diagnosis, and Load Following operation. The PODIA system has led to a new integrated operator console design, with indicators and CRT's to provide improved man-machine communication. The Plant Diagnosis System provides early fault detection by noise analysis methods, comparing power spectra, correlation functions etc. to reference patterns. The load following behaviour is improved by using simplified predictive core models and monitoring the core and plant status.

The lively discussion started with questions on how auxiliary computers performing the described functions are attached to the existing equipment. The author replied that the connection between computers is achieved through data links. As to the necessary software modifications, they are done during the inspection time. With respect to questions on signals suitable for noise analysis, the core channel heating was given as an example. Asked about the use of noise analysis in the automatic control system, the author stated that such a system is being developed. Some questions concerned the redesign of the operator console, especially the hard-wired system and the great proportion of indicators. The author commented that in his experience the transition from conventional instruments to an extensive use of CRT's should not be too fast. However, the operator may rely only on the information displayed by the CRT if he wishes to. The hard-wired system also acts as back-up when the computer breaks down.

H.M. Wilkinson

EVOLUTION OF COMPUTER-BASED SURVEILLANCE, CONTROL AND MAN-
MACHINE COMMUNICATION SYSTEMS IN NUCLEAR POWER STATIONS



**Evolution of Computer-Based
Surveillance, Control and Man-
Machine Communication
Systems in Nuclear Power
Stations**

H. M. WILKINSON

**Prepared for the International
Atomic Energy Agency
Munich, Germany
December 5-7, 1979**

EVOLUTION OF COMPUTER-BASED SURVEILLANCE,
CONTROL AND MAN-MACHINE COMMUNICATION
SYSTEMS IN NUCLEAR POWER STATIONS

Prepared By H.M. Wilkinson

ABSTRACT

Over the past 15 years, covering five successive generations of instrumentation systems, Ontario Hydro nuclear generating stations have benefitted from rapid advances in computer and display technology and from experience gained during actual operation.

Reactor surveillance systems, man-machine communication, control methods and system reliability have steadily improved with successive designs. These improvements have been dramatic. Operational results from nine power-reactor units and preliminary results from 12 more units in various phases of implementation are now becoming available. The scope of the improvements ranges from the first design which used only lantern type displays to the latest which uses 18 colour cathode ray tubes (CRT). The operator can now scan a parallel presentation of annunciator messages, bar charts and graphical presentations.

The computer controlled displays employ a variety of communication techniques such as flashing characters, colour codes, and making mimic diagrams available in several levels of detail. These immediately attract the operator's attention and assist him in determining the cause of malfunctions.

The surveillance systems are integrated with manual-automatic control stations, other operator interfaces, the reactor regulating software system, and turbine generator control algorithms. The objective is to acquire all pertinent measurements of reactor and other unit parameters, which are then checked for validity. Some measurements provide direct inputs to computer control algorithms for automatic control of unit functions. These and other measurements, plus control outputs, are examined, sorted and presented to the operator so that he is able to comprehend immediately and clearly the status of all reactor processes. Failures or malfunctions result in control outputs moving in the safe direction.

The man-machine interfaces provide the operator with condensed detailed data so that any unusual conditions can be quickly and correctly assessed. The operator is able to call up CRT diagrams successively showing the overall process in increasing detail and to intervene selectively when action is justified. The display and controls are arranged so that the operator is guided toward correct action; inappropriate interventions are inhibited.

Very high reliabilities are achieved through the use of complete dual redundant circuitry and self-checking techniques. Experience is also teaching us the wisdom of using separate computer systems for indirectly related or auxiliary measurements and of keeping the unit control computer system dedicated to its principal objective of communicating with and sharing the control functions with the operator, each supporting the other.

INTRODUCTION

Ontario Hydro, established in 1906, is a crown corporation responsible to the Government of Ontario for the generation, transmission and distribution of electric energy in the province. It provides power to greater than 98 percent of the population of Ontario, and has ties to Quebec, Manitoba, and the United States. Ontario Hydro is one of the two largest utilities in North America, with an installed capacity (1979) of 25 000 MW.

The period of nuclear station construction covered by this paper is from 1962 to 1989, from the first 200 MW unit at Douglas Point to the proposed four, 850 MW units at Darlington.

EVOLUTION OF SYSTEM CONCEPTS

The advent of generating units greater than 500 MW coincided with the availability of process computers. The larger units require more complex instrumentation and the gathering, analysis and logging of more data than ever before. The control and instrumentation systems of CANDU nuclear power stations have undergone continual evolution in response to changes in regulatory requirements, increases in the size and power of the reactor, and the evolution of instrumentation and control technology itself.

The Douglas Point (Station 1) computer performs a monitoring function and employs a single, small computer. Only a six-character lantern type display is available to the operator. This may be contrasted with the dual-computer system for each of the generating units planned for Darlington (Station 6) where digital control is an integral part of the instrumentation system. An extensive man-machine communication system will be used, including 18 colour CRT screens for each unit and advanced operator interaction functions.

It is very important that reliability of these process control computer systems be extremely high. This has been achieved through the use of dual-computer systems (a master computer, DCC X, and 'hot' standby, DCC Y) incorporating self-checking, fault annunciation and automatic failover.

The computer system possesses a set of hardware and software checks which continuously monitors the system and takes appropriate action whenever an instrumentation fault is detected. The actions taken range from printing a message to the operator, to transferring control to the backup computer, to shutting down the generator in a safe manner.

Defenses (in depth) guard against computer and instrumentation failures. These include the operations monitor, executive software allied with countdown register and watchdog timers, software that allows restarts in the event of transient faults, and software data validity and input/output checks.

EVOLUTION OF DIGITAL COMPUTERS

Central Processing Unit Configuration

In 1962 a digital computer system was installed at Station 1. It consisted of a single CDC 636 computer with a 15-bit word and 8 k of core memory. All computer control systems installed in later stations use the dual redundant configuration. The Pickering A (Station 2) system employs two IBM 1800 computers per generating unit. Each incorporates 16 k words of 16 bits each (32 k bytes).

Bruce A (Station 3), Pickering B (Station 4) and Bruce B (Station 5) all use the same Varian V-72 computers in their dual systems. Core memory is now 32 k words (64 k bytes). Station 3 also has twice as much fixed-head disk memory as did Station 2, and introduced the first use of moving-head memory. Station 6 system design employs dual DEC 11/70 computers per unit, introducing larger core memory.

Process Control

At Station 1, the computer system is not essential to keep the reactor unit active. The computer performs only minor control functions, e.g., reactor flux-tilt control and automatic power setpoint control.

The Station 2 computer system performs a greater variety of functions, many of which are control functions essential to operation, e.g., reactor power control, boiler pressure control, control of power output, turbine run-up, and fuelling machine control.

The general concept for the computer system remains the same at Station 3, with the exception that more functions are incorporated into the system; however, the fuelling machine control is transferred to a separate computer unit.

The computer-driven process controls at Stations 4 and 5 are very similar to those at Station 2.

Station 6, while employing the familiar dual configuration, uses the increased computing power to provide expanded functional capabilities.

Monitoring

The desire to provide the operator with faster and more reliable monitoring functions and more accurate process monitoring has been met by incorporating increased capability with each succeeding station.

The Station 1 system performs some monitoring tasks, e.g., alarm scanning and logging, fuel channel temperatures log and xenon poison monitoring.

In all computer monitoring systems after Station 1, large amounts of process data are acquired and processed directly by the control computers. Processing of the raw data is used to reduce the amount of information displayed on the control panels. Overcrowding is reduced and the status of the station is more efficiently presented. The operator is relieved of much routine logging of information.

Channel temperature monitoring and xenon poison level evaluation are performed by the computers in all stations. Hourly logs, trend logs, and billing and metering of station energy loads are also handled by the computers.

Digital and Analog Inputs and Outputs

The number of digital and analog sensors from the first to last unit has increased from 630 (80 digital and 550 analog) to 2736 (656 digital and 2080 analog), an increase factor of 4.3. A similar expansion has occurred for digital and analog outputs. Station 1 possesses a total of 63 (46 digital and 17 analog) compared with each unit at Station 6 which will handle 520 outputs (448 digital and 72 analog), reflecting an increase factor of 8.2.

Display Systems

In early process systems, instruments were mounted on the equipment they measured and controlled. The operator was able to observe the actual control functions being performed. As systems grew in size and complexity, control panels were built (all instrumentation at a single location). To assist the operator to associate instrument locations in the process, flow diagrams (or mimic diagrams) were included, with the instruments often located in their actual position on the diagram. Such techniques are in use at Stations 1, 2, and 3; however, this does not lead to compact control panels.

The application of computers to process control introduced several new factors:

Operator-Computer Communications. Highly reliable and sophisticated man-machine interfaces are now required to enable the operator to absorb this increased information and to instruct the computer to execute the appropriate control functions.

At Stations 1 and 2, the man-machine interface was considered primitive and access facilities relatively slow. As a result, both of these stations required many hard-wired control panel displays.

At Station 2, the control philosophy is such that all indications and controls essential for operation (start-up, shut-down, and normal) are located on control room panels. Controls for any system requiring attention within 15 minutes of an alarm occurrence are also located there. Controls are mounted in the plant for those systems which can wait longer without attention.

The control centre layouts are not identical for all four units and they are also *mirror-imaged. These two factors are now judged to be undesirable for the operators. The decision has been made that future control equipment layouts and functions will be identical for all units in one station.

The innovative aspect of the Station 3 computer control system lies in its man-machine subsystem. The decision was made to convert many of the Station 2 conventional analog loops, indicators and recorders to direct digital control.

The computer-based display system of Stations 3, 4, and 5 is extended and enhanced at Station 6. Formats are further developed and simpler and faster methods of initiating a display have been achieved.

A back-up system, consisting of a minimum complement of dedicated hardware display devices, sufficient to provide control and to ensure the safety of the unit in the event of a total failure of the computer driven display system, is also provided.

Alarm Annunciation. Station 1 employs 600 window annunciators to communicate alarm conditions to the operator. It is difficult for the operator to monitor the alarms.

At Station 2, the use of alarm windows was reduced by substituting a monochromatic CRT. Alarms are recorded on a hard-copy printer, to avoid their being lost or forgotten after being cleared from the CRT.

Two of the 10 CRT in each generating unit at Station 3 are used to display messages associated with alarm annunciation. These two CRT are mounted one above the other, directly in line with the operator's desk. Simultaneously, more detailed recorded messages of these events appear on a printer. Approximately 50 messages can be displayed at one time (25 per CRT). A full page CRT image can be recorded by the printer in two seconds.

Station 4 is the first to employ colour CRT. Two such colour CRT are used for alarm messages.

CRT and Other Devices. At Station 1, output to the operator is accomplished through printers and alpha-numeric indicators.

To display data at Station 3, monochromatic CRT supported by a minimum number of hard-wired display devices are used. Such CRT displays provide alpha-numeric tables, bar-charts, graphical trends, and special purpose formats. The operator selects a display by dedicated function pushbuttons.

Eight of 10 CRT at Station 3 are capable of displaying graphical information. Eight keyboards are available for operator-to-computer communications. Annunciation windows, two high-speed printers, electro-mechanical indicators and small indicator lamps also support the man-machine interface.

*Note: The control panels themselves were not mirror-imaged; only the computer racks installed in the equipment rooms behind the control panels. However, this caused difficulties in quickly locating specific units during emergencies.

Computer-driven, colour CRT display systems are proving to be a powerful tool in enhancing the man-machine interface. Despite a high degree of automation, the operator is required to evaluate the station conditions quickly and correctly during abnormal conditions and to initiate the appropriate corrective action. To do this at Station 2, the operator depends heavily upon information provided by conventional indicators.

At Station 4, the computer processes plant data and related information which is presented on a single CRT, in a format designed to aid correlation. Also, approximately 350 separate process control panel indicators are used for each unit. If the CRT computer-based indications were not available, the number would be much larger; however, at this station there is no reliance on the CRT for critical parameter displays.

The Station 4 system is further expanded at Station 5. An extensive graphic colour CRT display system is employed, further reducing conventional instrumentation in the control room. Approximately 80 indications are located on the unit control panel, while 650 indications, on 105 different screens, may be found on the CRT monitors. Standard displays include status displays, bar-charts and trend plots. Hard-copy facility is available. A total of 10 computer-driven colour CRT monitors are provided for each unit, eight of which have full graphic and alpha-numeric capability.

The system planned for Station 6, Ontario Hydro's most modern nuclear plant, uses colour CRT monitors as the main output device, with a small number of alpha-numeric indicators and printers in a support role. Each CRT has the following capabilities: full colour, dedicated keyboard, 48 hours historical data, and provision for hard-copy output. Input devices include pushbuttons, keyboards and light pens for the CRT. The display system is organized in a hierarchical fashion, with flow diagrams as the primary format. Secondary formats are bar charts, graphical trends, and instrument and equipment status tables.

FUTURE INSTRUMENTATION SYSTEMS

Dramatic improvements in electronic solid-state technology and in display techniques continue unabated and advances in data storage have been achieved. In view of the significant advance in the technology available to system designers, the basic dual-computer configuration bears re-examination.

A promising approach lies in the development of distributed computer systems incorporating multiple smaller computers (or computer pairs for redundancy). This next generation of instrumentation systems will supply much higher reliability, simpler maintenance and improvement in operator interface.

The control systems designs presently being implemented for commissioning in the middle 1980s will likely be, despite their maturity, the last of their generation.

The next generation of computers in control systems will consist of a hierarchical structure of hardware and software sub-functions or modules partitioned according to process function (as opposed to partitioning according to computer function). Each one of these sub-functions of the total instrumentation system will incorporate its own computer. This will acquire data from sensors, process the data and develop its own control and display outputs according to target performance parameters received from an upper level processing unit.

When reliability targets dictate, each such sub-system will also incorporate a redundant computer system, or alternately, the upper level unit may be given sufficient capability to keep the system going in the face of a complete failure of the sub-system.

Another important consideration in future digital control systems is the desired degree of operator prompting provided by the computer monitoring and control system. It is important that there be a judicious balance between too much, where the operator makes essentially no decisions himself, and too little, where the operator is required to digest a mass of information in a short time and, as a result, can make incorrect decisions. Prompting should avoid specific operator instructions such as 'close breaker number 2'. If the instruction is that clear-cut, it should be done automatically.

One possibility is to have the system present one, two or more paragraph numbers in an operating procedures manual, which the operator should follow under the particular existing conditions. Another possibility is to actually present the procedures on a CRT screen.

A survey was conducted amongst some of the Ontario Hydro operating and commissioning personnel to determine their view of the degree of prompting desired during various operating conditions. The results are attached to this report.

Even the best trained humans will always make errors. A good system will prevent operator errors from having serious consequences and will also support or prompt the operator to make good decisions. The total instrumentation design should take the operator into partnership to achieve a balance of information in a practical and common-sense way.

BIBLIOGRAPHY

Boucher, D. and F. Shady. Control centre equipment - Pickering GS B design manual. Ontario Hydro, 1979.

Fenton, E. Control centre equipment - Pickering GS A design manual. Ontario Hydro, 1970.

Fenton, E. Darlington GS A preliminary report - control centre equipment study. Part 1 - control centre layout. Ontario Hydro.

Fenton, E. Darlington GS A preliminary report - control centre equipment study. Part 2 - man-machine interface. Ontario Hydro.

Hepburn, G.A. DCC software - Pickering GS B design description. AECL, 1977.

Kee, F. and J. Smith. Development of a reliable single channel direct digital reactor control system. IAEA-SM-226/103, 1978.

Kee, F. and W. Cooper. Control and instrumentation systems in CANDU plants. 1979.

Koekebakker, J. Digital control of nuclear power stations. Power Engineering, 1975.

Lee, S. Unit computer systems - application software - Darlington GS A design description. Ontario Hydro, 1978.

Magagna, L. Control computer systems in generating stations in Ontario Hydro - design approach and experience. 1976.

Magagna, L. and J. Smith. Control computer applications in Ontario Hydro's nuclear stations. 1976.

Mahood, T. Computer control of the Bruce Nuclear Power Station. 1975.

Moore, B. Control room design and man-machine interface - operations requirements for nuclear-electric station design. Ontario Hydro, 1978.

Olmstead, R. and P. Dai. CRT man-machine communication systems - Bruce GS design manual. AECL, 1975.

Ontario Hydro. Power resources report. April 1979.

Tong, H. Digital control computer system - Bruce GS B design description. AECL, 1978.

West, R. Control centre - Bruce GS design manual. AECL, 1974.

Wilkinson, H.M. Electrical generating stations course lecture notes on control computers. Ontario Hydro, 1978.

Acknowledgements: In addition to those mentioned in the above references, the author wishes to acknowledge the following who made valuable contributions and significant comments during the preparation of this article: D. Ammerman, D. Beattie, R. Burnard, G. Hall, R. Hohendorf, B. Kostic, L. Maki, M. McPhedran, D. McQuade, B. Moore, D. Walsh.

TABLE 1
Nuclear Generating Stations Overview

STATION	#1 DOUGLAS PT.	#2 PICKERING 'A'	#3 BRUCE 'A'	#4 PICKERING 'B'	#5 BRUCE 'B'	#6 DARLINGTON
ELECTRICAL ENERGY OUTPUT	1 x 200 = 200 MW	4 x 540 = 2160 MW	4 x 750 = 3000 MW	4 x 540 = 2160 MW	4 x 750 = 3000 MW	4 x 850 = 3400 MW
REACTOR THERMAL ENERGY OUTPUT	1 x 660 = 660 MW	4 x 1655 = 6620 MW	4 x 2700 = 10 800 MW	4 x 1655 = 6620 MW	4 x 2700 = 10 800 MW	4 x 2800 = 11 200 MW
IN SERVICE DATES (FIRST/LAST UNIT)	1962	1971/73	1977/79	1982/83	1983/87	1987/90
INSTRUMENTATION & DISPLAY DDC	CDC 636	4 UNIT x 2 + 1 IBM 1800	4 UNIT x 2 + 1 VARIAN V-72	4 UNIT x 2 + 1 VARIAN V-72	4 UNIT x 2 + 1 VARIAN V-72	4 UNIT x 2 + 2 DEC 11/70
NO. OF DIGITAL INPUTS	80	400	512	448	576	656
NO. OF ANALOG INPUTS	550	1152	1408	1408	1840	2080
NO. OF DIGITAL OUTPUTS	46	272	408	256	504	448
NO. OF ANALOG OUTPUTS	17	42	32	42	36	72
TOTAL NO. OF INPUTS & OUTPUTS	693	1866	2360	2154	2956	3256
DISPLAY CRT (PER UNIT)	NONE (CHAR- ACTOR ONLY)	2 CRT 6 NIXIES	10 CRT	9 CRT	10 CRT	18 CRT (COLOUR)
PRINTERS	3 TYPEWRITERS	2	2	2	2	2
MIMIC DIAGRAMS	0	0	2	1	6	48
NO. OF MAJOR REAL-TIME SOFTWARE ROUTINES	4	10	18	14	18	19

TABLE 2
Control and Monitoring Instrumentation

	#1 DOUGLAS PT.	#2 PICKERING 'A'	#3 BRUCE 'A'	#4 PICKERING 'B'	#5 BRUCE 'B'	#6 DARLINGTON
1. POINT ALARM SCANNING	D	D	D	D	D	D
2. CHANNEL TEMPERATURE MONITORING	D	D	D	D	D	D
3. XENON MONITORING (1) PLUS PREDICTION (2)	D (1)	D (2)	D (2)	D (2)	D (2)	D (2)
4. REACTOR REGULATING SYSTEM		D	D	D	D	D
5. UNIT POWER REGULATION	D	D	D	D	D	D
6. BOILER PRESSURE CONTROL		D	D	D	D	D
7. MODERATOR TEMPERATURE CONTROL			D	D	D	D
8. REACTOR STEPBACK			D	D	D	D
9. FLUX MONITORING & MAPPING			D		D	D
10. TURBINE MONITORING			D	D	D	D
11. TURBINE RUN-UP		D	D	D	D	D
12. FUELLING MACHINE CONTROL		D	D (3)	D	D (3)	D (3)
13. SEQUENCE OF EVENTS MONITORING		D	D	D	D	D (3)
14. PRIMARY HEAT TRANSPORT CONTROL					D	D
15. BOILER LEVEL CONTROL						D
16. DEAERATOR CONTROL						D
17. CRT MESSAGES (ALPHA-NUMERIC)		D	D	D	D	D
18. CRT GRAPHICS			D	D	D	D (4)
19. HISTORICAL DATA STORAGE					D	D

D - DIGITALLY CONTROLLED

NOTE: 3-CONTROL IN SEPARATE COMPUTERS
4-EXTENSIVE GRAPHIC CAPABILITY

TABLE 3
Degree of Prompting Survey

CONDITION	NONE - LITTLE - SOME MAJOR FUNCTIONS - MORE DETAIL - COMPLETE										
	0	1	2	3	4	5	6	7	8	9	10
1. NORMAL OPERATION (NOTE 1)	[Graph showing average value at 3 and range from 0 to 6]										
2. UNIT START-UP (NOT INCLUDING TURBINE RUN-UP)	[Graph showing average value at 6 and range from 2 to 8]										
3. TURBINE RUN-UP	[Graph showing average value at 6 and range from 4 to 8]										
4. NORMAL LOAD CHANGES	[Graph showing average value at 4 and range from 1 to 10]										
5. REACTOR TRIP (SAFETY SYSTEM INITIATED)	[Graph showing average value at 3 and range from 2 to 5]										
6. TURBINE TRIP (GRID DISCONNECT)	[Graph showing average value at 4 and range from 2 to 6]										
7. LOSS OF AN ELECTRICAL POWER BUS	[Graph showing average value at 4 and range from 2 to 6]										
8. MAJOR ALARM CONDITION	[Graph showing average value at 6 and range from 3 to 10]										
9. MINOR ALARM CONDITION	[Graph showing average value at 3 and range from 0 to 6]										

NOTE 1: DURING THIS TIME, THE OPERATOR IS PRIMARILY OCCUPIED WITH WORK ORDERS, REQUESTS, ADMINISTRATION, ETC.

KEY:
● = AVERAGE VALUE
[Wavy line with dots] = RANGE OF VALUES, HEIGHT INDICATES RELATIVE BUNCHING OF RESPONSES

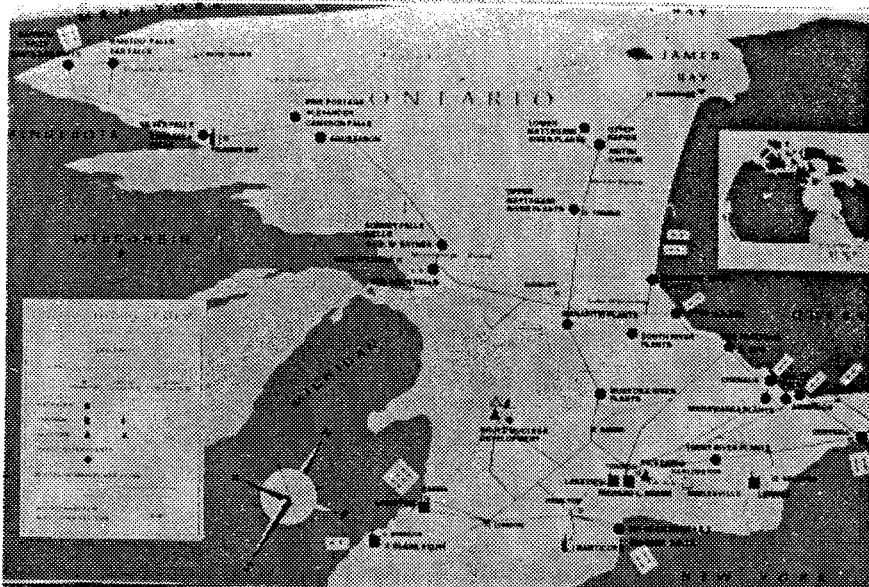


FIGURE 1
Ontario Hydro System Map

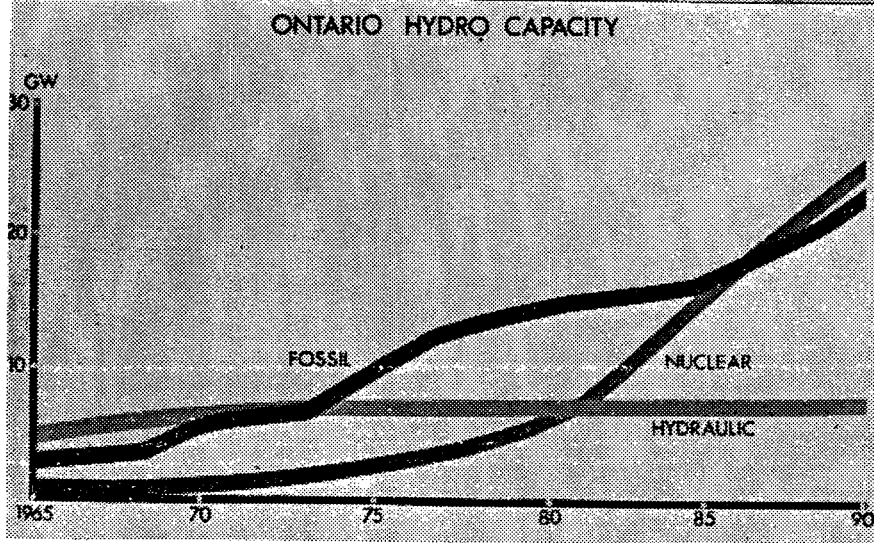


FIGURE 2
Ontario Hydro Capacity

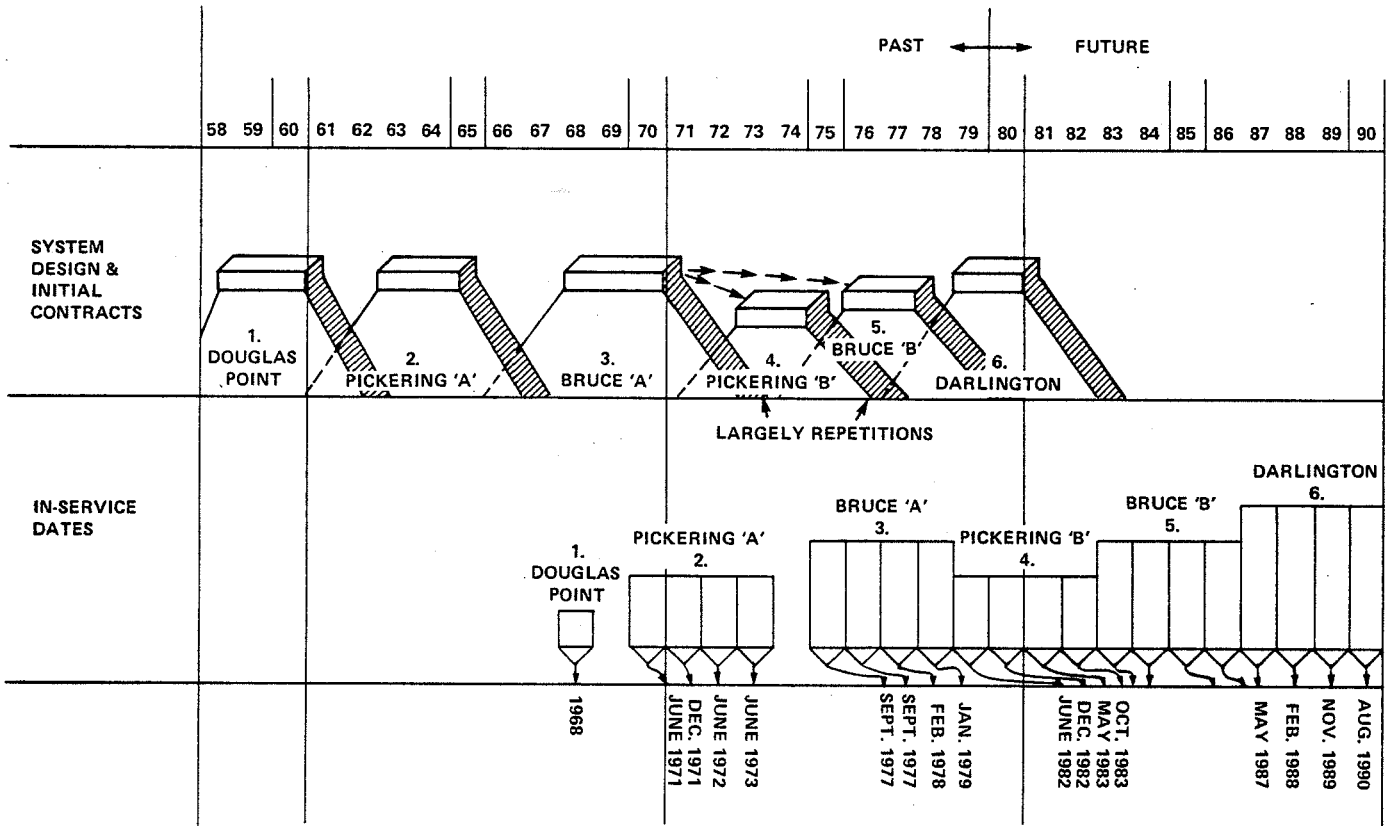
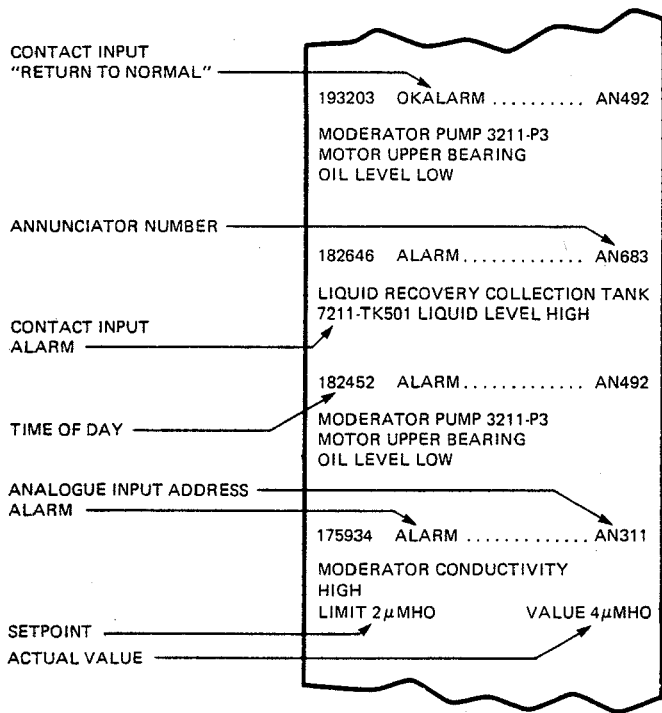


FIGURE 3
Station Design and Implementation Dates



TYPICAL COMPUTER ALARMS
PICKERING 'A' (STATION #2)

FIGURE 4
Example of Alarm Display and Printout

C	00:00:00:000	B20P A50N IRX
C	00:00:00:020	B20P A50 IRX
C	00:00:00:052	B20P A21P2 KD4
C	00:00:00:064	PROT B20P A2161 KDGH
C	00:00:00:084	B20P A21G2 KDGH
C	00:00:00:096	B20P A77SP PERM T11
C	00:00:00:096	PROT B20P A21P1 KD4
C	00:00:00:116	B20P A94TT INST TRIP
C	00:00:00:128	TRIP B20P LINE MAIN A
C	00:00:00:148	P20P A94RTS INIT TT T13
C	00:00:00:160	B20P A94RTSA TT T13
C	00:00:00:180	DIL20 A94-1 INIT CBT
C	00:00:00:192	BREAKER DIL20 A33A
U	00:00:00:212	B20P A77SP PERM T11
U	00:00:00:224	B20P A50 IRX
U	00:00:00:244	B20P A21P2 KD4
G	00:00:00:256	P20P A94RTS INIT TT T13

FROM BRUCE 'A' (STATION NO. 3)

FIGURE 5
Example of Sequence of Events Printout

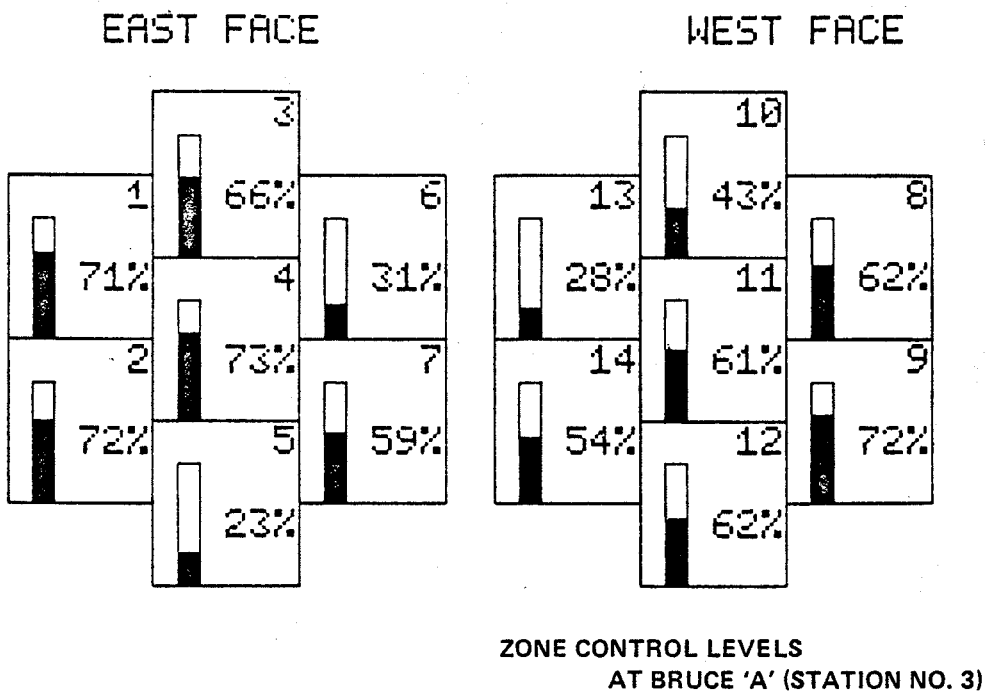


FIGURE 6
Example 1 of Graphic Display Printout

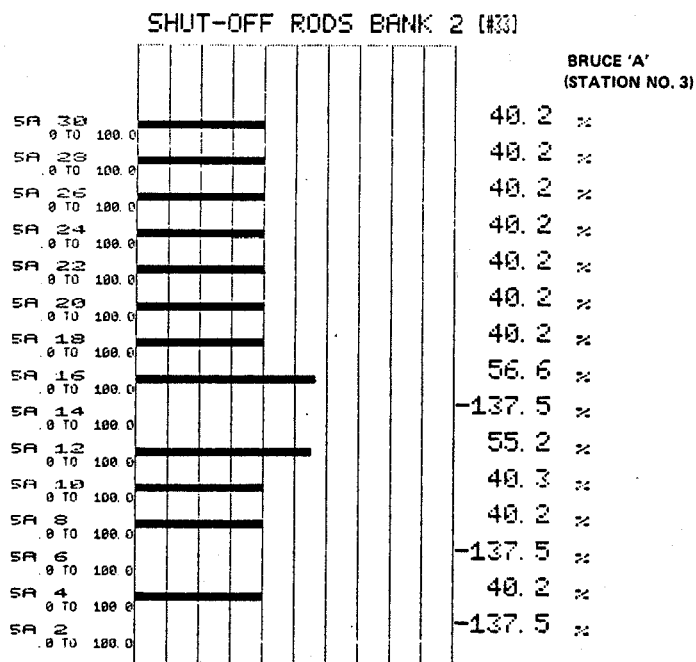


FIGURE 7
Example 2 of Graphic Display Printout

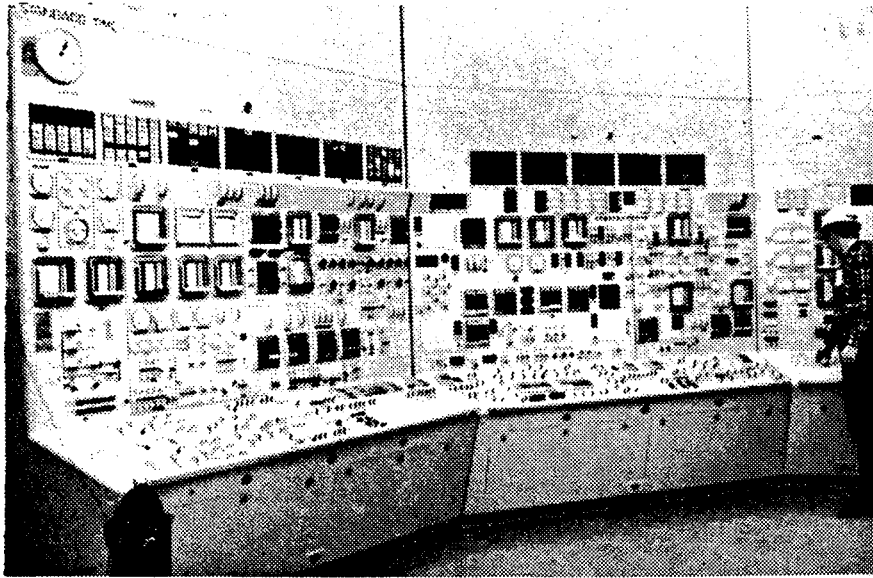


FIGURE 8
Example 1 of Control Room Layout
Douglas Point (Station 1)



FIGURE 9
Example 2 of Control Room Layout
Pickering 'A' (Station 2)

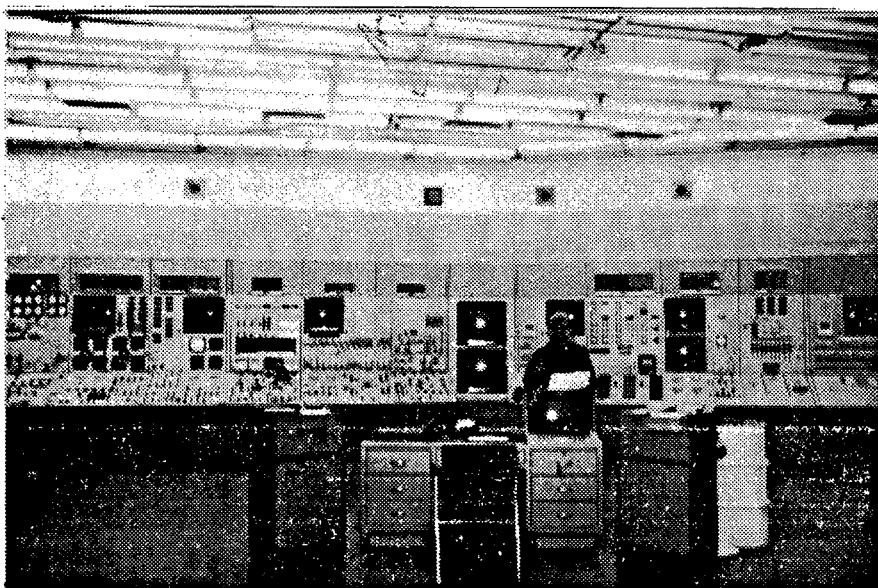


FIGURE 10
Example 3 of Control Room Layout
Bruce 'A' (Station 3)

C. Hermant, G. Guesnier

DATA PROCESSING AND DATA DISPLAY IN ELECTRICITE DE FRANCE PWR
1300 MW NUCLEAR POWER PLANTS

I.A.E.A. working group on nuclear plant control and instrumentation.

Specialists' meeting on

"Procedures and systems for assisting an operator during normal and anomalous nuclear power plant operation situations".

December 5 - 7, 1979 - Munich - R.F.A.

DATA PROCESSING AND DATA DISPLAY IN
ELECTRICITE DE FRANCE PWR 1300 MW
NUCLEAR POWER PLANTS

By C. HERMANT
G. GUESNIER

ELECTRICITE DE FRANCE

Service Etudes et Projets Thermiques et Nucléaires

Abstract : In E.D.F. PWR 1300 MW nuclear power plants, digital control is achieved by automatic devices using electronic integrated components with programmed logic. These modular systems have been designed by CGEE-ALSTHOM under E.D.F. requirements and are named CONTROBLOC. They actuate digital control of 1300 MW unit equipment and also provide logic indications and warnings on conventional displays and on alphanumerical colour CRT's.

Moreover, a dual-computer system designed by CERCI-SINTRA centralizes logic and analog data. Logic data generated by CONTROBLOC cabinets are sent to computer on multiplexed lines. Analog data are transmitted conventionally or by digital means.

The paper describes the design of that system and explains the features which facilitate control and monitoring of the whole generating unit.

I - OVERALL STRUCTURE OF THE INSTRUMENTATION AND CONTROL

The level of technological advancement of the Instrumentation and Control for the PWR 1300 MW units of "ELECTRICITE DE FRANCE" (The French National Electricity Utility) is considerably ahead of the similar systems for the PWR 900 MW units : on the 900 MW units, almost all the automatic control equipment was based on electro-magnetic relays or, for some of them, based upon wired logic modules. For the 1300 MW units, programmed digital techniques are used :

- the reactor protection system (R.P.S.), developed under the name S.P.I.N., has a multiprocessor structure and an architecture based upon quadruple redundancy,
- the logical automatic control for the unit to be in and out of service and for automatic protection of conventional equipment, developed under the name CONTROBLOC, have a modular structure, and is programmed, multiplexed, using the technique of distributed software,
- the equipment for controlling and measuring the positions of the control rods and the equipment measuring the flux in core, are also designed around microprocessors.

This wide use of programmable equipment makes it possible to develop multiplexed links among these equipment items and the complementary data processing system, and also to implement, more easily than with wired equipment, the control logic and the signalling logic. The cost of this signalling and alarm logic, logic which must be fairly sophisticated if it is desired that the operator be supplied only with information which is judicious and unambiguous, actually becomes marginal when using programmed logic.

For the processing and presentation of the data, the general approach decided upon, is as follows :

- the analog values presented in the control room on conventional equipment (recorders, indicators) are those which are necessary for the normal running of the plant unit, or those which are important from the point of view of safety and security of equipments,

- the reactor protection system (SPIN) generates and initiates the protection actions, directly affecting the actuators ; the signals and alarms which it generates, are, on the other hand, transmitted to the "CONTROBLOC" controller,
- the "CONTROBLOC" controller performs all the alarm processing. It performs the logic processing which makes it possible to only supply the operator with the data which is necessary for him at a given moment.

The alarm signals are presented on annunciator windows when they require immediate operator action, otherwise they appear on visual data display units. For the mimic panels and the state of the protection system sensors, the signals are presented using LEDs (Light Emitting Diodes).

- Almost all the measurements, all the status signals and alarms, a major part of the sensor and actuator status are input to the complementary data processing. The logic status are transmitted from the "CONTROBLOC" equipment via multiplexed links ; the measurements acquired by the SPIN are transmitted from the SPIN equipment via multiplexed links; all the other measurements are transmitted by wires.

With this organization, the complementary data processing system is not indispensable for a steady running of the plant unit. However, owing to the volume of data which it receives, to its processing and memory capacity, it supplies the operators with more complete and more sophisticated information than the information directly associated with the automatic control systems, which make it possible for the operating team to better understand the installation, to optimize its operation, to reduce its downtime.

II - THE ROLE OF THE COMPLEMENTARY DATA PROCESSING (TCI)

The complementary data processing has a triple role :

1/ an operating assistance role, consisting of :

- . automatic supervision of measurements,

- . man-machine conversational facilities so that the operator, upon request, can have tables, curves, informational flow diagrams,.... immediately giving him the precise elements on the state or the trends in the installation, or giving him the possibility of analyzing a situation,
- . calculating and simulating functions making it possible to optimally act on the control rod assemblies and on the boration during programmed charge variations (so-called reactor control function).

2/ An after-the-fact analysis tool role, consisting of :

- . the man-machine conversational facilities for the analysis of the immediate past of the installation,
- . data logging facilities for off-line processing of malfunction data, or analysis of the statistical behavior of the equipment.

3/ A role of acquisition and processing of in core recordings, consisting of :

- . acquiring the data necessary to understand the distribution of nuclear flux in the reactor,
- . to perform calculations on this data,
- . to transfer this data onto a portable medium for later use.

III - STRUCTURE OF THE TCI

Unlike the structure for the 900 MW plant units, the TCI for the 1300 MW plant units has a two-level processing structure.

The first level acquires the logic and analog data coming from the installation and performs the necessary processing to supply the operator, with the information which is immediately usable for the running of the unit ; a second level, connected to level one, receives all the data acquired by the first level and performs all the other processing.

This two-level structure is not redundant since the loss of level one, results in the loss of level two which would no longer receive data ; however, this structure provides the following advantages :

- it makes it possible to share the processing and acquisition job between two processors, lightening the load for each of them ; the volume of data to be acquired (5000 logic data elements, 1200 measurements) and the existence of a complex processing for reactor control, strongly motivated this organization,
- it makes it possible to quickly make available on the site, from the beginning or the tests on the plant unit, a simple structure, that of level one, whose relatively small programs are conventional and will probably evolve little, but are sufficient to run the start-up tests under good conditions while level two, whose programs are more complex and are subject to a certain amount of evolution, has more available time to be carried through in workshop, before installing on the power plant itself,
- it makes it possible to specialize the functions assigned to the two levels : the essential functions of level one are acquisition and real time processing while level two, separated from the process by level one, is less specialized and is essentially used as "management-calculation" function.

3.1 - Structure and functions of level 1

Level 1 acquires the state changes of the logic data coming essentially from the "CONTROBLOC" via multiplexed links (approximately 5000 data elements, distributed over 80 links) and the analog data coming from instrumentation (approximately 1000 measurements) and from the SPIN (400 measurements).

a/ Logic data

. Chronological storage

The logic data changes are intended to be stored in chronological order.

They are transmitted to level 2.

. Data logging

On one of two semi-graphic polychrome screens assigned to level 1, and arranged in the normal operating zone of the plant unit, the operator can obtain, upon request, the last 23 status changes.

He can also obtain a print-out on one of the two printers assigned to level 1.

b/ Analog data

. Acquisition

The 1000 analog signals coming from the instrumentation (thermocouples and 0-500 mV signals) are acquired at rates of 2 seconds (100 measurements) 20 seconds (160 measurements), 60 seconds (750 measurements), linearized and validated (measurement range check), while the 400 measurements coming from the SPIN are transmitted by four asynchronous multiplexed links ; the control rod assembly position data and the flux measurement data acquired by the in core recording control system, are also transmitted by multiplexed links.

. Supervision

An automatic surveillance processing, covering about 700 measurements, compares each measurement to one or several thresholds values and actuates an alarm when a threshold is exceeded. The alarm message is presented on screen.

The operator has dialogue facilities making it possible for him to temporarily modify the threshold values, within a limit of 23, and a table of modified thresholds, automatically updated, is presented to him on screen or on printer, upon request ; any threshold which is exceeded is processed as a logic state change.

The redundant measurements coming from the SPIN are compared among themselves and an alarm message appears on screen when the redundant analog measurements differ from each other by more than a given value,

. Inhibition

The operator has dialogue facilities making it is possible for him to inhibit a measurement or a group of measurements, that is to interrupt all the processing relative to this measurement or to this group of measurements. The inhibited measurement table (maximum capacity 300 measurements), is presented to him upon request, on printer or screen.

. Evolution

The operator can also request display or printing of evolution of one or several measurements in time, at one column per measurement (maximum 20 columns), the total capacity being limited to 60 values per measurement. On the screen, the operator can consult all these 60 values to know the trend of those measurements.

3.2 - Structure and functions of level 2

Level 2 receives from level 1 :

- the logic states, every 2 seconds,
- the status changes, stored in chronological order,
- the measurement values at their acquisition speed.

The dialog facilities at the disposal of the operator include two semi-graphic polychrome screens, with two associated keyboards and an electrostatic printer ; the conversation station is organized in such a way that the two screens can be managed each independant from the other.

a/ Presentation of status data

Upon request, the operator can obtain, on screen or printer, the presentation of :

- . tables of logic states and measurement values for a functional element,
- . tables of values for groups of measurements whose composition and modification are accessible to the operator on demand,
- . the list of alarms present,

- . the list of non-available actuators,
- . temperature maps,
- . circuit flow charts with the information concerning the values and states of the main elements.

b/ Log and history of state changes

The laster 10,000 logic status changes are stored on disk and the operator has facilities for dialogue and seeking which make it possible for him to restore any hourly section on screen or printer.

c/ History and follow-up of measurements

Since the measurement values are stored on disk over a period of 24 hours, at their normal acquisition rate, the operator can obtain on screen, in the form of curves or digital values, a presentation of the trends of these measurements, by groups from 1 to 6, in any hourly section. The trends may be restored on electrostatic printer.

d/ Turbogenerator data

Fast recording processing is intended to present concisely, a certain number of events concerning the position of the main steam valves of the turbine and its speed, whose rapid evolution is to be correlated.

The changes of approximately 80 logic status are permanently stored in memory in a table where is stored, at the acquisition rate of 0,2 s, the speed of the turbine ; this data is accessible to the operator over a period of 24 hours.

e/ Fault analysis

The purpose of this processing, whose precise specifications are not as yet established, is, for certain types of disturbances, to supply the operator with the indication of the signal initiating triggering, and a diagnostic concerning the origin of the disturbance.

f/ Assistance for reactor control

EDF's 1300 MW reactors are controlled with advanced grey rods system, with protections by DNB and F_0 meter, use of multistage ex-core chamber, the units being studied for load following. The functions to be fulfilled for control by TCI are now being defined. The code used enables operator to obtain an axial representation of the core, with on-line identification of the module ; as a possible function, it is anticipated to provide off-set axial monitoring, taking into account the Xenon oscillations, a guide to minimize effluents, the optimum conditions for power return after emergency shut down....

g/ Calculations, in core measurement processing

In addition to the calculations linked to the assistance for reactor control, the main calculations performed, either periodically, or upon request, essentially consist of :

- the thermal power,
- the Xenon calculation,
- the reactivity analysis,

During the in core surveys, the TCI receives from the mobile detector control system, the flux values measured every eighth millimeter. These values are processed by the TCI so as to eliminate the aberrant values and, with a certain number of complementary data elements (position of the control rod assemblies, core temperatures, power...) loaded on a floppy disk for processing in the computer center.

h/ Daily analysis and daily history of the plant unit

This function leads to the automatic printing of a reference document summarizing the physical operation of the plant unit during the preceding day.

It includes overall analysis (number of hours of operation, energy analysis, fuel irradiation), a summary with the time and date of the main malfunctions and the half-hourly values of the principal physical parameters.

i/ Recording

The recording functions performed at level 2 are important because they concern the 10,000 latest logic state changes and all the measurements over a period of 24 hours. This data must be permanently accessible to the operator and it is stored on disk, with possibility to be loaded on a magnetic tape, each day.

°
° °

C.D.P 1300 MW

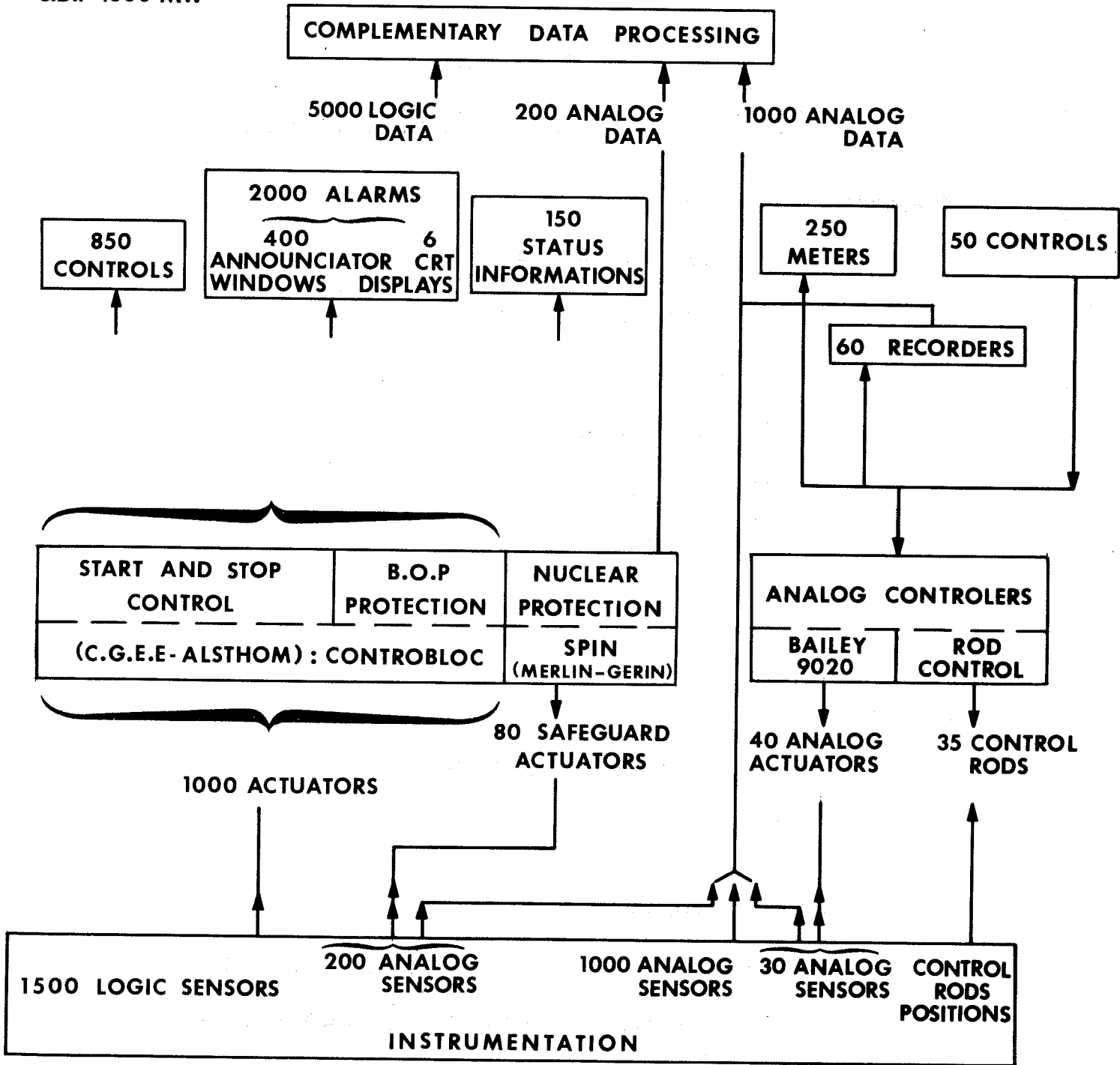


Figure 1

1300 MW PWR UNITS

COMPLEMENTARY DATA PROCESSING FUNCTIONS

I HELPING OPERATORS

AUTOMATIC SUPERVISION OF MEASUREMENTS

COMPARING TO THRESHOLDS

COMPARING THEMSELVES

OPERATOR SYSTEM DIALOG

MIMICS

MEASUREMENTS

STATUS TABLE

CHANGES OF STATUS

II CALCULATIONS

IN CORE MEASUREMENT PROCESSING

THERMAL POWER

III AFTER THE FACT ANALYSIS

IMMEDIATELY BY MEANS OF OPERATOR DIALOG

OF LINE, THANKS TO STORAGE ON MAGNETIC TAPE

IV ASSISTANCE FOR REACTOR CONTROL

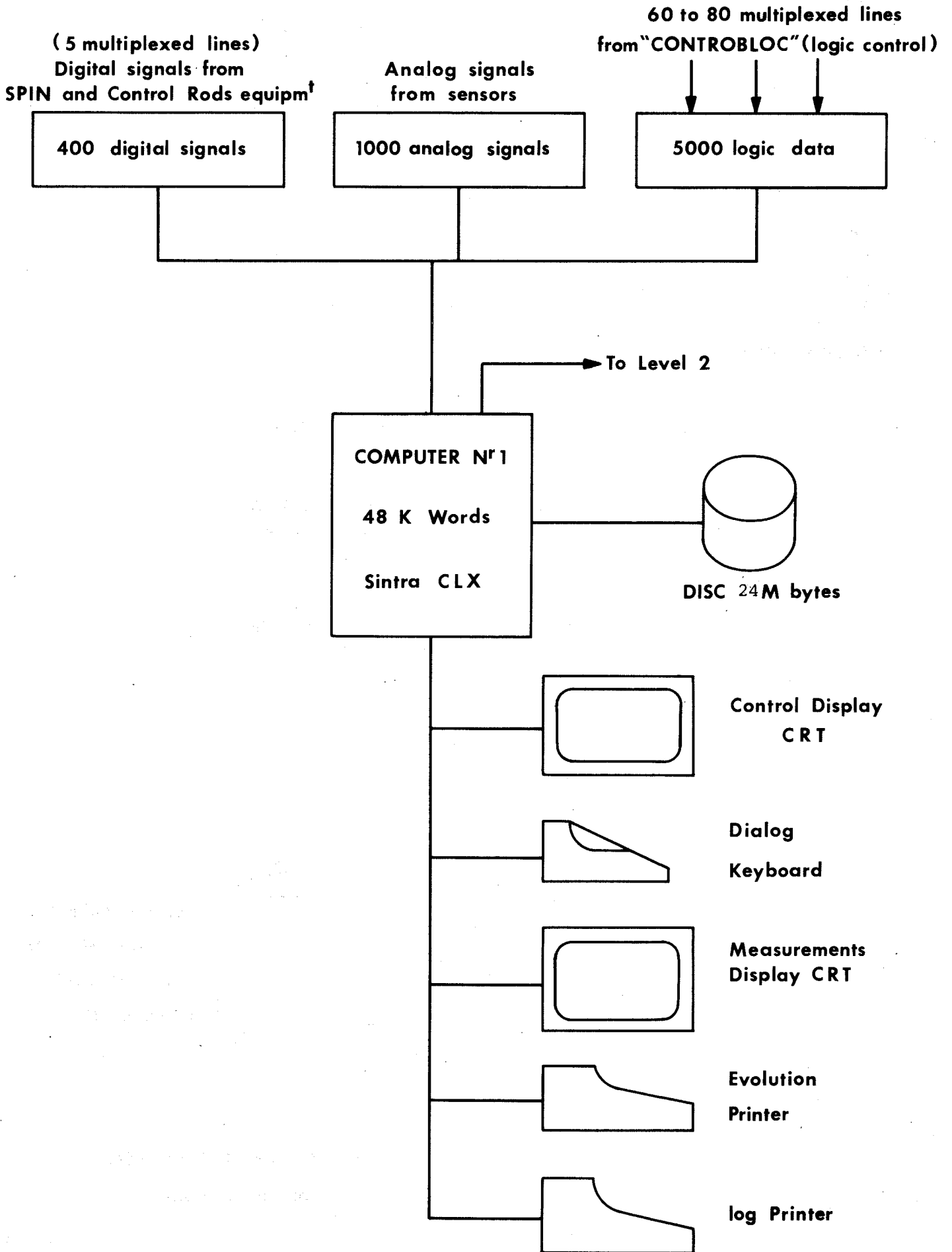


Figure 3

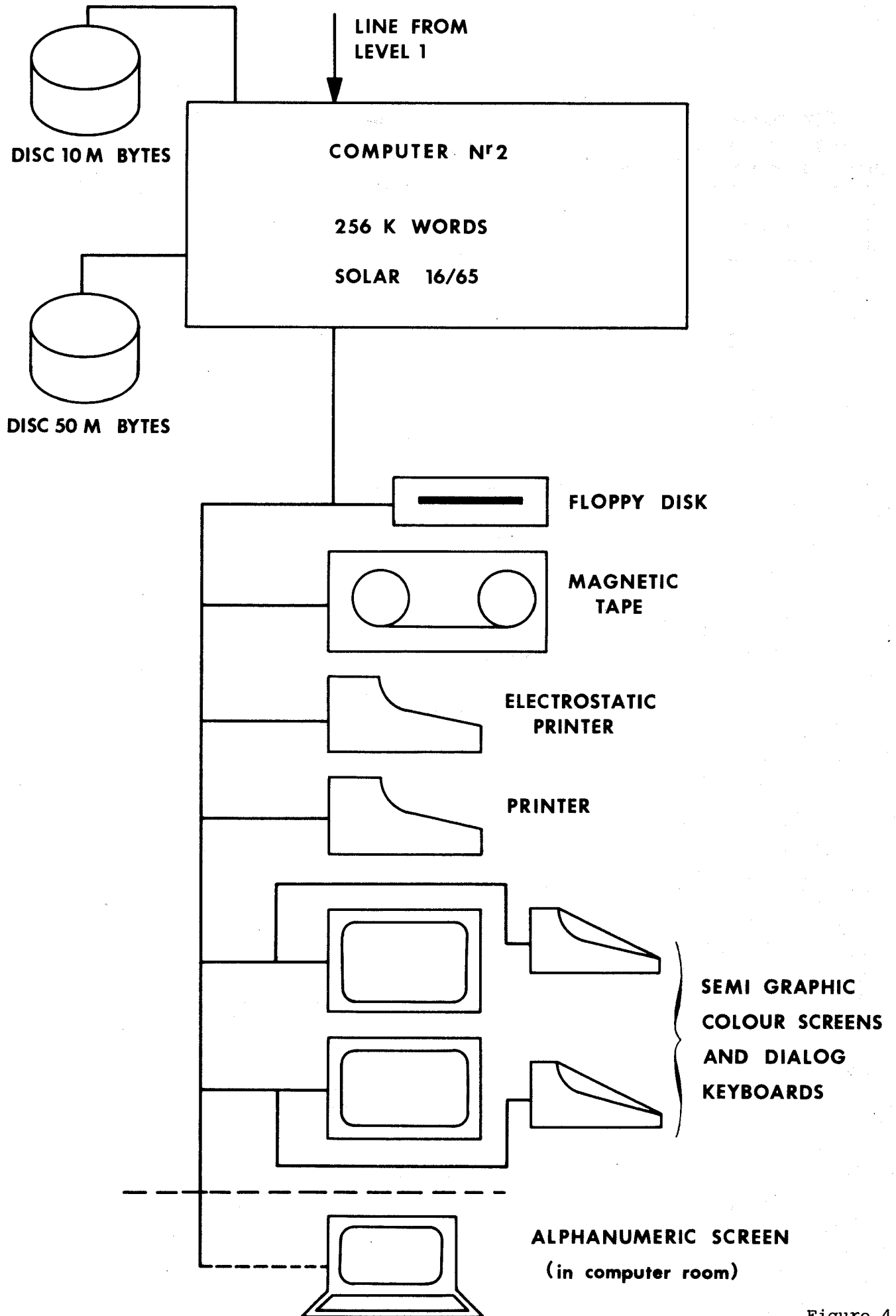


Figure 4

J. Helske, B. Wahlström

ON THE DETECTION OF PLANT ABNORMALITIES BY SUITABLE CONTROL ROOM
LAY-OUT, EQUIPMENT AND POSSIBILITIES FOR COMPUTERIZED OPERATOR
SUPPORT SYSTEMS

J Helske
B Wahlström

ON THE DETECTION OF PLANT ABNORMALITIES BY SUITABLE CONTROL ROOM
LAY-OUT, EQUIPMENT AND POSSIBILITIES FOR COMPUTERIZED OPERATOR
SUPPORT SYSTEMS

1

Introduction

Rare incidents have got an increasing attention when the safety of nuclear power plants is considered. The main difficulty in treating such incidents systematically is that a long chain of events leading to the incident has to be postulated and evaluated. In the case human intervention is possible either by correcting or worsening the situation a reliable estimate of the probability of the incident is even harder to give. The human component is however very important in determining the overall safety of a plant and it is clear that the environment for the operating personnel should be designed for the highest possible reliability.

In considering the reliability of human work the operating personnel could influence the safety of the plant either in a positive way by doing outstanding work or in a negative way by making errors. The human errors are very much situation dependent and if sabotage could be neglected then it could be postulated that all human errors are situation induced.

Before considering the quality of human work in more detail it is necessary to consider the division of tasks between man and machine. The philosophy for the design of automation systems and control rooms is very much dependent on tradition and views and is therefore varying between different countries and companies. Considering the division

of tasks from a safety point of view it however seems clear that actions responsible for the immediate safety of the plant should be automated and actions requiring understanding and planning should be reserved for the operating personnel.

When the control room situation is evaluated with the aim of finding ways for giving the operators the best support and for decreasing the probability of operational errors both the control room lay-out and the control room procedures have to be considered. In the control room important information could either be non-existent, awkwardly obtainable or masked by other information. The procedures again could place too high a demand on the operators or be difficult to learn and remember.

In the control room information could be presented either as a raw information with meters and indicators connected directly to the sensors or as processed information with displays connected to some signal processing device. The main difficulty in presenting only raw information is the large amount of information which is coming to the control room. Important information is then easily lost if not cued in some suitable way. It is therefore often advantageous to present processed information which means that a form of data reduction is done automatically. On the other hand the use of too much processed information will increase the danger of having an important single sensor masked by other information.

2

The nuclear power station Loviisa (2 x 440 MW)

The reactor of Loviisa NPS is a pressurized water reactor (PWR) of type VVER-440 (465 MW). The primary circuit of each unit comprises six loops with six steam generators of horizontal type and the secondary circuit of each unit is built with two turbines, two feed water tanks and full condensate purification plants. Due to this and other reasons the number of components is exceptionally large, about 2 - 3 times more than in other PWR-plants. We have, for instance, about 14000 valves.

Atomenergoexport (USSR) have delivered the reactor, the turbines and the main processes. The instrumentation is mainly from Siemens AG of West-Germany. The computer system, the civil engineering, the electrical equipments and some auxiliary processes are from Finland. Imatran Voima Oy, the owner utility, has had a pretentious task in joining all these deliveries together to a well-working power station, working as architect engineer in close cooperation with the Soviet main supplier.

The many components brought forth the need for a large amount of information (circa 2000 analogical measurements, 4500 bi-signals, 4000 alarms). Only by using computer systems is it possible to handle such an amount of information in a reasonable way. The computer of Loviisa NPS gives us, for instance, the following information.

- alarms to the main control room in three priorities, of which the two first displayed on cathode ray tubes
- process diagram formats, graph formats or measurement value formats. For example: it is possible to call the process diagram format and check the status of the process after an alarm; does it support the alarm information or not. Fig. 1.
- measurement values on request
- reports: operation reports, plant status reports and process condition reports
- plant performance calculations, efficiency coefficient, burnup distribution of fuel, marginals etc.

All information can be received centralized on six display tubes and printers in the main control room. Enclosed is a hardware configuration of the computer system. Fig. 2.

3

Operational experience

The problem with the great amount of information was well-known to Imatran Voima already at the beginning of the planning. Some methods that we have used in order to identify essential information:

- there are three different categories of alarms, of which the most important ones are realized in a conventional way in parallel to the computer display
- many interlockings to prevent wrong information
- blinking alarm values in process diagram formats
- a continuous calculation of the plant performance and the data received about divergences give valuable information about the condition of both equipments and measurements, and thus facilitates the planning of necessary repairs in good time, and the plant can be operated almost at its maximum. A continuous calculation of the plant performance concerning for instance the following points is made at intervals of one hour: reactor power, efficiency, plant flow balances, mass balances and the condition of main components such as big pumps and heat exchangers.

The practical problems that have required attention during the operating phase include the following:

1. In the first priority there may be five "pages" of alarms, on each page 20 alarms in an emergency situation, and in the second priority 20 pages with 20 alarms on each, too. How to enable the finding of really important signals?
2. How could leakages in the containment be indentified easily? We have connected to the computer mass balances and flow rate measures of condensate from cooling ventilation system, but for one thing they are not accurate enough and, secondly, they may not be reliable.

3. On the control room panels it was earlier possible to see, for example, the positions of the valves: white closed, red open; but, red also indicated valve or pump disturbances. We could not see the deviations or if an important valve was in a wrong position.

Point 1 is the most important one in emergency situations and points 2 and 3 are valuable during normal operation and at minor disturbances.

Point 1: Against this large amount of information we have one plan; we need a separate emergency format in the display unit or, even better, a separate emergency panel. On this emergency panel we will have the important information from our processes and it can be seen clearly and independently from other information. See fig. 3.

During emergency situations the most important thing is to analyze how the core cooling is working, the tendencies of the critical parameters, and to decide how the situation can be improved. But it is rather difficult to analyze anything, if you do not soon enough distinguish the signals which tell you that something is wrong.

Point 2: For finding leakages in the reactor building we had earlier "on/off" alarms from the special sewerage pump in the third priority and they were recorded on a printer. Now we have put these alarms in the second priority and ordered the operators to write down in a separate logbook every pump start and to calculate the time intervals. Now it is possible to notice at once even very slowly growing leakages. I am quite sure that the best way of finding a leakage is to do it manually. When we know that there is a leakage, we can inspect the inaccessible rooms in the reactor building by means of mirrors and endoscopes. Endoscopes can be put into these rooms through special instrumentation penetrations.

Point 3: We decided to change the colours of some lamps. Now we have for example: green light meaning that "pump is running in normal situation", "valve is open normally", "automatics normally on", white light meaning "valve normally closed", "automatics normally off", "pump not running", and red light meaning "valve in abnormal position", "automatics off abnormally", "valve disturbance", "emergency pump is working". This shows that in some cases the red light can indicate that the valve is open or that it is closed and this can cause confusion. But the most significant thing is that when you see a red light you know that there is something wrong. This is the philosophy of the "green board".

Altogether the information system of Loviisa NPS has operated excellently, although we still have problems with the amount of information at large disturbances. Of course the future can bring even better systems; at emergency situations not all alarms would be displayed by the computer, but most of the alarms concerning especially the secondary circuit would be switched over to another information unit.

As a practical result from our information system of Loviisa human mistakes have played an insignificant role at our plant. The reasons for the non-availability at Loviisa NPS are as follows:

- 8 % power restriction	7,8 %
- annual maintenance	10,6 %
- other general maintenance	0,4 %
- technical defects	2,0 %
-pumps, valves	
-turbogenerators	
-instrumentation	
- stretch-out loss	0,3 %
- grid regulation	0,6 %
- guarantee tests, other tests	0,3 %
- tolerance to max. power and other human factors	0,3 %

4

Possibilities in the future for computer aided operation

With the introduction of powerful and inexpensive micro-computers new possibilities is emerging for computer support during abnormal situations in the plants. The colour displays are also enabling the development of advanced man machine dialogues. Taking however into account the extreme requirements for the reliability of the nuclear power plants it however seems more probable that these systems will be an addition to a conventional panel with the most important variables. Such a system could then be thought of as an instrument for computer aided operation.

In considering possibilities for computer aided operation the tasks of the operator should be identified. The tasks as required during an abnormal situation could be identified as /Ras 1976/.

- alert
- identify
- restore
- evaluate
- operate

The operator has to be alerted by some means that the operation of the plant has changed, then he should identify the cause and restore the normal operation. After that the operator should evaluate possible consequences and operate to eliminate the cause of the disturbance. A system for computer aided operation could in principle be designed to assist the operator during all these phases.

For the alerting of the operator that the plant has entered some abnormal state alarming systems have been designed. Especially important are the existence of different prewarning signals to alert the operator in time for a remedy to be found. The main difficulty with the alarming systems used today is that alarms are active during normal operating regimes which means that important alarms could be masked by abundant "cry wolf" alarms. With the introduction of computers it would be possible to use more efficient alarm filtering to make an active alarm to indicate an abnormal situation. Innovation in the presentation of

alarms could also be done with the use of videodisplays.

Aids for identifying the cause for an alert signal could be built around systems for hypothesis generation and hypothesis testing. Different methods from advanced pattern recognition to straight-forward searches through cause consequence diagrams have been proposed.

To help the operator in choosing the correct sequence of actions different checklists and operational instructions have been generated. To ease the use of such checklists and instructions they could be integrated in a man computer dialogue. One advantage of such a system is that it would be possible to integrate also the plant design data in the main data base.

Consequences of actions should be carefully evaluated before applied because the different systems of nuclear power plant is heavily interconnected and actions could therefore introduce unwanted side-effects. One possibility is to use fast models to simulate responses to proposed actions to facilitate a correct prediction of the plant response. The simulation models could be based either on continuous variable simulation or cause consequence diagrams for presenting possible scenarios to the operator.

The operation could be eased by using the computer to cue different actions to be initiated by the operator. The computer could also be programmed to perform an alarm bell function for the operators.

In considering the type of plant disturbances which should be the target for the development of computer aided operation it is quite clear that they coincide with the situations where the operator has an active role. This means that the large single accidents of the LOCA type will not be the main target for the systems because they will be taken care of by automatic systems. On the other hand it seems clear that smaller disturbances where the automatic system will not function but which could develop into larger disturbances if no measures are taken.

One of the most important questions to be considered is however connected to the problem of data reduction. How should the information in the control room be processed and displayed to easily grasped and used for the operation according to the defined goals.

5

Conclusions

A lot of new possibilities are emerging with the introduction of new equipment. A lot of the benefit available with such systems could however be obtained also with more conventional systems if they only are properly designed.

There is a clear benefit in using the colour displays because of the possibilities of having a very compact system where the information is presented only when called. For the most important information on the state of the plant a separate panel is however needed.

/Ras 1976/ J. Rasmussen: Outlined of hybrid model of the process plant operator, in T. B. Sheridan, G. Johannesen (ed): Monitoring behaviour and supervisory control, Plenum press (1976)

/Ras 1979/ J. Rasmussen: Personal communication

PÄÄLAUHE
MAIN CONDENSATE

PÄÄEJEKT ULOSPUH AKT X.X-X CI/M3

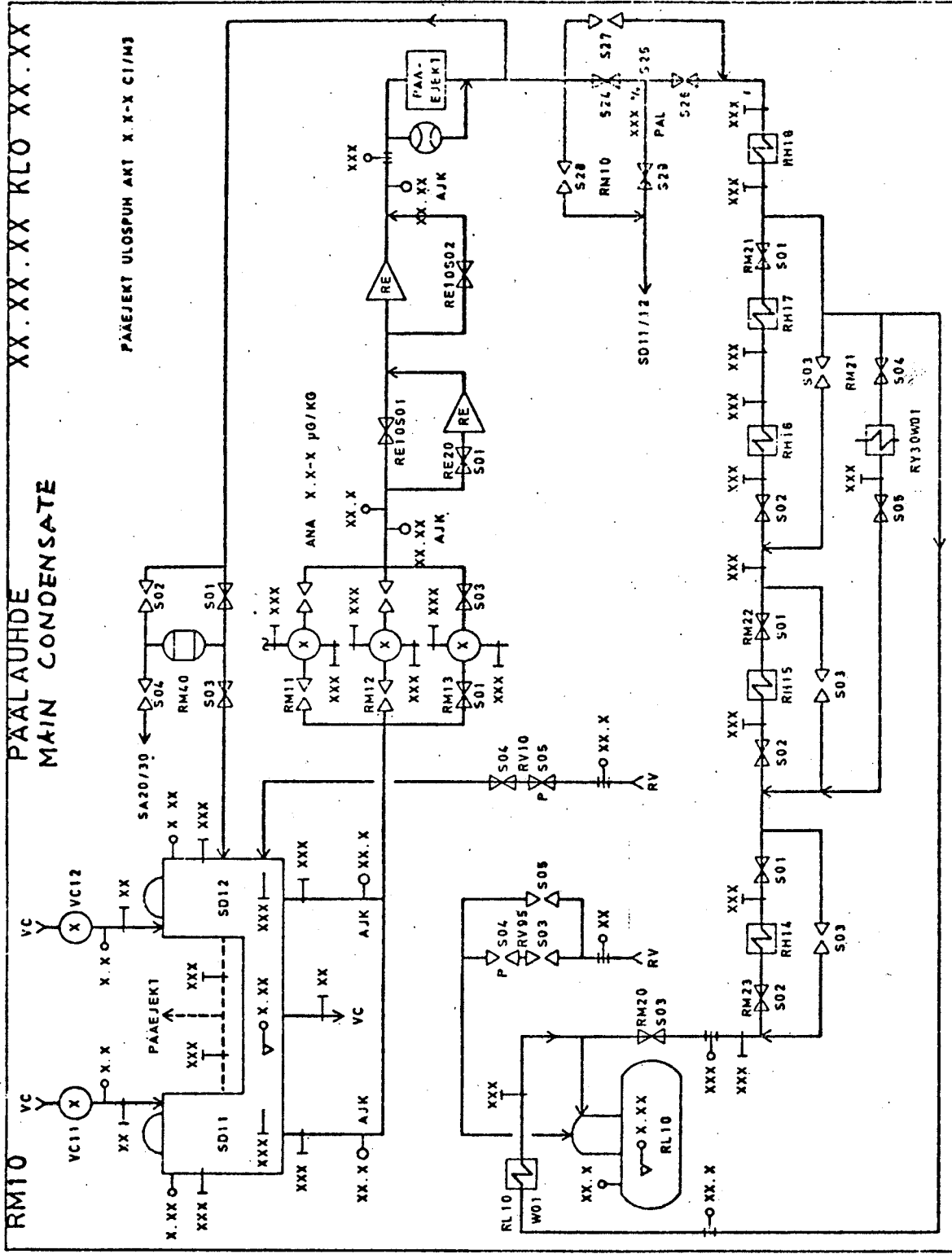


FIG 1.

IMATRAN VOIMA OSAKEYHTIO	
LOVIISAN VOIMALAITOS 2	
Formaatti	
Pöytäkuide	3
A 2 LO2 688 017 A	

Multiprocessor Two-Unit VVER-440 Nuclear Power Plant Monitoring System

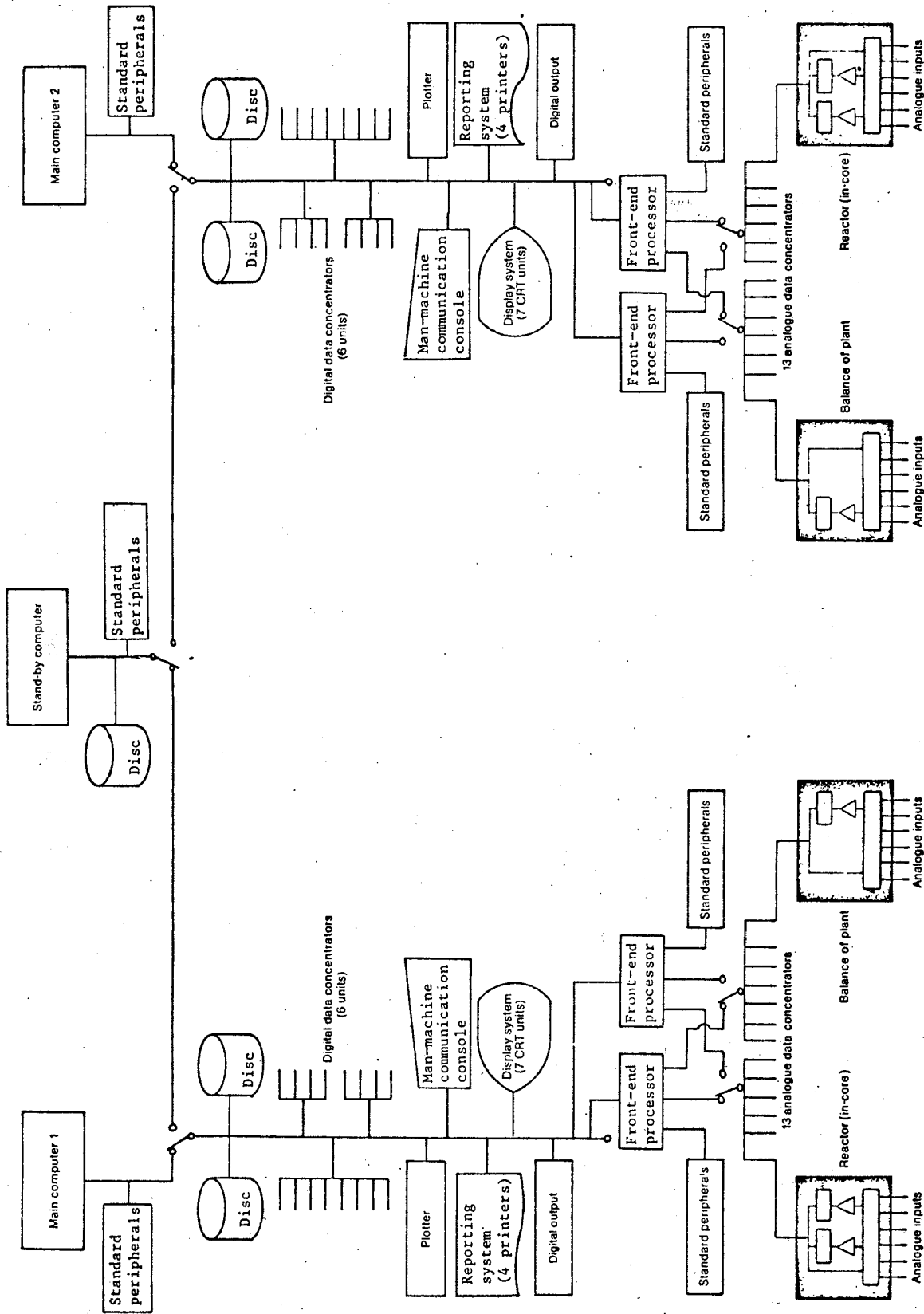


Fig 2.

EMERGENCY FORMAT

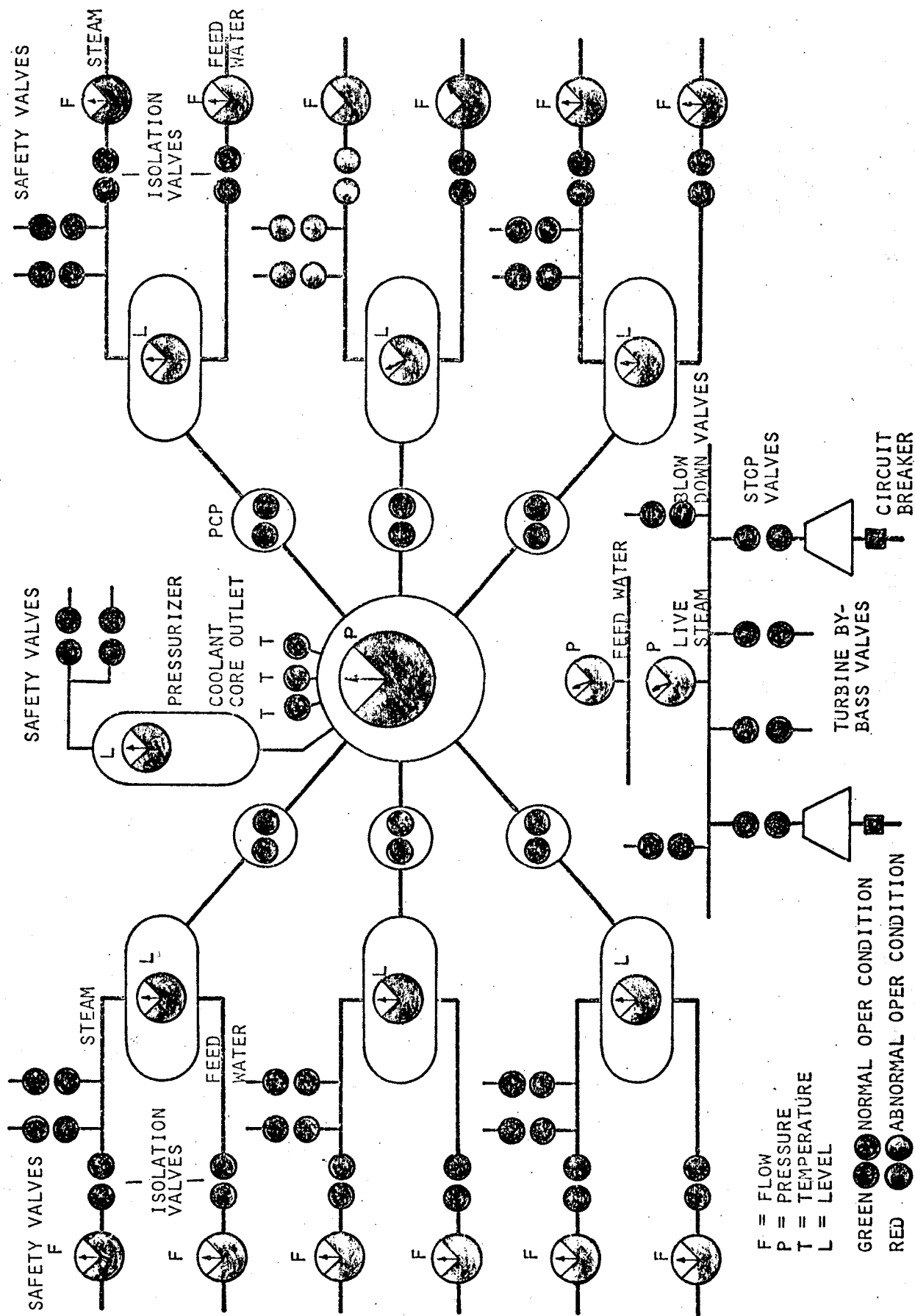


FIG 3.

K.P. Ojha

AUGMENTING OPERATOR GUIDE FOR ROUTINE AND EMERGENCY OPERATIONS

AUGMENTING OPERATOR GUIDE FOR ROUTINE
AND EMERGENCY OPERATIONS

K.P. Ojha - Control Maintenance Engineer,
Rajasthan Atomic Power Station,
Kota, India.

ABSTRACT:

Plant parameters are exhibited in Control Room to guide operator in taking operational decisions. It is necessary that these exhibits be in accordance with the operational procedure and steps. To minimise time required for analysing the information and also to reduce the need of verbal communications.

The paper reviews the parameters displayed and their layout at Rajasthan Atomic Power Station. Additional displays provided and more under consideration are described.

A transmitter power supply failure alarm unit has been installed to identify abnormal indications due to loss of power supply to a transmitter, so that approach for rectification is easy. Additional displays such as steam flow discharge rate, rate of change of heat transport pressure etc. are under consideration. Absence of primary heat transport flow indication has been felt to be a great handicap.

During a disturbance, it is necessary that the operator is able to identify the cause from the effects. Normal recorders having chart speed of one inch per hour are unable to assist the operator in analysis of the disturbance, when very fast transients in many parameters occur. Feasibility of increasing the speed of the recorders, during a transient, is being investigated. A disturbance analyser, with twenty analog inputs has been installed, to print out pre-incident and post-incident values of important parameters.

Introduction of a separate analyser for electrical systems, is also being considered. Existing contact input event sequence recording annunciator has been extended to include more inputs. In many redundant and coincident logics partial failure was not evident until a completed trip took place. Indicating lights were installed to indicate partial/single channel failures. Ready to start light for important standby equipment were also installed.

1.0. INTRODUCTION:

Reliable, accurate and comprehensive display of status of nuclear power plant parameters is very important for taking operational decisions, during normal and abnormal conditions. Since the number of parameters tend to be large, it is important to ensure careful selection and location of displays, so that priorities are clear and operation is convenient. Some of the operational requirements are not envisaged during design and construction. Therefore, displays and controls are under constant review to implement modifications and incorporate operational requirement, which become evident as operational experience builds up. The paper describes reviews carried out and changes implemented at Rajasthan Atomic Power Station, Kota, India.

2.0. LAYOUT OF DISPLAYS ON CONTROL PANELS:

2.1. General considerations in layout and parameters chosen for displays are as follows:

- i) Displays should be such that operational steps are evident. Alarm descriptions and indications should be a pointer to action to be taken by the operator.
- ii) The displays should be near operational point (handswitch, knob etc.). In some cases a strategic display for a plant subsystem is important to be watched while operating hand switches etc. of another subsystem. In such cases, display may have to be duplicated so that it is visible to the operator while he is operating.
- iii) Alarm priorities should be clear. Alarm windows may be colour coded, so that in case of simultaneous alarms, operator's attention is drawn to one with higher priority first.
- iv) Display of parameters and alarms not required during operation should either be deleted or recorders, printers for such parameters should be located in a separate room, not in Control Room.

2.2. Generally panels are divided into subsections, as per systems and subsystems of the plant. Control room display in Rajasthan Atomic Power Station, is distributed on six panels, each panel divided into subsystems as follows:

- i) Electrical generation and output system, station supplies, boiler steam and feed water systems.

- ii) Primary heat transport, moderator and reactivity systems.
- iii) Reactor power control and protection.
- iv) Fuel handling systems.
- v) Auxiliaries systems.
- vi) Heavy water leak detection systems.

However, certain indications/displays of parameters of a system, which are vital for operation of another system, are displayed on the relevant panel, in addition to or instead of displays on the panel for the system. For example, delayed neutron signal to indicate failed fuel (auxiliary system) is also displayed on fuel handling control panel. Additional displays were provided, as described in subsequent sections, to fulfil more such requirements. Alarm windows were colour coded and certain alarm windows not found necessary, were deleted.

3.0. ADDITIONAL DISPLAYS AND ALARMS:

3.1. TRANSMITTER POWER SUPPLY FAILURE ALARM:

Various transmitters for process system parameters are powered by 65 volt D.C. power supplies. Sometimes, the indication went down due to drop in this voltage caused by deterioration, of components or complete failure due to blowing of fuse. To distinguish such failures from those of transmitters and also from genuine drop in signals, a transmitter power supply alarm unit was installed. The voltage at output of each power supply unit is monitored and a common alarm is annunciated in control room to draw operator's attention. Indication on local panel identifies the faulty power supply. Thus, considerable time is saved and fault can be rectified quickly.

3.2. OTHER POWER SUPPLIES:

Other power supplies used are 48 volt D.C. for relay logic systems and 118 volt A.C. for instruments. Fusing system for both types of power supplies were reviewed and rearranged so that generation outage is avoided when a single fuse fails. Fuse failure for 48 volts D.C. is annunciated in control room. Need has been felt for similar annunciation for 118 volt A.C. also, so that failure of power supply to an instrument is easily identified by the operator and quick action can be taken. Feasibility for providing such alarm for important instruments is being studied.

3.3 ADDITIONAL LIGHT INDICATIONS:

Light indications were installed to indicate "Ready to Start" condition of standby pumps, such as boiler feed pumps. Light indications are also being considered for position of relief valves of primary coolant and steam systems. In some coincidence logic circuits, single instrument failure was not evident till a completed trip took place. Single failure indication lights were installed in such cases. For example, reactor is tripped when level in three out of four boilers on one side of the reactor is low. However, there was no indication to the operator when one or two of the level switches have failed to be in condition of low level even though actual level is not low. Light indications now installed for each level switch are very useful.

3.4 LOAD LIMIT INDICATOR AND ALARM:

The turbine load is limited by a relief type of limiter for governed oil pressure. The setting of the limiter is indicated in control room, But this indicator was originally calibrated in terms of percent of electrical power. Therefore, accuracy of the indication was subjected to drift in calibration of governor valve and such other parameters affecting relationship between governed oil pressure and power. Also precise calibration of the indicator was not practicable as it needed variation of load, while connected to grid. The load limit indicator was therefore, calibrated in terms of governed oil pressure and an indicator for governed oil pressure was installed by its side to facilitate easy comparison and off load calibration. This has been found very useful.

An alarm was also installed to annunciate when governed oil pressure is not rising because of load limiter action, when speeder is being driven up and reaches its limit. A continuous indication of speeder position would be very useful to the operator.

3.5 INDICATION OF GROSS FLOW OF PRIMARY HEAT TRANSPORT (PHT):

At present primary heat transport (Reactor coolant) flow is monitored only for few selected channels of the reactor and gross flow is not indicated. Indication of PHT gross flow would be very useful to the operator in assessing situation during transients and for accurate calculation of thermal power of the reactor during steady operation. A conventional flow measuring device cannot be installed because of absence of sufficient length of pipe. Effort was made to monitor the flow by measuring differential pressure developed across PHT circulating pumps. Another device now under consideration is using spectrum of energy emissions from PHT, due to nuclides present in the system. The spectrum will be monitored at two fixed places in the flow path of PHT, separated by a known distance. The time interval of appearance of identical perturbation and distance between the two monitoring points will give an indication for velocity of the fluid from which flow can be calculated.

3.6. RATE OF CHANGE OF HEAT TRANSPORT PRESSURE:

Reactor trip due to PHT pressure exceeding low limit has been most frequent among the reasons for outages. Most of these outages were not really warranted, because there was no loss of coolant, against which this trip provides the protection. A PHT pressure rate instrument was installed to investigate if "low pressure" trip can be replaced by "high rate of falling pressure" for some conditions, to reduce the unwarranted trips and maintain the reliability of warranted trips. While this does not appear to be advantageous, the parameter is very helpful to operator as a guide while unloading/loading the turbine and raising/lowering of reactor power, to avoid reactor trip due to PHT pressure high, as well as PHT pressure low. It is proposed to install indicators for this parameter on turbine as well as reactor power control panels. It would be a better guide for the operator to assess how turbine loading/unloading rates and raising/lowering of reactor power contribute to the changes in PHT pressure.

4.0. NARROW DOWN AREA REQUIRING OPERATORS ATTENTION:

It is necessary that during a disturbance in some systems of the unit, other equipment and system parameters be left as close to normal operating condition as possible so that operators attention can be concentrated on the disturbed area. Disturbances considered here are reactor trip, turbine unloading or trip and boiler feed pump trip.

4.1. REACTOR TRIP:

A trip reset scheme is being considered to minimise changes in reactor process system. At present moderator is dumped out of reactor core during a trip. Feasibility of keeping moderator level as high as safely possible, is being considered

Steam to turbine is stopped in five seconds after the reactor trip, so that steam pressure can be conserved to maintain the vacuum and other services. Feasibility of motoring the turbogenerator also is being studied, to reduce time for turbogenerator run up and synchronisation, so that loading can be started as soon as reactor power can be raised.

4.2. TURBINE TRIP:

When turbine trips or gets unloaded, steam produced in reactor is discharged to atmosphere as a heat sink for reactor to ensure minimum disturbance in nuclear systems. Reactor power is reduced automatically at a fixed rate of 1/2 per cent of full power per second (reactor set back). An override feature was introduced to arrest this reduction of power if sufficient feed water at required temperature is available or the

reactor boiler. Display of feed water temperature and rejected steam flow rate, by way of position of steam discharge control valves, is being considered to be located on reactor power control panel, to enable operator to operate in this mode in a safe and optimum manner.

Steps are also being considered to increase pressure of steam drawn from boiler to feed water deaerator heater, so that feed water temperature can be maintained within acceptable limit even in absence of extraction steam from turbine used in feed water heaters. An indicator for boiler feed water temperature, to be installed on reactor control panel is also being considered.

4.3. BOILER FEED PUMP (BFP) TRIP:

When a running boiler feed pump trips and there is a delay in automatic starting of standby feed pump due to any reason, pressure of primary heat transport system goes up, due to loss of cooling in preheat leg of the boiler even though sufficient water is available in boiler drum. This increase in pressure of the primary heat transport system causes reactor trip. Fast power reduction of reactor (Reactor Set Back) is being considered so that cooling due to reduction in power compensates for loss of cooling in preheat leg of the boiler and reactor trip is avoided. Thus operator can concentrate his attention on restart of boiler feed pumps. Even if generation outage becomes eminent, reactor can be kept operating at low power by small BFP, steam pressure and condenser vacuum can be maintained, thus narrowing down the area of work for the operator and helping quick restart.

5.0. DISTURBANCE ANALYSIS:

It is very important that during a disturbance the operator is able to identify the cause from the effect. Modifications/additions done to augment information to the operator so that he is in a better position to identify the cause from the effect, are described in the following paragraphs.

5.1. RECORDING ANNUNCIATOR:

Original recording annunciator prints out sequence of events during a disturbance with time when each event took place. It has been of great help, and has been extended to include more inputs. In addition to this contact input device, need was felt for analog values for various important parameters, during a disturbance. This need was met by additional disturbance recorder.

5.2. DISTURBANCE RECORDER:

A microprocessor based disturbance recorder has been

installed to print out process parameter values during a disturbance. Since this data is helpful in analysis of the incident and the information is not required for operations during the disturbance, this equipment has been located in control equipment room.

The analyser scans 20 analog voltage inputs. The inputs are sampled every second, the voltage values are converted into actual engineering units and stored in the predisturbance memory. This predisturbance memory has sufficient capacity to store data collected for a period of five minutes. The scanning and storage of data is continuous. When the predisturbance memory is full, space is created for the fresh values, by dropping the oldest values. Thus, at any instant, the predisturbance memory contains the data for the last five minutes. Contact inputs indicating disturbance have been wired to trigger the analyser. The triggering can also be done by the operator. When triggered, the predisturbance memory is frozen and system enters the after scan mode. Now the values are stored in the post-disturbance memory. Post-disturbance data is also sampled every second and continues for 5 minutes. Then the system enters in the output mode. The data stored in the memory for a period of ten minutes are printed out on the console printer. After all the values are printed out the system automatically returns to predisturbance mode. If printer is not ready due to inadequate paper or any such reason, the printer ready switch can be put in "not ready" position and printing is suspended without any loss of data. Printing is resumed, when printer is ready.

A separate disturbance analyser has been proposed for electrical systems.

5.3. CONVENTIONAL RECORDERS:

Chart speed of conventional recorders is one inch per hour. Therefore, their utility is limited as sequence of fast changing parameters cannot be identified. Important parameters were connected to a fast speed, narrow range recorder. The operator can select a parameter for recording on this recorder to get trend of the parameter more precisely. Feasibility study is on hand to increase the speed of all conventional recorders, during a disturbance.

6.0. DATA HANDLING SYSTEMS:

Suitable data acquisition and processing systems help operator in getting quick, concurrent and comprehensive information about the status of nuclear power plant, which is very important for taking operational decisions during normal as well as abnormal operating situations. Originally a data logger was provided to print out process parameter data and alarm. However additional data handling and computer systems were added later for channel activity monitoring system and channel temperature monitoring system.

Because of the large amount of data involved, collection and processing of data for each channel of reactor was very time consuming. Installation of data handling and computation systems has been a great advantage to the operator.

6.1. FAILED FUEL DATA SYSTEM:

The system is meant for detecting failed fuel by monitoring the delayed neutron activity level due to fission products in the reactor coolant. The system takes pulse inputs from Boron Trifluoride (BF₃) detectors, and gives output printed on a paper tape either on demand by operator or under alarm conditions. The output of the BF₃ detectors are connected to the input of count rate meter (CRM) units which give output in terms of DC voltages proportional to the rate of input pulses. These voltages are fed to DATA acquisition (DA) unit and Data Display (DD) unit. The DA unit goes on scanning the input voltages sequentially. The output voltage of channel under scan is also compared with limits, preset for high and low alarms. If the voltage is found to cross the set limits, corresponding alarm lamp comes ON and printing cycle is initiated.

6.2. CHANNEL TEMPERATURE MONITORING COMPUTER:

The computer takes voltage input from resistance temperature detector network for 306 channels of the reactor. Output printers give complete data, trend for selected channels and average temperatures. Important process parameters are also connected for computation of reactor power, individual channel power and such other information as may be required by the operator.

7.0. UPKEEP OF INSTRUMENTS:

It is very important that reliability of displays and handswitches, knobs etc. be maintained very high for proper guidance of operator and execution of operational steps. The instruments must be kept in dust free and air conditioned atmosphere. This needs special effort in tropical countries like India.

Climatic control and preventive maintenance of the instruments must be started right when the instruments are received from the vendors and be maintained through preinstallation storage and installation periods.

8.0. CONCLUSION:

Modifications and additional displays and controls provided at Rajasthan Atomic Power Station have been very helpful to the operator. It has helped improve the availability of the unit and reliability of the safety systems. Built in spares in panel space, cabling and wiring were very helpful in effecting these modifications and additions. While designing control and display panels of a nuclear power station, sufficient spare space, wiring, cabling should be provided to facilitate such improvements, as operational experience builds up.

K. Kaneto, S. Ohteru, H. Natori

DEMONSTRATION AND VERIFICATION OF ON-LINE CORE EVALUATION SYSTEM
IN THE STARTUP TEST OF HEAVY WATER REACTOR FUGEN

Demonstration and Verification of On- line
Core Evaluation System in the Startup Test of
Heavy Water Reactor, FUGEN

KUNIKAZU KANETO

Hitachi Works, Hitachi Ltd.
Hitachi, Ibaraki, Japan

SHIGERU OHTERU

FUGEN Nuclear Power Station,
Power Reactor and Nuclear Fuel Development
Corporation
Tsuruga, Fukui, Japan

HISAHIDE NATORI

Energy Research Laboratory, Hitachi Ltd.
Hitachi, Ibaraki, Japan

1. Introduction

An on-line core performance evaluation system is an important component of power reactor plant recently. It brings safe and efficient reactor operation by supplying the detailed and useful information inside core immediately, such as the power distribution, thermal operation limits and so on.

ATROPOS is the system developed for the 165 MWe FUGEN nuclear power plant, which is a heavy-water moderated boiling-light-water cooled pressure tube type reactor, and developed by the Power Reactor and Nuclear Fuel Development Corporation(PNC), Japan. The startup test of FUGEN was performed on schedule during about a year from March, 1978, and the commercial operation license of the plant was given by the government on March, 1979. The usefulness of ATROPOS was also demonstrated through the same period, and its validity was verified by the data of reactor physics measurements.

2. The outline of FUGEN core configuration

The core consists of the following components.

- (1) Fuel assemblies ;
 - (i) 96 mixed oxide fuels (0.66 w/o Pu fissile + natural U) being loaded in the center region of the core.
 - (ii) 124 slightly enriched uranium oxide fuels (1.5 w/o U²³⁵) being loaded outside of the mixed oxide fuels.
 - (iii) 4 special test fuels (1.8 w/o U²³⁵) being located in the highest fast flux region.

By loading the mixed oxide fuels, the coolant void reactivity coefficients are kept in the vicinity of zero. The special test fuels are intended to supply the test specimens exposed with higher fast neutrons than the pressure tubes. These specimens will be tested periodically to estimate the ductility loss of pressure tube materials.

- (2) Control rods ;

There are 49 control rods and four of them are regulating rods driven automatically according to the regional power signal. All control rods are inserted from top of the core and their axial positions can be controlled continuously.

- (3) In-core neutron monitors ;
 - (i) 4 start-up monitors (SUM)
 - (ii) 6 power-up monitors (PUM)
 - (iii) 64 local power monitors (LPM) being located at 4 axial positions in 16

radial strings.

- (iv) 2 power calibration monitors (PCM) being traversed inside the LPM strings.

LPMs are used for estimating the power distribution, and they are calibrated by PCMs, twice a month, usually.

(4) Liquid poison

Boric acid poison is dissolved in the heavy water moderator and utilized to compensate for burnup reactivity loss. By regulating the concentration of boron-10, power can be raised within the restricted rates.

The core configuration of FUGEN is shown in Fig. 1.

3. The main characteristics of ATROPOS

There are two main distinctive methods for estimating the power distribution, in general. One is characterized by direct use of in-core neutron monitors readings, the other is done by simulator with no use of monitors. Their main features can be said as follows,

(1) Monitor base method ;

The time required for estimation is shorter, but it is almost impossible to furnish a system with predictive functions. The more accurate estimation needs the more monitors and the failure of them affects the results seriously.

(2) Simulator base method ;

A system can be furnished with predictive functions. The time for estimation depends on the simulator adopted, the more detailed simulator takes the longer time. Generally, it is difficult to select a suitable simulator.

In ATROPOS, aiming to take up the above merits, it makes use of both simulator and monitors. As a simulator, one-group coarse-mesh neutron balancing program like FLARE was selected. In heavy water reactor, the local power depression caused by control rods is relatively small because of longer migration area, therefore a simple simulator like this can be expected to give a fairly good estimation results. The predictive functions included in ATROPOS are summarized with other functions in Table 1. All these functions can be requested any time by operators.

The computer system is composed of 48 K-words CPU, 768 K-words magnetic drum, a line printer, a cathod ray tube, 4 type-writers and a magnetic tape deck. It takes about 6 minutes to get new evaluation results.

4. Evaluation methods of main functions

(1) Procedures of estimating the power distribution

The 3-dimensional power distribution and thermal operation limits are evaluated according to the following procedures.

- (a) Calculate the 3D power distribution by simulator
- (b) Estimate neutron flux at LPMS points from the results of (a)
- (c) Take the differences of neutron flux between the estimated and the actual values.
- (d) Interpolate them radially to the locations where there are no LPMS. (pseudo-strings)
- (e) Fit them axially with 5 th order polynominal at each actual and pseudo-string.
- (f) Redistribute them to the power of each segment of the surrounded fuel assemblies.
- (g) Calculate the coolant flow rate of each fuel channel by making use of the correlations between channel powers and flow rates.
- (h) Estimate thermal operation limits (maximum linear heat generation rate, MLHGR and minimum critical heat flux ratio, MCHFR)

In the above procedures, thermal-hydraulic treatments are based on the full-scale mock-up experiments, for example ;

- (i) The design formulas of pressure drops in fuel channels were verified by the data obtained at Component and Instrument Test Laboratory (CTL) of PNC, and the correlations between power and flow rate were given to representative channels through the detailed thermal-hydraulic program using the above formulas.
- (ii) The burn-out heat flux of fuel cladding was formulated as a function of bundle average steam quality by adjusting the data obtained at Heat Transfer Test Loop (HTL) of PNC.

The contents of power correction steps are summarized in Fig.2.

(2) Prediction methods

The object of predictive functions is to make reactor operators enable to get anticipated grasp and judgment of the core conditions after the maneuvering of control equipments. In view of quick response, some simplified models have been developed for them.

(i) Core thermal power prediction

Core thermal power is predicted by critical search calculation using an axial one-dimensional model. This model has been derived from the horizontal integration of the parameters such as transport kernels, infinite multiplication factors and neutron sources, as follows,

$$\frac{\lambda S_k}{K_{\infty k}} = W_{k+1}^V S_{k+1} + W_{k-1}^V S_{k-1} + W_k^S S_k$$

where

$$S_k \equiv \sum_{ij} S_{ijk} \quad , \quad K_{\infty k} \equiv \sum_{ij} S_{ijk} / \sum_{ij} \frac{S_{ijk}}{K_{\infty ij k}}$$

$$W_k^{V,H} \equiv \sum_{ij} W_{ijk}^{V,H} \cdot S_{ijk} / \sum_{ij} S_{ijk}$$

$$W_k^S \equiv 1 - 2W_k^V + \alpha_k^H W_k^H + \alpha_k^V \cdot W_k^V$$

- λ ; effective multiplication factor
- S_{ijk} ; neutron source of segment (i,j,k)
- $K_{\infty ij k}$; infinite multiplication factor
- W_{ijk}^S ; self-absorption probability
- $W_{ijk}^{V,H}$; vertical or horizontal transport kernel
- $\alpha_k^{V,H}$; vertical or horizontal albedo at integrated segment k

In the above homogenizing process, the horizontal albedo is adjusted to give the same eigenvalue as 3D model.

(ii) The power distribution prediction

Two different methods are installed in the system. The first is used for monitoring the thermal operation limits around the specified control rod and the second is for the overall power distribution in core.

In the first method, assuming that the range of the perturbation of power distribution due to control rod movement is limited in the small region, the power distribution is solved in the local region (6x6 fuel assemblies) around the specified control rod with the boundary conditions unperturbed.

In the second method, the whole core calculation is performed by the simulator but the change of the coolant void distribution is neglected in the calculation because of its small reactivity.

5. Verification results

(1) Estimation error of the current status in-core.

(i) The power distribution

The accuracy of the estimation was evaluated by the differences between the actual PCM readings and the estimated values from the corrected power distribution, this comparison was done at each power level 15, 25, 35, 50, 75, 100% rated power, which average fuel exposure was about 50, 100, 150, 250, 450 and 1300 MWD/T, respectively. The root mean square of the differences at 240 points (15 strings x 16 axial nodes) was less than 3% at any power levels. Examples of the comparisons are shown in Fig. 3.

(ii) The channel flow distribution

The flow rates of 18 fuel channels obtained by ATROPOS were compared

with the measurements which were converted from the differential pressures measured at their feeder pipings. The locations where the gauges are installed are shown in Fig. 4, and the estimation errors are summarized in Fig.5. The discrepancies are small and it seems that they are within the experimental errors.

(iii) The thermal operation limits

Their uncertainties at rated power were evaluated to be about 6% from the sensitivity coefficients and the standard deviations of the independent variables such as thermal hydraulic data, input constants and so on. The relative power is also treated as an independent variable in the evaluation because of the small coolant void reactivity. The error of the correlations between channel power and flow rate is also included as a component. The deviations used in the evaluation are 3% for power and 5% for flow rate.

(2) Prediction error

The changes of core status by maneuvering the regulating rod were measured and compared with the predictions by ATROPOS.

(i) Core thermal power

The change of the power was measured by means of Total Power Monitor which indicated the average value of all LPM readings. The measurement was done within a few minutes to exclude the influence of xenon transient. The discrepancies between the measurements and the predictions are quite small as shown in Fig. 6. The prediction depends on the doppler reactivity coefficient to be used, because the power coefficient of FUGEN is almost equal to it.

(ii) Thermal operation limits around the specified rod

The actual values to be compared with the predictions were evaluated by ATROPOS using LPM readings after the control rod insertion. The prediction errors were less than 4% for the three different power levels. The axial power distribution of the fuel assembly neighbouring the specified rod is plotted in Fig. 7.

(iii) The whole core power distribution

The actual values were obtained by the same way as the above. The prediction errors excluding core peripheral segments were about 6% and slightly large in comparison with the above. This is caused by the present model that LPM readings are not used for the prediction. An improved method is now under consideration which can include the monitor readings in the prediction.

6. Conclusions

Validity of FUGEN on-line core performance evaluation system, ATROPOS, was verified through the startup test. The main verification results are as follows ;

- (1) The estimation error of the power distribution was less than 3% at any power levels.
- (2) The differences were about 4% between channel flow rate converted from the measured pressure drop and that estimated by ATROPOS.
- (3) The uncertainties of the thermal operation limits were evaluated to be about 6%.
- (4) The core thermal power can be predicted accurately and the prediction depends on the Doppler reactivity coefficient to be used.
- (5) The prediction errors of the thermal operation limits were less than 4% within the specified region.
- (6) The whole core power distribution was predicted with about 6% error excluding core peripheral segments.

7. Acknowledgment

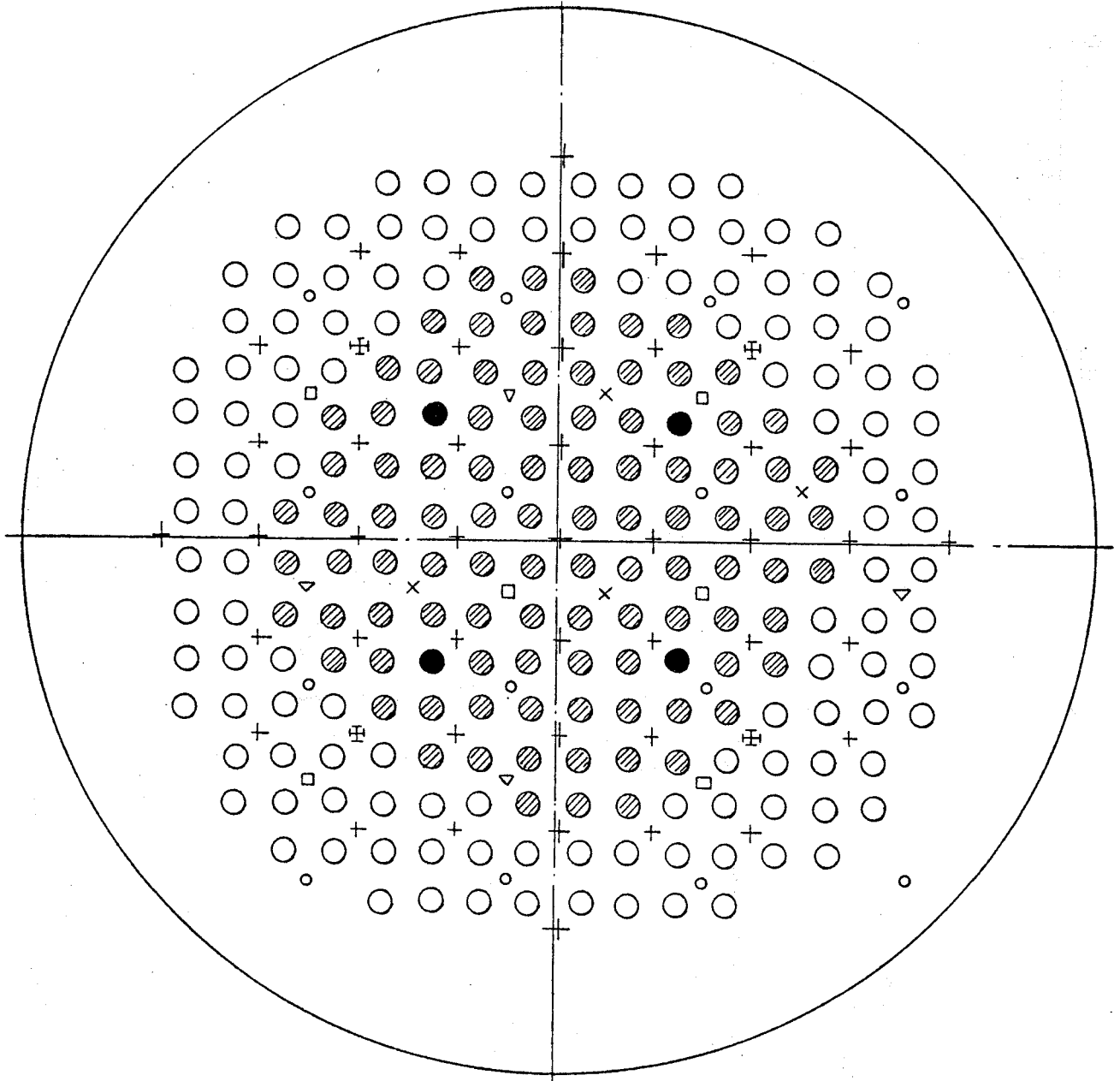
The work presented in this paper was based on the efforts of many people of the Power Reactor and Nuclear Fuel Development Corporation. In particular, we express our gratitude to T. Yamaho and T. Furubayashi for their support to this work.

8. References

- (1) S. Sawai, M. Akebi, et al ; FUGEN HWR reaches commercial operation; Nuclear Engineering International P.33 August 1979.
- (2) S. Sawai, M. Akebi and A. Yazaki ; Power up of FUGEN reactor and development of demonstration plant ; The 19-th CNA Conference, Toronto Canada, June 1979.
- (3) D. L. Delp, et al ; FLARE a three dimensional boiling water reactor simulator ; GEAP-4598, 1964.

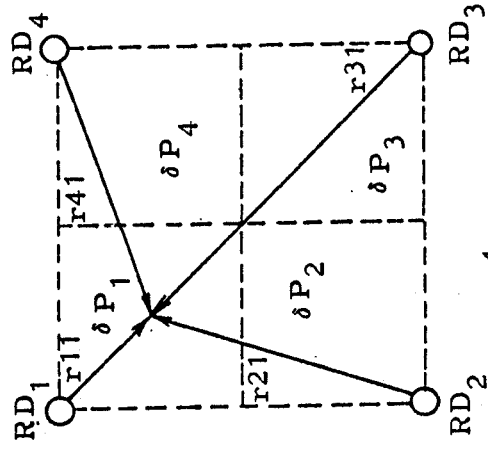
Table 1 Available Functions in ATROPOS

Function	Contents
Prediction	<ul style="list-style-type: none"> ○ Core thermal power after control rod or liquid poison operation ○ Power distribution after control rod operation ○ Liquid poison quantity to be regulated for compensating reactivity for burn-up loss ○ Shut down margin with one stuck rod
Estimation of Present Core Status	<ul style="list-style-type: none"> ○ Thermal operation limits around the specified control rod ○ The whole core thermal operation limits ○ Fast neutron fluences at pressure tube
Data Edit	<ul style="list-style-type: none"> ○ LPM readings ○ Control rods positions ○ Detailed thermal data in the specified fuel assembly ○ Specified data array
Edit and Storage of Fuel Assembly Data	<ul style="list-style-type: none"> ○ Storage data for fuel management ○ Exposures, isotopic compositions of loaded fuel assemblies
Maintenance of ATROPOS	<ul style="list-style-type: none"> ○ Revision of the library data for core performance evaluation ○ Data adjustment at refuelling ○ Security data in magnetic tape for the break down of drum



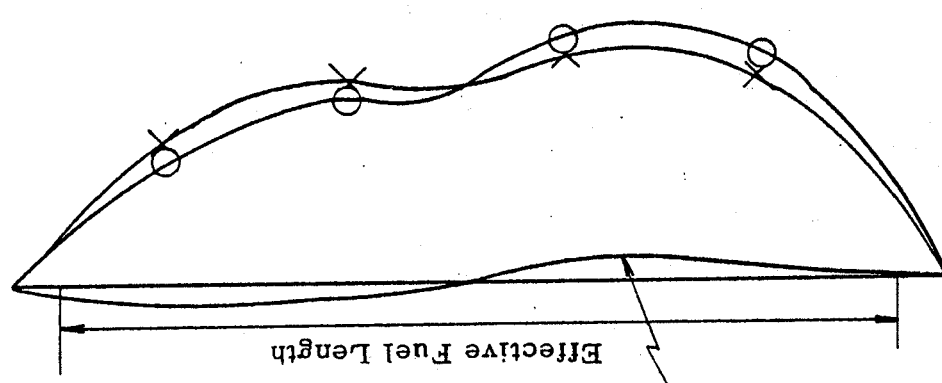
○	Oxide fuel (UO_2)	124	○	Local power monitor	16×4
◐	Mixed oxide fuel (PuO_2+UO_2)	96	□	Power-up monitor	6
●	Special fuel	4	▽	Start-up monitor	4
+	Control rod	45			
⊕	Regulating rod	4			

Fig. 1 Core Configuration of FUGEN



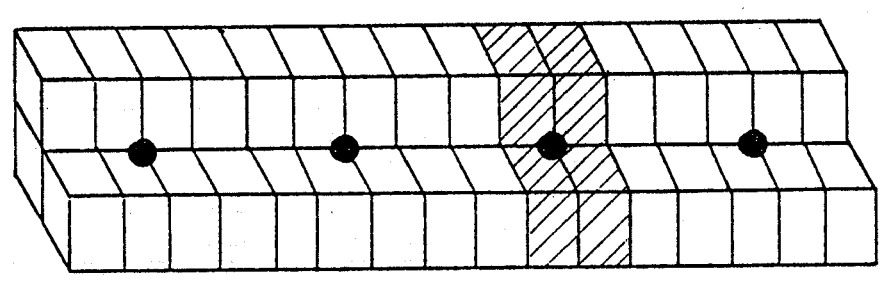
$$\delta P_j = \sum_{i=1}^4 W_{ij} RD_i$$

$$W_{ij} \propto \frac{1}{r_{ij}^2}$$



- Actual Reading (RA)
- × Estimated Reading (RE)

Axial distribution of RD (=RA-RE)



● LPM

Fuel Segment

$$RE = \sum a_{ijk} P_{ijk}$$

Estimate of LPM Reading RE
(Step b)

Axial fitting of the difference RD
(Step e)

Distribute RD to Segment Power
(Step f)

Fig. 2. Power Correction Method by LPM Reading

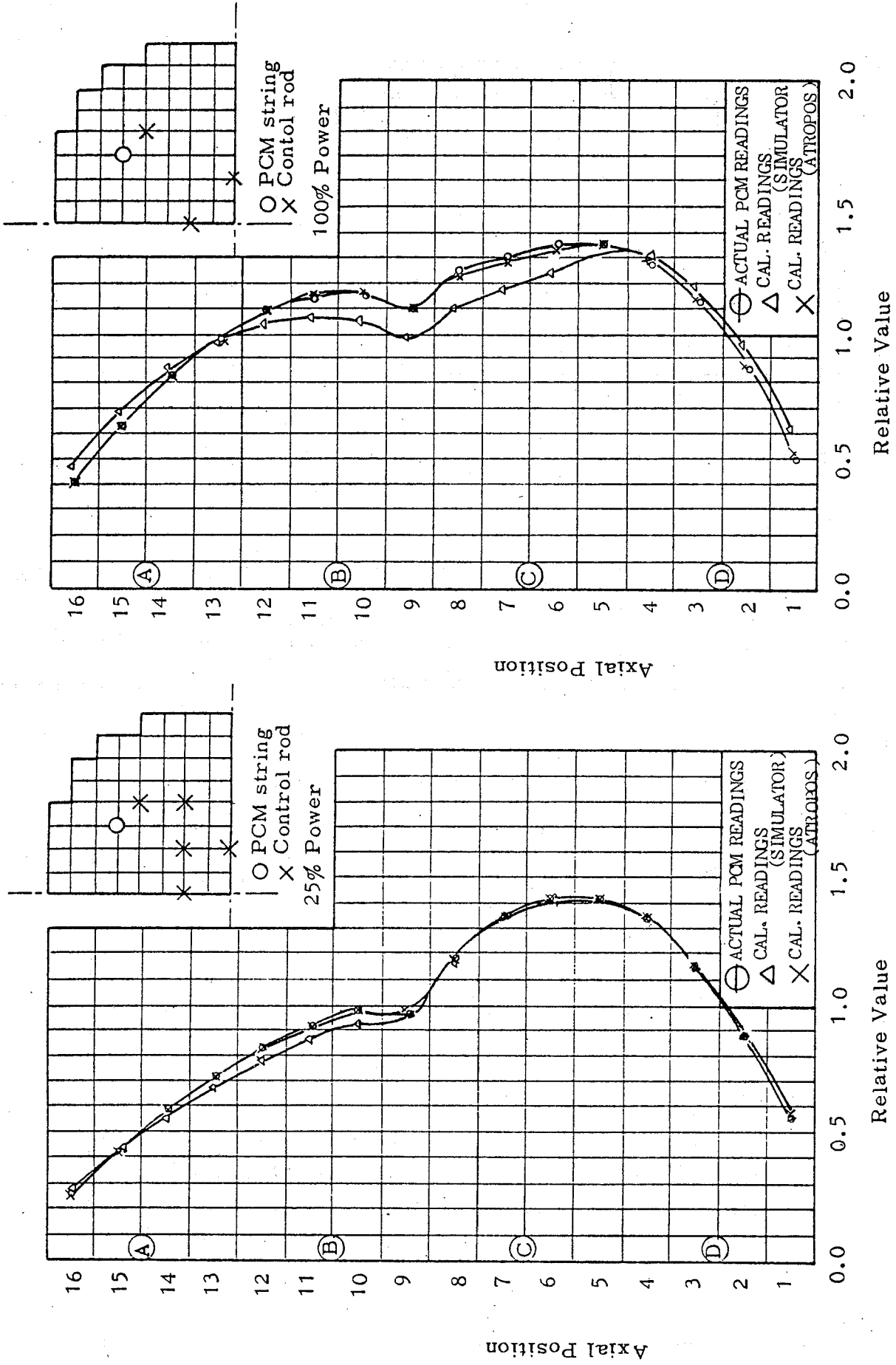


Fig. 3 Comparisons of axial flux distributions between the actual and the estimated readings.

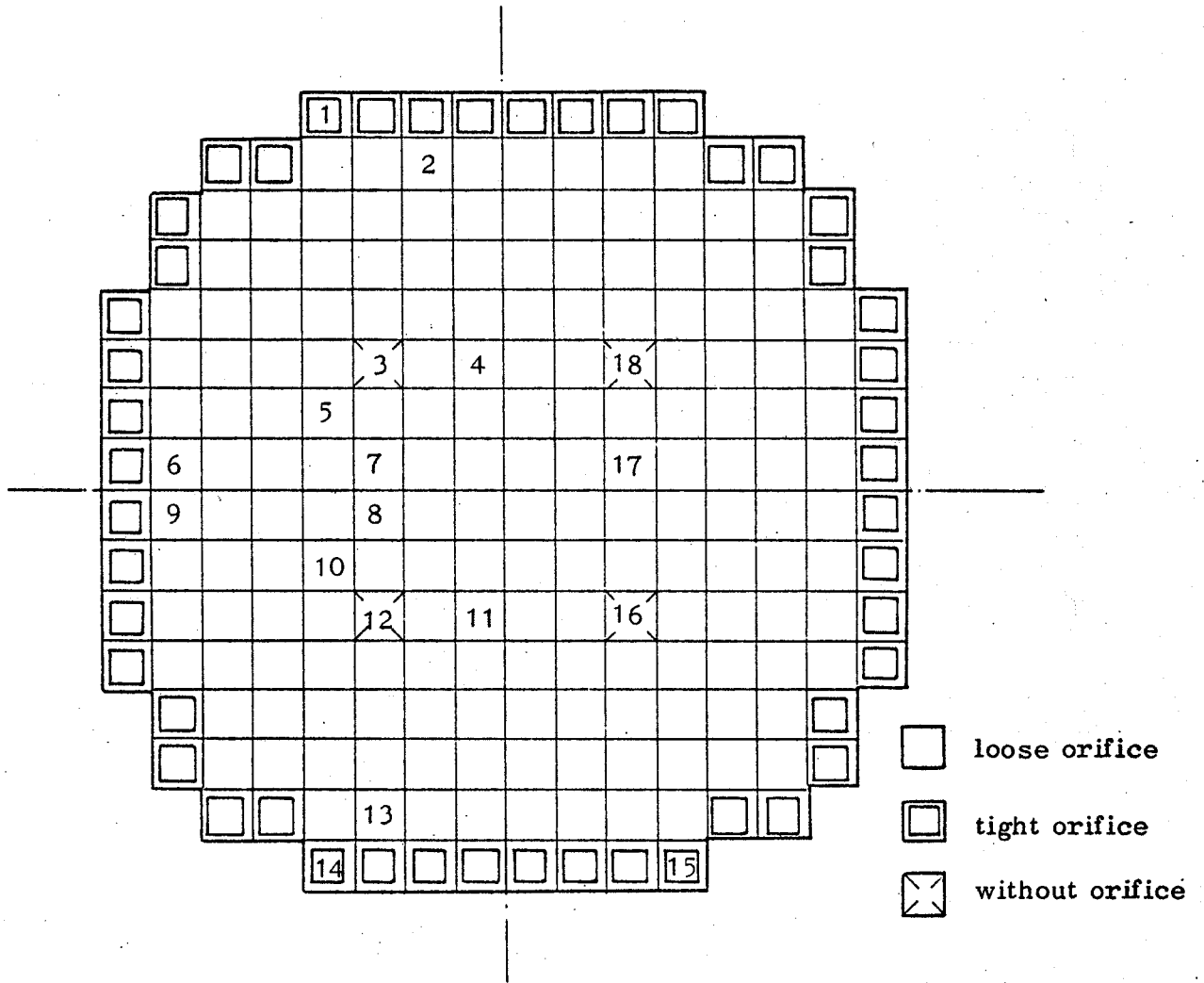


Fig. 4 The locations of the channel with the differential pressure gauge (No. 1 ~ 18)

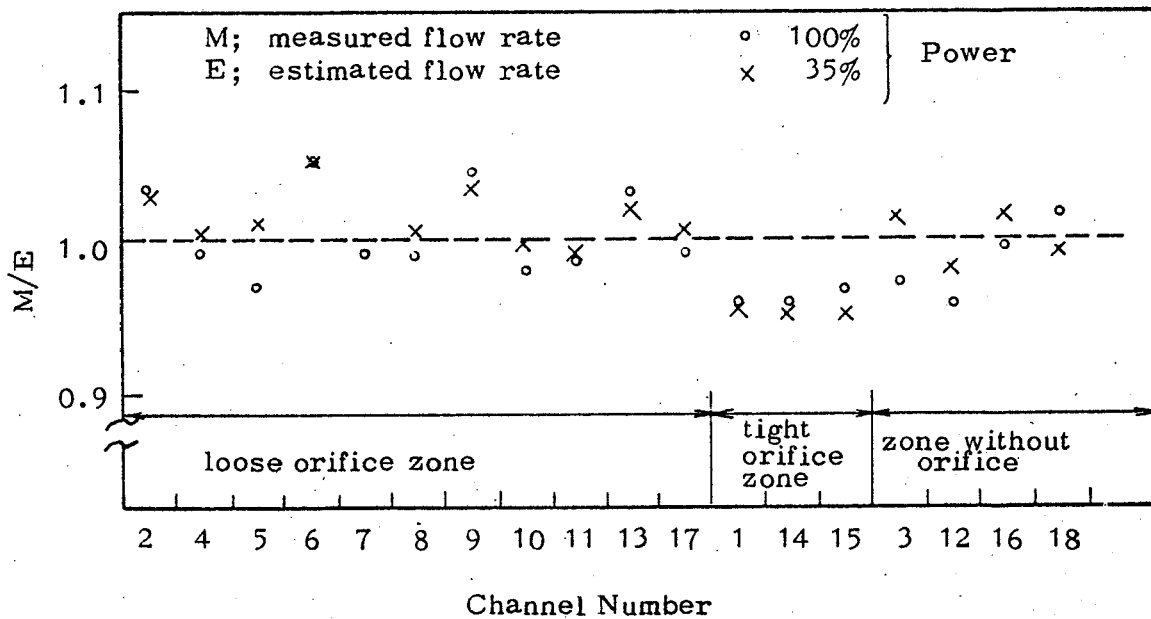
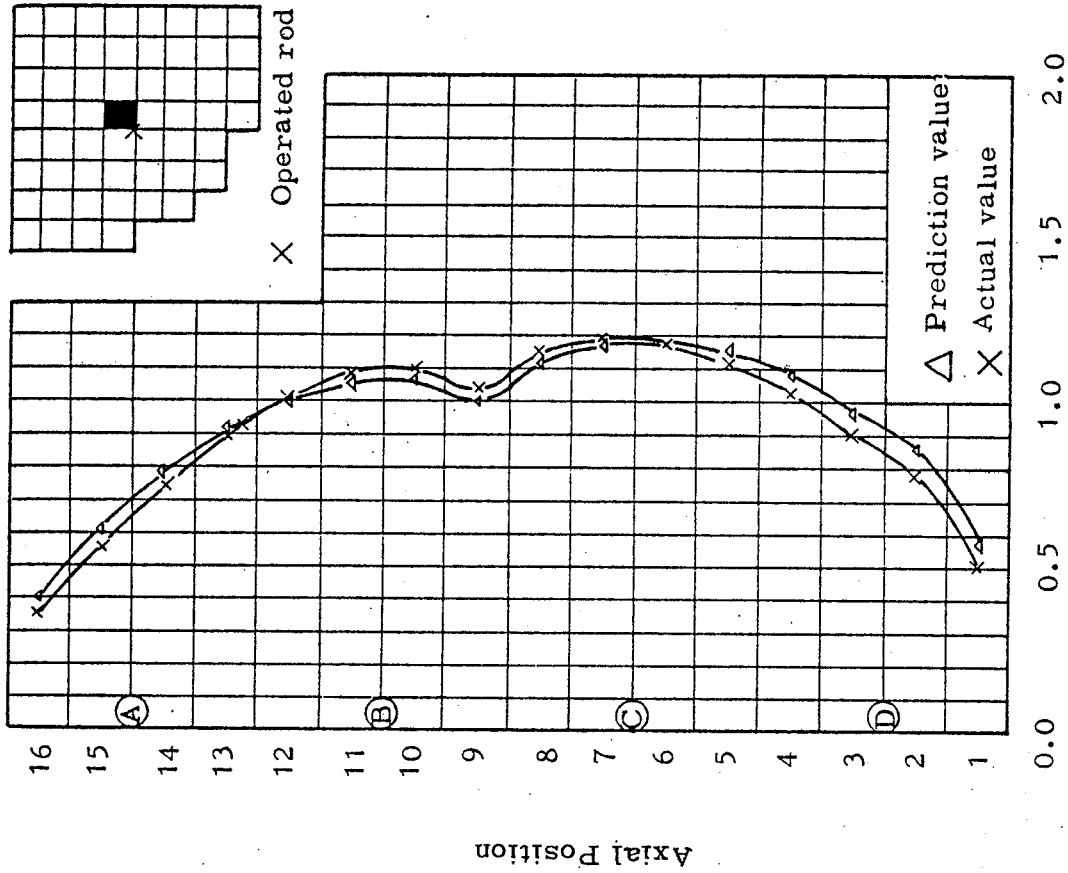


Fig. 5 Comparisons of channel flow rates between the measured and the estimated values



Relative Power of the above Shaded Channel

Fig. 7 Predictive Power Distribution of the Channel neighbouring the operated rod.

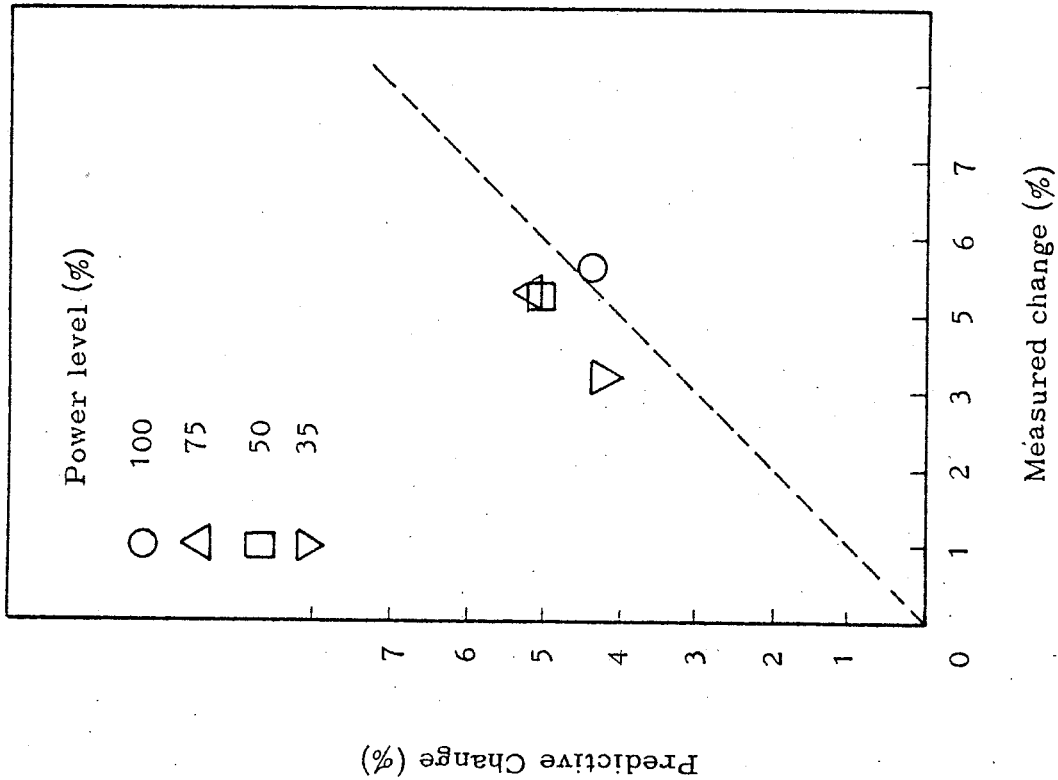


Fig. 6 Comparisons of Power Changes between Measurements and Predictions in the case of the regulating rod insertion

B. Eales, I.C. Smith

FIVE YEARS OPERATIONAL EXPERIENCE OF A MINI-COMPUTER BASED
AUTO-CONTROL SYSTEM ON THE WINDSCALE ADVANCED GAS COOLED REACTOR

FIVE YEARS OPERATIONAL EXPERIENCE OF A MINI-COMPUTER BASED AUTO-CONTROL SYSTEM
ON THE WINDSCALE ADVANCED GAS COOLED REACTOR

BY

B EALES
I C SMITH

Introduction

The prototype advanced gas cooled reactor at Windscale has two 600 psi experimental loop facilities. Each of the loops has its own independent coolant system. The power output of a fuel stringer loaded into one of these loops is determined by the general level of the neutron flux in the reactor. The fuel cladding temperatures can however be independently controlled by altering the in-core loop coolant flow.

Figure 1 shows a schematic diagram of a loop coolant circuit. The flow of gas through the loop is controlled by varying the speed of the circulator or by adjusting the setting of the three-way by-pass valve. The temperatures of the fuel pins being controlled are not measured directly but have to be calculated from a number of parameters. In some cases the control temperature itself may be specified as a function of various measured parameters. Some of the experiments loaded into these loops have coils containing Helium-3 gas wrapped around the fuel stringer. By altering the pressure of the Helium-3 in the coils, a varying degree of neutron flux absorption can be obtained. Such experimental rigs are used to study the ability of fuel pins to withstand regular power cycling.

Because each new experiment requires a different set of calculations to be programmed into the auto-controller it was decided to use an auto-control system based on a mini-computer. In order to ease the job of re-programming for each new set of calculations that part of the software was implemented in BASIC. The scanning routines and other routines controlling the interfaces to the actuators were written in assembler language and were not designed to be modified between experiments.

Data from the two experimental loop facilities is also fed into a separate mini-computer based data logging and alarm system which serves the whole reactor system. For ultimate safety protection the loops are also connected into the completely independent analogue reactor trip system.

Description of the auto-control system

Figure 2 shows a schematic diagram of the auto-control system. Both loops are independently controlled by a single mini-computer. Readings are taken automatically of outlet temperatures, in-pile flow, reactor control rod position etc and fed into a PDP 11/20 mini-computer. A total of 100 items of analogue data per loop are scanned in under software control every 5 seconds. The required cladding temperatures are then evaluated as a predetermined function of the calculated fuel pin ratings. The actual cladding temperature at the control position is then evaluated from measurements of coolant temperature and mass flow using the appropriate values of heat transfer coefficient and axial flux distribution. Any difference between the actual and the required cladding temperature is then used as an error signal to increase or decrease the in-core loop mass flow.

Because the details of the calculations vary from experiment to experiment the mini-computer was not completely programmed in assembler language to perform a fixed duty but was designed to be partly programmed in the simple high level language BASIC. This enabled loop operators to construct and modify the calculations within the control programs without necessarily having a deep

understanding of the PDP 11 computer.

The decision to provide a high level language for control purposes in order to ease the task of the operators had however some disadvantages. The computer core size was significantly larger than would have been required for a fixed duty control system programmed entirely in assembler. Also because BASIC is an interpretive language and in effect compiles as it runs there is an additional time overhead. Typically a BASIC program is a factor of 20 slower than the equivalent compiled FORTRAN program. This reduction in execution speed could prove an embarrassment in systems with fast response times. However the facilities described here have high thermal capacities and large inertias and response times are relatively slow. Furthermore a completely separate and independent analogue reactor trip system provides ultimate protection against fast transients.

The software package used was based on Dec 1 to 8 user BASIC⁽¹⁾. In order to make the language suitable for auto-control applications additional functions were added to the standard package⁽²⁾. Within the auto-controller the time-shared BASIC package supports three partitions, one for the control of each loop and one to monitor the other two. Running completely separately and checked by a clock driven timer routine, a scanning routine continuously scans 200 analogue points into fixed locations in the computer memory. The most recent data continuously overwrite the previous data.

The system has two digital voltmeters. With the full 200 points being scanned and both digital voltmeters working a whole scan is completed in 4 seconds. When only one DVM is serviceable, the scanning rate halves. In order to keep the scanning rate approximately constant for the auto-control algorithm, selected points are scanned twice in the sequence when only one DVM is working thus maintaining an update interval of four to five seconds for these points.

Within a BASIC partition, a call to access data from an analogue point causes the data currently available in memory to be returned to the program without effecting the data scanning in any way. Within the two auto-control slots substantial software protection has been incorporated which essentially groups one block of 100 analogue points a valve controller and a circulator speed controller together as being all associated with one particular loop and allows access only to one loop per partition. The monitor partition has access to data from both loops but is protected from initiating control actions.

All 200 items of analogue data are also scanned by the general reactor data logging system.⁽³⁾ This system uses two PDP 11/20 data processors. One of the processors is used for essential operational and experimental functions including alarm scanning for which continuity must be guaranteed. A second identical data processor is used for operational and experimental computation which while still important to the running of the plant can be interrupted in the event of the breakdown of the first essential processor. This second processor provides the guaranteed availability of an alarm scanning facility by taking over from the first processor in the event of its failing.

Both processors have a disk backing store. The first processor writes all the scanned data onto its own disk. Access to this data can be obtained by users of the second processor. The second processor runs under the DEC multi-user time-sharing BASIC system RSTS. Programs written in BASIC by the operators provide computed information on the state of the plant which is displayed on video units mounted in various control panels in the reactor control room. Each of the 600 psi experimental loops is an independent user in the RSTS system and each has a video display unit mounted in its control panel. In addition to the programmable

displays the video unit can also be switched to display the latest alarm messages sent out by the first alarm-scanning mini-computer.

Finally as a third switchable option, the monitor program in the auto-controller provides computed information for display on the video screen. While the auto-controller is controlling the mass flow, information is displayed giving the currently calculated values of cladding temperature that the auto controller is using as well as the current deviation from the calculated demanded temperature etc. Because the control temperatures are not directly measured, if the auto-controller were to trip out for any reason other than computer failure, or if the operator were to decide to take over control manually, calculated control temperatures are displayed on the video screen in both the auto and manual mode. This provides driving information for the operator updated every 5 seconds. If the auto-control computer itself fails then the operator has still got available via the selector switch computed driving information provided by the second reactor data logging computer. This driving information is only updated every 30 seconds. Thus computer failures lead to a gradual degradation in the updating frequency of the driving information available to the operator.

Interface design details

A specially designed auto/manual interface is provided to transfer control of the coolant flow in the loop from the operator to the computer and vice versa. In order to ensure that control is handed back to the operator if the computer system should fail, the interface is an inter-active device which remains switched to the AUTO state only if it is repeatedly and correctly addressed by the processor between certain limits of time. These limits are set at 1 second and 20 seconds so that an otherwise undetected computer failure will alarm and return control to manual within 20 seconds. If the control program running in the computer detects a fault it switches control to manual immediately by making use of the lower time limit and addressing the interface twice in rapid succession. On failure of the mains supply to the computer the interface will immediately switch to the manual state.

To hand over control of the loop to the computer control system, the operator presses and releases an AUTO REQUEST button on the control panel which then lights up. The control program running in the computer which is written to be looking for the AUTO REQUEST signal will then switch the interface to AUTO, switch on the AUTO light, switch off the MANUAL and AUTO REQUEST lights and take over control of the loop. This positive handshake procedure ensures that if erroneously a control program is not running in the computer or contains mistakes in the hand-over routine then control will remain on manual and the AUTO REQUEST light will go out after 20 seconds. The operator can of course at any time take over control of the loop by pressing the MANUAL button which effects an immediate and bumpless transfer to manual control.

The interface for the by-pass valve controller is in two parts. One part is housed in the interface box on the computer and the other part is housed in a box mounted on the loop panel. In the AUTO state, data is transferred serially between the two parts of the interface so that in the event of computer failure the valve will maintain its last requested position. A sequence of pulses increment or decrement a 10-bit reversible counter which holds the digital equivalent of the current which is sent to the valve positioner. The same counter is used in both auto-control and manual operation so that bumpless transfer is achieved between the two modes.

The serial transmission to the panel part of the interface incorporates a parity check. No movement of the valve is initiated until the parity has been checked.

as correct. If an error is detected then two further attempts are made to transmit correctly before setting an error bit. If the parity check reveals no error then the valve moves to its new position at a rate set by the auto-control program.

Changes in circulator speed when under auto-control are effected by the closure of contacts. The contacts energise a relay which in turn drives a motorised potentiometer supplying the demanded speed signal to a servo system. To change circulator speeds when the system is on manual, the same contacts are energised by the operator holding over a circulator speed control switch in either the raise or the lower position. On releasing the switch the system reverts to a state where neither the raise nor the lower contacts are energised. Thus, as in the case of the valve position controller, completely bumpless transfer is achieved between AUTO and MANUAL modes of operation and in the event of computer failure, the circulator continues to run at its last demanded speed.

To protect all interfaces on the loop panel from a loss of electrical supply, two sets of power supplies are provided each of which is capable of supplying the total power requirement. Each of the two power supplies is fed from a separate guaranteed supply

Dual actuator control algorithm

Figure 3 shows the combined valve and circulator characteristics for the loop coolant circuit. Clearly at maximum circulator speed the full range of mass flow can be covered by adjustment of the three way by-pass valve. However if the valve is allowed to reach the limits of its travel it will tend to stick and smooth control will be impossible. Thus in order to cover the maximum range in loop mass flow use must be made of both control devices. In addition figure 3 shows that the line representing the maximum power the circulator can safely produce further reduces the available operating region. The control algorithm should therefore be such as to drive the loop from minimum to maximum mass flow along a line such as the one illustrated.

In order to achieve this the circulator speed and valve position should ideally always be related by the line shown in figure 4. So as to avoid two control loops competing against each other the computer adjusts only one actuator at a time. By checking the valve position and circulator speed it determines whether the combination is above or below the ideal line. If above the line increases in mass flow are made by opening the valve and decreases by reducing the circulator speed. Conversely if below the line increases in mass flow are made by increasing the circulator speed and decreases by closing the valve. Thus control actions always lead towards convergence onto the chosen line.

Should the operator select to go onto auto-control with the valve position and circulator speed markedly displaced from the line the auto controller will switch out its normal dead band and use the random noise in the system to drive the actuators slowly in towards the chosen line. As soon as the two parameters situated sufficiently near to the line the dead band is reinstated and the small noise driven movements of the actuators halted.

Plant commissioning

The construction programme was arranged so that both the loop plant and auto-control system should be completed and component tested at the same time.

This allowed the parameter scanning hardware and auto-control processor to be used in the role of a commissioning data logger during the general plant commissioning tests.

The choice of BASIC as the system language allowed flexibility, though the ability to make rapid "on line" modifications to the data logging programmes.

Simultaneous collection and reduction of data gave guidance on the next required experimental settings when plant characteristics were being derived.

It was therefore possible to use the most economical route to give adequate cover of any characteristics minimising any interference with reactor operation, and to obtain them immediately in a form which was non-dimensionalised with respect to temperature and pressure. Consequently tight control of the latter variables was not essential and normal control manpower requirements were found adequate for the tests.

A good example of the improvement in experimental technique is given by considering the combined loop-circulator characteristics (figure 5).

Previously such characteristics had been obtained by adjusting the circuit resistance and setting the circulator to a series of standard speeds so that the mass flow/pressure drop relationship along a single "load line" was obtained. This was repeated for a series of such 'load lines'.

Inevitably pressures and temperatures varied, sometimes very significantly, due to such things as changing reactor operation during the progress of the tests. The result with the form of presentation chosen (figure 5), was an accurate definition of a series of arbitrary "load lines" and a poor definition of lines of non-dimensional circulator speed N/\sqrt{T} .

Using the autocontroller in its commissioning role the loop circulator speed and resistance (via manual isolation valves) were controlled with the VDU giving continuous indication of "non dimensional" mass flow - $W\sqrt{T}/P$, and speed - N/\sqrt{T} . It was in this manner possible to define accurately and economically lines of constant N/\sqrt{T} , which were of more value than arbitrary load lines.

During the whole series of plant definition tests logging and data reduction manpower requirements were reduced and the time to carry them out considerably shortened, minimising interference with the operating programme of the reactor.

With two shift working by rotas of one operating and two commissioning team members a series of 13 scheduled investigations on one loop were completed over 21 days of testing.

Plant supply system, pressure control system, normal and emergency cooling system and safety system were tested together with the combined loop-circulator-control valve characteristics. In addition to these a contractual acceptance test on the loop circulator was made in the presence of manufacturers representatives.

The software for this phase of commissioning consisted of 6 basic logging programmes which were modified "on line" to meet the needs of a specific test schedule or any new test objectives as they arose.

Plant modifications in the form of a by-pass circuit resistance orifice plate, and new trims for the 3 way control valve, were undertaken during the tests in an attempt to bring the combined circulator speed and control valve characteristics (figure 3) as close to those assumed in design as possible.

From the final experimental form of figure 3 it was possible to specify the preliminary practical control algorithm which would match up to design intent.

Auto control commissioning

Preliminary tests on the auto control system were made with an empty loop in which the flow resistance of a fuel stringer was simulated by partial closure of manual isolation valves in the in-reactor circuit.

Combined experimental control and logging were achieved by running an experimental auto-control programme in one computer slot whilst simultaneously running a data logging programme in a second. Both programmes were in BASIC.

The initial auto control programmes were written to demand changes in mass flow by continuous ramping, limited ramping or step change, using in turn the control valve and the circulator speed as single parameter control.

Optimisation of control response and adjustment to control algorithms, were all carried out "on line".

The process was repeated using two parameter control, and the final optimised system tested by imposing externally applied mass flow perturbations.

This initial "empty loop" phase was completed in 5 days of testing and resulted in the development of a preliminary control programme suitable for use with a fuel stringer in the loop using outlet gas temperature feedback.

The objective of the next series of tests, with a stringer in the loop, was to adjust the gain terms in the control programme to allow for the additional lag involved in using these gas temperatures.

As before, logging and operating programmes were used in parallel being subjected to more closely controlled "on line" modifications. All loop safety systems were fully operative and the auto control programme was provided with routines which "froze" auto control operation if parameters moved outside permitted margins.

From the gas temperature, in conjunction with other parameters, expected values of maximum surface temperature on the fuel elements were calculated.

This latter parameter was used as the control set point and, as in the empty loop programme, ramps and step changes in demand were made by an annexe to the control programme which exercised both single and two parameter control.

The operational control programme was continuously updated so that at the end of the test series an optimised version was in existence.

This was then tested by external changes in parameters such as mass flow and overall reactor power.

Considerable testing had been done on the loop/stringer combination, using the auto-controller in its data logger role, before these final auto control tests commenced. They were then completed on a three-shift basis over a period of 5 days.

Operational experience

During the early stages of operation it was found that aerodynamic vibrations induced in the loop were causing a long period precessional movement of the stringers within the loop. This movement was induced by "ratchetting" contact between the vibrating loop tube and stringer.

The outlet gas temperatures of the stringer sensed by control thermocouples oscillated with the same period as this movement due to gas stratification within the stringer and there was only a slight oscillation in the mass flow. The mean outlet temperature remained relatively constant.

The controller had not been designed to cope with such a phenomenon, and could therefore do nothing about removing the oscillations. However it was found that they only occurred over a relatively small region of the loop/valve/circulator characteristics, and by a small alteration to the amount of cooler used in the circuit it was possible to move operation out of the critical zone.

During such an unstable period the derived temperature error would intermittently go out of range and cause an auto/manual trip. However re-selection of auto would permit a prolonged period of operation before the error caused a further trip and the operators could take longer term measures, by use of the loop cooler, to avoid the problem.

After a critical "shakedown" period the controller settled into a steady pattern of operation. Typical statistics for the period covering the last two years are appended on Table 1 and Table 2 for both loops under control of the system.

Table 1 shows details reflecting the reliability of the system. It will be noted that the utilisation is at a very satisfactory level having a mean value of 94.25% for both loops.

The number of trips from auto to manual appears to be quite large. However most of these were only associated with very short outages, the operator having re-selected auto after having ascertained the reason for the trip and having alerted the relevant plant service section to the cause.

During the period before the fault could be cleared, further auto/manual trips were accepted and the system re-set.

The longest outage is recorded in the table. This period of 245 hours was caused by a "fleeting" hardware fault in the CPU.

Table 2 contains a breakdown of the auto/manual trips into categories typified by various faults.

The flow oscillation phenomenon mentioned previously is responsible in both loops for a large number of trips of very short duration.

A further regular cause is transducer faults. This was again associated with relatively short outages once the offending transducer had been identified.

Loop plant faults are associated with such things as circulator speed control, loop pressure control etc. A large number of trips assigned to this category on loop HP1 were due to an excitation fault on the motor alternator of that loop. Again the outage was not large as trips were accepted after the fault had been recognised and until it was rectified.

It will be seen that faults in the auto control system itself are relatively few in occurrence.

The apparently larger number of these faults on loop HP2 are due to its having been in operation for approximately twice as long as loop HP1.

For each loop the frequency of occurrence of these trips is approximately one per month.

The faults have been almost exclusively hardware originated and with the exception of the 10 day outage already commented upon have been found and cured in a period of a few hours.

References

1. PDP 11 1 to 8 user BASIC 1971. DEC-11-ZJPA-D
2. ELLIS W. "PDP 11 1 to 8 user BASIC for multi-task data acquisition and control"
DECUS EUROPE 9th SEMINAR PROCEEDINGS 1973. p95.
3. ELLIS W et al. "The new WAGR data acquisition scheme" TRG REPORT 2783 (W).

TABLE 1

OPERATIONAL STATISTICS FOR 2 YRS ENDING SEPTEMBER 1979

	Loop HP1	Loop HP2
Percent time with loop containing fuel stringer at power	36.6%	78.0%
Auto control system utilisation	94.9%	93.6%
Total no of trips 'auto' to 'manual'	192	194
Longest single period on 'manual'	245 hr 1 min	245 hr 45 min
Average time on 'manual' per trip (excluding longest period above)	27.3	3 hr 22 min

TABLE 2

BREAKDOWN OF AUTO-MANUAL TRIPS
INTO FAULT CATEGORIES

Type of fault	Loop HP1		Loop HP2	
	No of trips	Percent of total	No of trips	Percent of total
Transducer fault	31	16.1%	65	33.5%
Loop plant faults	57	29.7%	3	1.6%
Auto control system faults	12	6.3%	27	13.9%
Flow oscillation	69	35.9%	60	30.9%
Unidentified	23	12%	39	20.1%

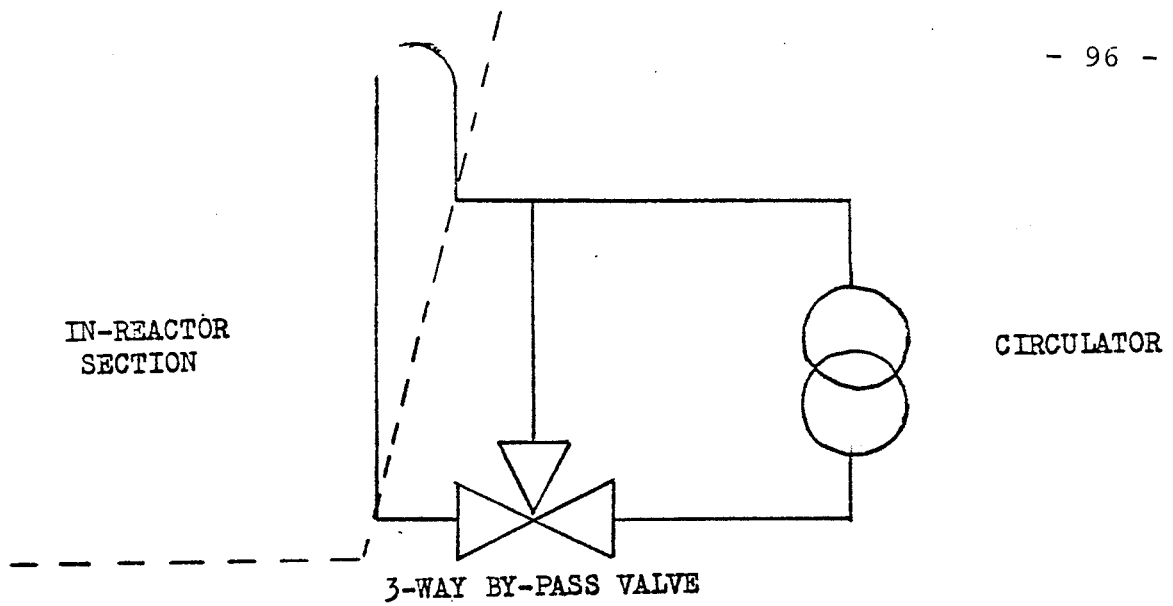


Figure 1. SCHEMATIC DIAGRAM OF A LOOP COOLANT CIRCUIT.

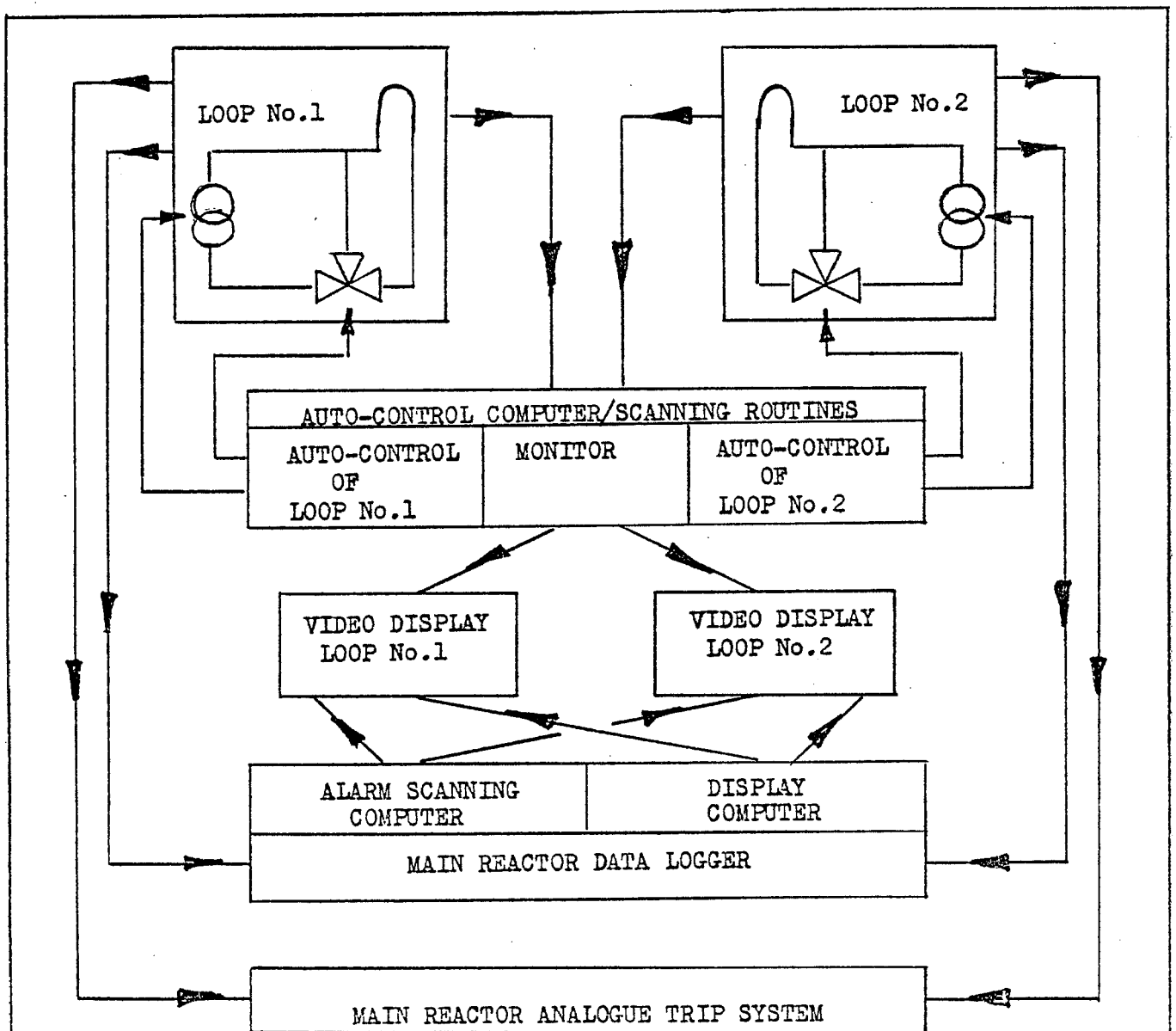


Figure 2. SCHEMATIC DIAGRAM OF THE SYSTEMS CONTROLLING THE LOOPS.

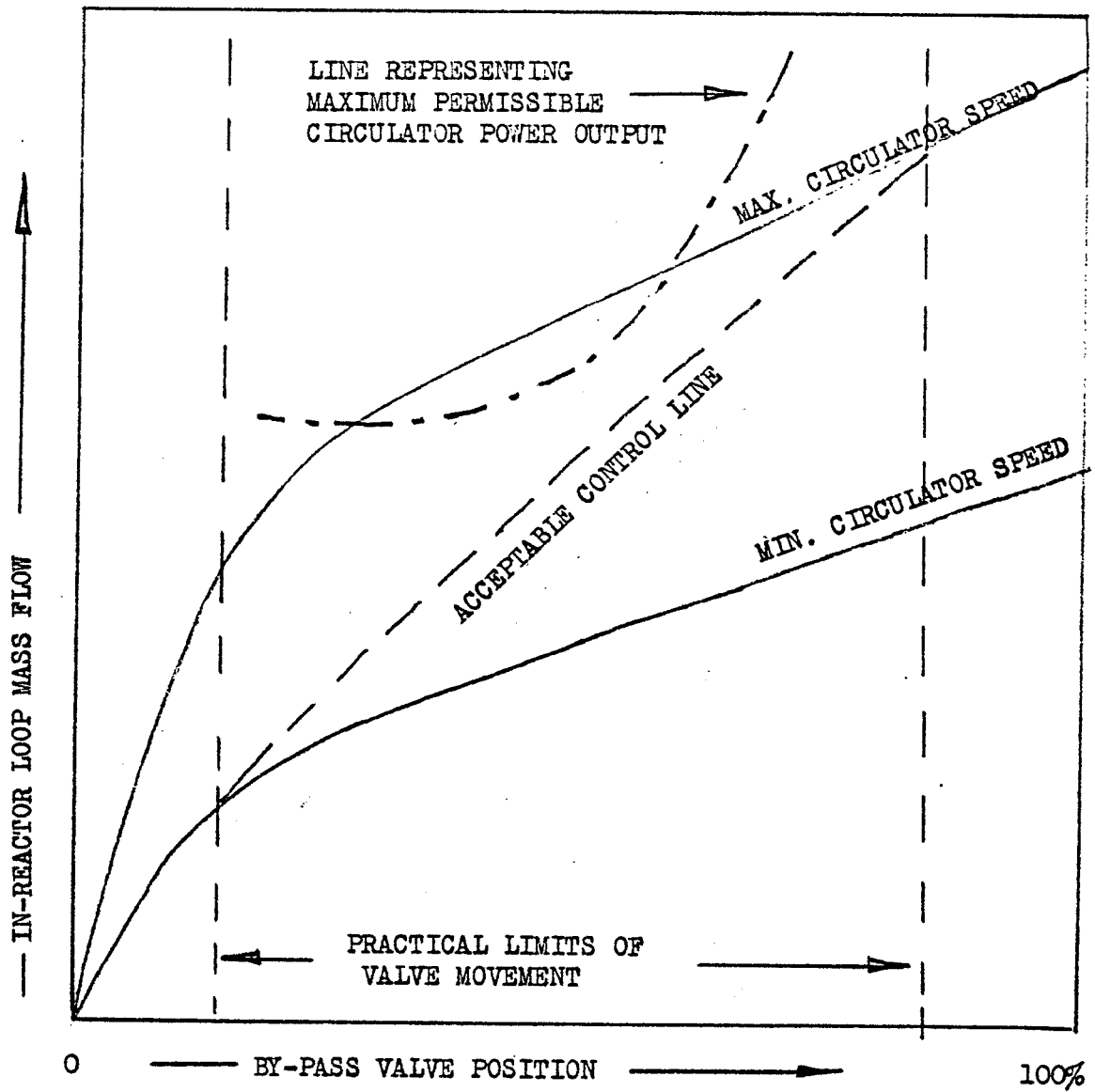


Figure 3. COMBINED CIRCULATOR AND BY-PASS VALVE CHARACTERISTICS

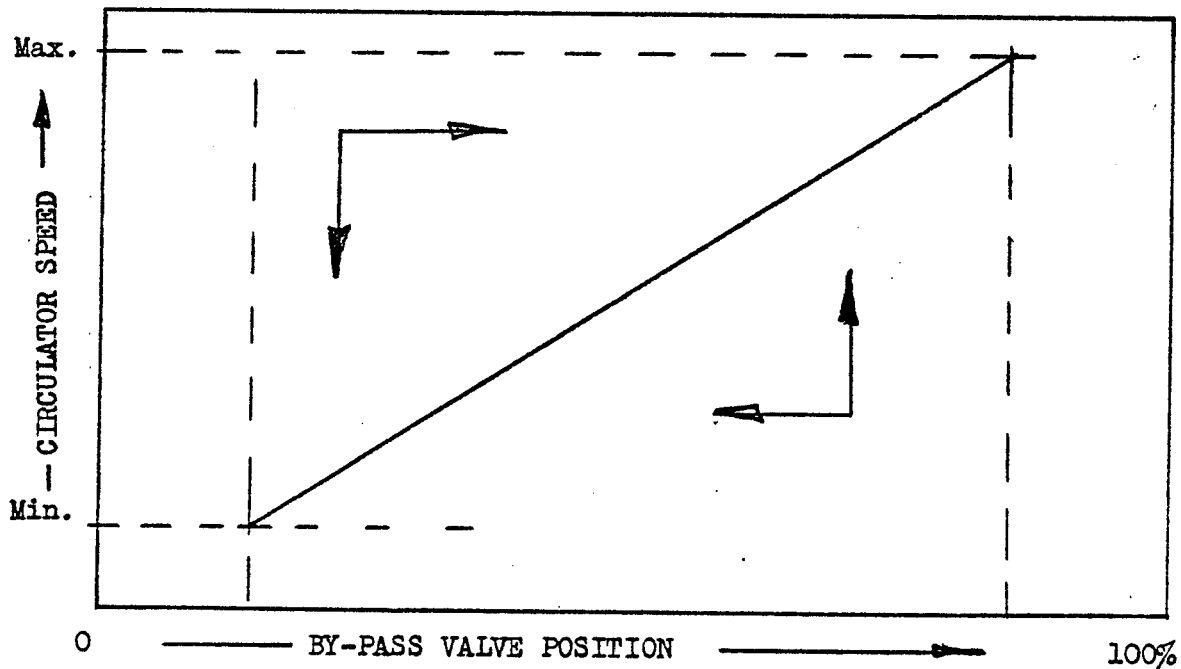


Figure 4. CIRCULATOR SPEED VERSUS BY-PASS VALVE POSITION FOR ACCEPTABLE CONTROL.

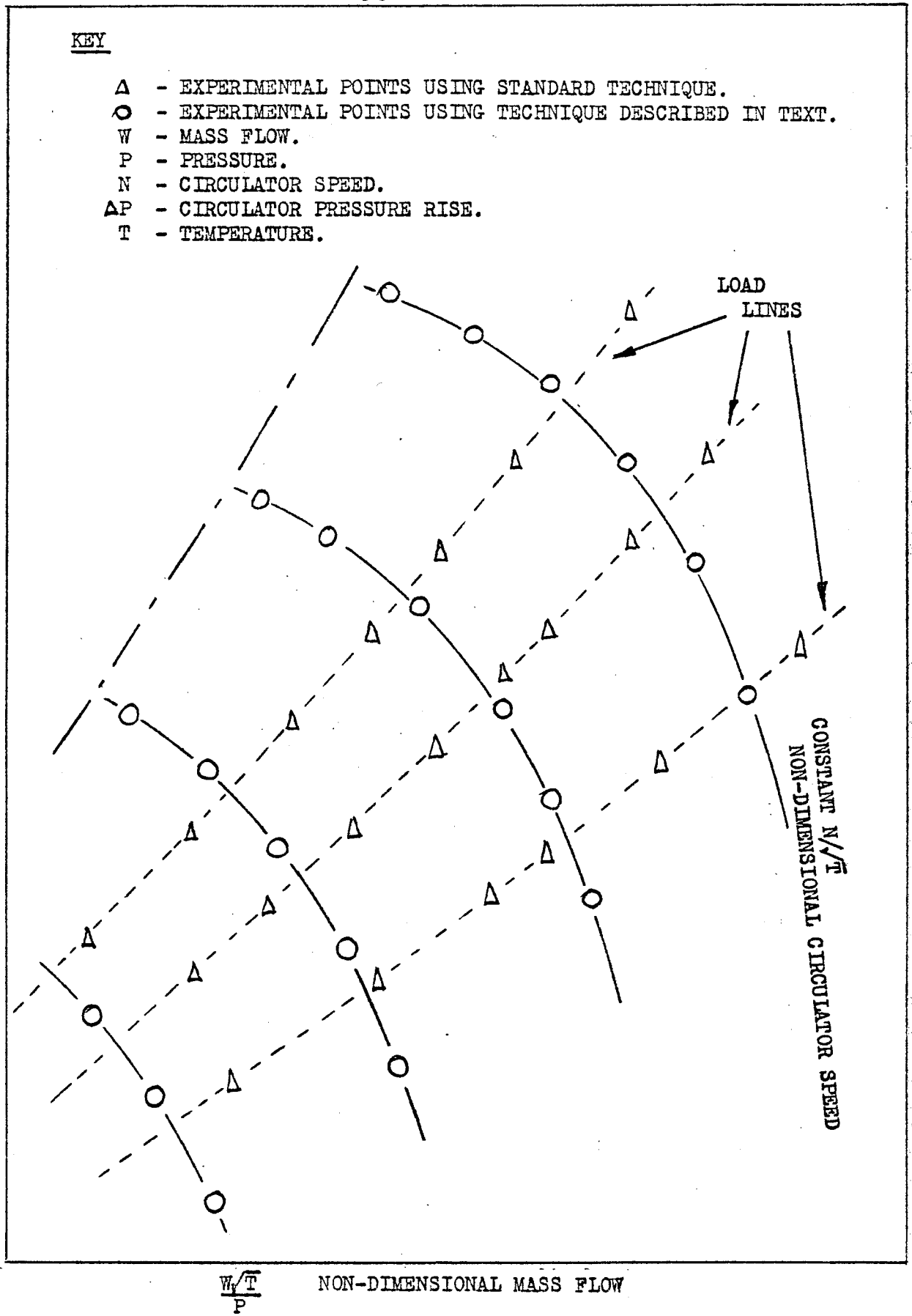


Figure 5. EXPERIMENTALLY DETERMINED CIRCULATOR CHARACTERISTICS.

H. Kawahara, K. Monta, M. Itoh

ON-LINE PROCESS COMPUTER APPLICATION FOR OPERATOR'S AID IN
TOSHIBA BWR

ON-LINE PROCESS COMPUTER APPLICATION FOR OPERATOR'S AID IN TOSHIBA BWR

H. Kawahara*, K. Monta**, M. Itoh***

- * Power Generation Control Systems Dept., Fuchu Works, Toshiba Corp.
- ** Nuclear Eng'g Dept., NAIG Nuclear Research Labo., NAIG Co., Ltd.
- ** Control & Electrical Eng'g Dept., Nuclear Energy Group, Toshiba Corp.

INTRODUCTION

From the beginning of commercial use of nuclear power, the process computer has been used for the purpose of plant control and performance monitoring. But, recent improvements of computer technology have led to apply the computer to the area of operator's aid more widely.

Toshiba as a nuclear plant and computer supplier, is acting this area also, and has recently established the hierarchical computer complex in BWR plant ^{<1>}. This paper describes following three systems which are effective to reduce operator's burden.

Most popular application for this area will be the display system with colour CRT techniques. PODIATM (Plant Operation by Displayed Information and Automation) system which has been developed by Toshiba is a typical one of this application. Currently, we are reviewing this PODIA system for the use of operator's guide even in abnormal occurrence.

Computer application to plant diagnosis is another one of recent interest. The earliest abnormality detection and prompt countermeasure against failure development into a large scale accident are of greatest importance for nuclear plant safety. The data base computer and high speed I/O system can analyze a large number of plant noise signals which contains information of earliest abnormality of plant systems and equipments.

Load following operation of nuclear power plant seems to be a real necessity in near future. Even though BWR plant can control its power easily with recirculation flow rate change, the consideration should be given to Xenon transient and reactor status such as fuel burn-up, power distribution and control rod pattern. To assist plant operation in load following operation, mini-computer system and a μ -computer based automatic reactor power regulation system has been developed.

Though process computer including μ -processor are applied as a part of controller such as safety, power generation control and data transmission function. As described above, the properly designed process computer systems can greatly reduce the operator's burden and increase plant reliability.

NEW CENTRALIZED SUPERVISORY AND CONTROL SYSTEM

In BWR power plant, all of the plant operations including plant start-up, shutdown, normal operation and anomalous operation can be performed from the central control room. According to the increase of the unit capacity and the trend of controls and monitors centralization, control and monitor devices on the control panels are increasing in number. Consequently operations of the plant has become sophisticated and burden to the operator has been increased.

Since BWR power plant control system is designed so that it provides the capability of plant operation from the central control room, a large number of control and supervisory devices are mounted on control panels.

CONCEPT OF PODIA^{<2>}

The supervisory and control devices on the conventional, control bench boards have been evolved from many functional viewpoints; frequency of operation, response time required, operating timing in the plant operation state, human engineering aspects and etc. Consequently a more efficient, coordinated supervisory and control can be attained with the PODIA system, which is based on the recent process computer and colour graphic CRT techniques. The PODIA system configuration is as follows:

- (1) A PODIA operator console, which houses the control devices and colour graphic CRT displays required for normal operation of the plant, enables operator normal operation with compact panel. (size reduction is about one third)
- (2) Nuclear Steam Supply System (NSSS) Auxiliary and Balance of Plant (BOP) Auxiliary bench board provide with control devices and supervisory instruments requiring no quick actions such as preparation of plant start-up operation and surveillance tests during operation.
- (3) Emergency Core Cooling System bench board contains the controls and instruments for engineered safeguard systems.
- (4) Supervisor Monitoring Console provides the colour graphic CRT displays for the shift supervisor to monitor of the plant operation without disturbing operator's action.
- (5) Process Computer System performs plant supervisory and control, reactor core performance calculation and process variables display on the colour CRTs. Figure 1 shows the PODIA operator console.

ADVANCED MAN-MACHINE INTERFACE UTILIZING COLOUR GRAPHIC CRTs^{<3>}

The plant informations to the operator have been centralized, integrated and optimized in quantity and in quality utilizing high information processing capability of the process computer and high flexibility of the colour graphic CRT display. Figure 2 shows a schematic diagram of the conventional control concept and Figure 3 shows the control concept with the PODIA system. The process computer system and the colour CRT displays are assigned in information loop of plant operation as a part of PODIA system. So that, reliability and availability of them are considered as follows:

- (1) The PODIA System Configuration
The PODIA system configuration, shown in Figure 4, consists of three subsystems, the High Speed Display System (HSD), Supervisory and Control Subsystem and Reactor Monitoring and Management Subsystem (RMM). Each subsystem provides with redundant process computer system.
- (2) Man-Machine Interface
Optimal man-machine interface has been achieved by considering human engineering factors to make display formats and arrange the devices. Selections of display format and assigned CRT display are easily done by combination of two push button switches, and also provide the capability of display format transfer from failed to any sound CRT. Plant monitoring status, plant automatic control state and reactor core operation state can be easily readout through colour CRTs and key boards. Figure 5 shows an example of colour CRT display formats.

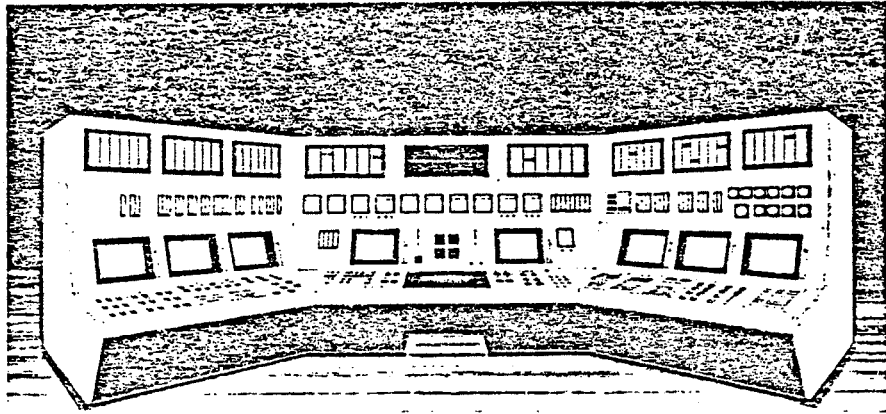


Fig. 1 PODIA Operator Console

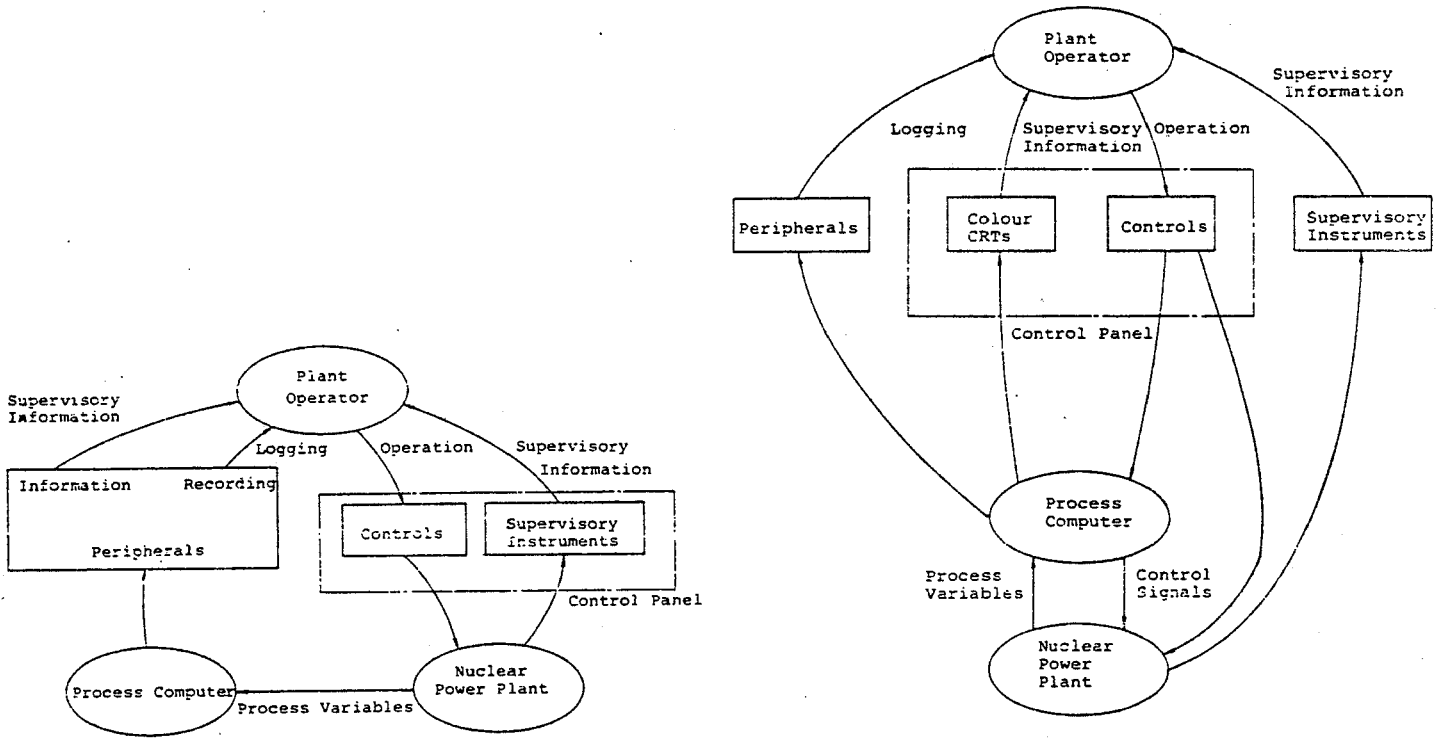


Figure 2 Conventional Control Concept.

Figure 3 Control Concept with PODIA System.

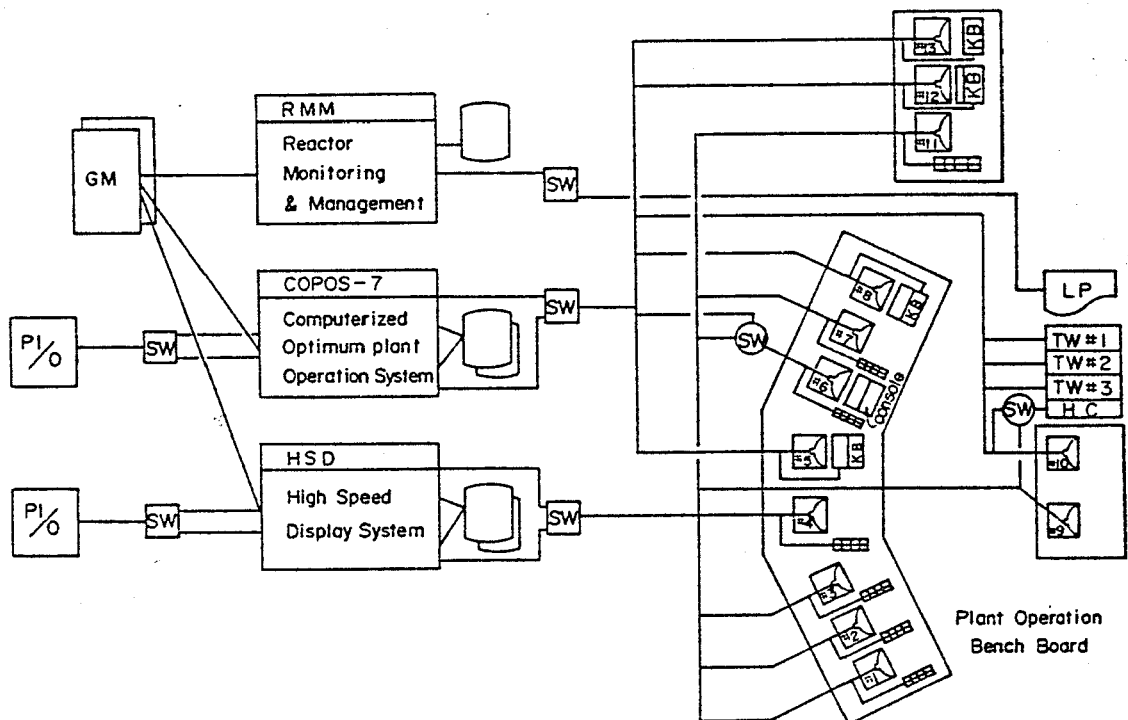


Fig. 4 PODIA System Configuration

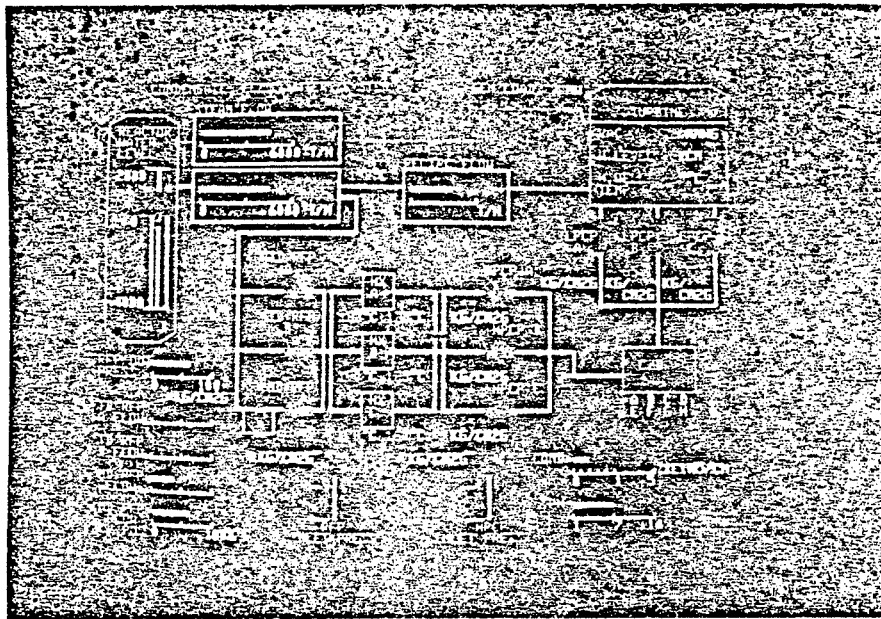


Fig. 5 An Example of colour CRT Display

PLANT DIAGNOSTIC SYSTEM<3>

Failure indication earliest abnormality detection and prompt counter-measure against failure development into a larger scale accident are of greatest importance for nuclear power plant safety and safeguards. Moreover, early failure detection works for integrity preservation and preventive maintenance, also contributing to plant availability improvement and employee's radiation exposure decrease owing to maintenance period and expenditure reduction. On this viewpoint, studies have been promoted, for over ten years, on a noise analysis technique (fluctuation from steady state plant parameters) for failure early detection, mainly in experimental reactors. Toshiba has engaged in reactor noise analysis and diagnosis technique development for years. Lately, Toshiba has completed reactor diagnosis system design, also conducting field tests in commercial nuclear power plants. An outline of reactor noise analysis technique and diagnosis computer system is discussed here.

Nuclear power plant noise analysis and diagnosis intends abnormal condition early detection, which couldn't be performed by conventional instrumentation systems due to moderately aggravating properties of concern. Figure 6 shows functional differences between them. Conventional systems activate alarm or scram signals when safety operation limit is exceeded, while reactor diagnosis system continuously monitors plant condition and integrity, based on data obtained from plant design, construction and operation after commissioning. This system can detect abnormal plant conditions at the earliest stage and diagnose them, seeking countermeasures against propagation and expansion of those adverse conditions.

Such functions are implemented by the following procedure.

- (1) Plant conditions are monitored by measuring plant parameters and determining correlation among them.
- (2) When plant parameters have changed, these are identified.
- (3) Examination is made to determine whether or not abnormalities exist.
- (4) Abnormality aggravation and extension are predicted beforehand.
- (5) Countermeasures are presented for abnormal condition recovery and removal. :

Items (1) through (5) hold diagnosis basis. The previous discussion may clarify that the diagnosis system differs from conventional systems in emphasis placed on abnormality early detection and countermeasure determination. This system is compared to medical services. Conventional systems operate in such a manner that likes to care (alarm) or hospitalization (scram) directed to a patient who consults for an unusual health condition. Meanwhile, the diagnosis system corresponds to regular health examination which is held with no regard to any particular consciousness of illness.

The following are purpose for developing a diagnosis technique for nuclear power plants.

(1) Plant availability improvement

Early abnormality detection and prompt countermeasure enable failure recovery at the earliest stage and maintenance period decrease. Well planned maintenance will also improve plant availabilities.

(2) Radiation exposure decrease

Since maintenance periods are decreased and failures are recovered before they reach a serious stage, periods during radiation controlled area operation and resulting radiation exposure are reduced.

(3) Continuous plant safety condition monitoring

Since plant condition deviations from normal conditions are continuously monitored, plant safety factor is always verified.

REACTOR DIAGNOSIS IMPLEMENTATION METHOD

For conducting a diagnosis, much more detailed monitoring is needed than in conventional systems.

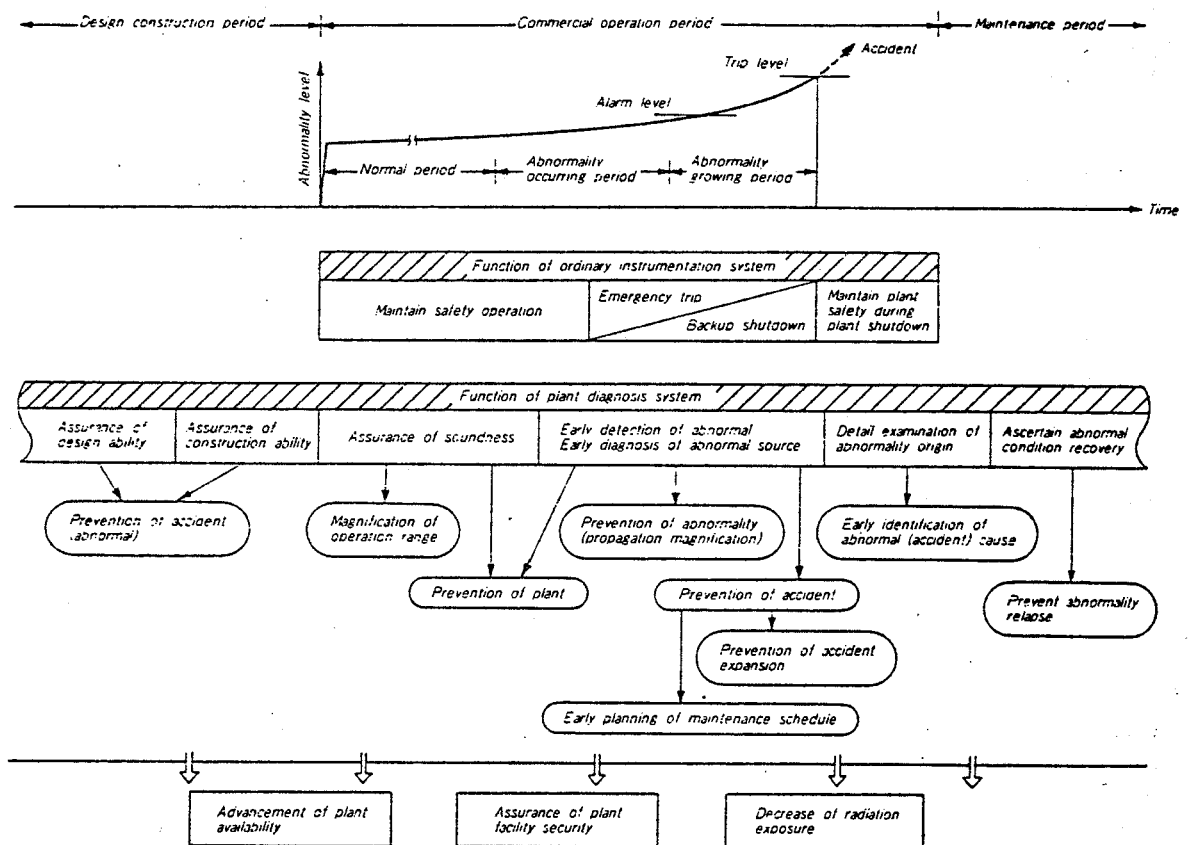


Fig. 6. BWR plant diagnostic system function

This requirement is a matter of fact, since abnormality detection and identification must be performed before abnormalities become explicit.

Therefore, what kind of methods will be adopted for analyzing monitored phenomena weighs greatly in diagnosis technique. The following are required for these techniques.

- (1) Sensitively responding capability→leading to early detection.
- (2) Capability of providing for information regarding plant parameters and correlation among them→leading to timely problem identification.

Toshiba has conducted reactor noise analysis research and development as a promising method for meeting these requirements.

Figure 7 shows the noise analysis and diagnosis method. This noise analysis is organized with frequency and/or time domain analysis of plant parameter fluctuation (noise) for investigating and monitoring plant dynamic characteristics and conditions. Figure 6 shows a case for abnormality indication of valve activation parts, wherein fluctuation varies greatly

from that in normal conditions with remarkable large power spectrum density shift. Noise analysis method can be adopted, because the following two properties are utilized, namely, fluctuation sensitively responds to system condition variation and information regarding plant parameters and correlations among them are obtained by analyzing cross correlations between them.

Figure 8 summarizes noise analysis and reactor diagnosis features.

REACTOR DIAGNOSIS SYSTEM OUTLINE

(Reactor Diagnosis System functions and Monitoring Items)

Toshiba has studied a BWR reactor diagnosis method by a noise analysis for over ten years and has investigated correlation between plant operational conditions and noise pattern properties from a huge amount of accumulated noise data. This investigation clarified that reactor diagnosis technique by a noise analysis is effective for early abnormality detection. In order to ascertain effectiveness in actual units, Toshiba has designed and trially manufactured a reactor diagnosis mini-computer system, shown in Figure 9. This system has the following functions.

- (1) Plant parameters needed for plant diagnosis are collected and analysis results in particular periods are preserved.
- (2) Collected data are compiled and converted into power spectrum density, correlation function, transfer function and so on for a comparison to referencing patterns for diagnosis (power spectrum density, cross correlation function and so on.).
- (3) Diagnosis results are output on a teletypewriter or CRT. In case an abnormality is identified, the causes for abnormality are output. However, if the causes cannot be determined, correlation between abnormal condition and signal pattern is newly correlated for diagnosis function expansion.

This system is organized with Toshiba developed mini computer, TOSBACTM 40D, as a primary unit for reactor core and control system diagnosis. However, further functional and diagnosis item expansions are possible.

Table 1 shows items that can be subjected to diagnosis. For a reactor core, in the first place, core reactivity stability causing power oscillation, channel stability and in-core instrumentation tube vibration are monitored. When reactivity stability and channel stability become worse, power oscillation results, causing adverse effects on nuclear fuels. This stability monitoring is of greatest importance for this reason.

Second, as to controlling systems, pressure control system, feed water control system and recirculation flow control system, controlling characteristics and stabilities are monitored. Early abnormality detection by monitoring these control systems can prevent a reactor from being scrambled by the control system abnormality.

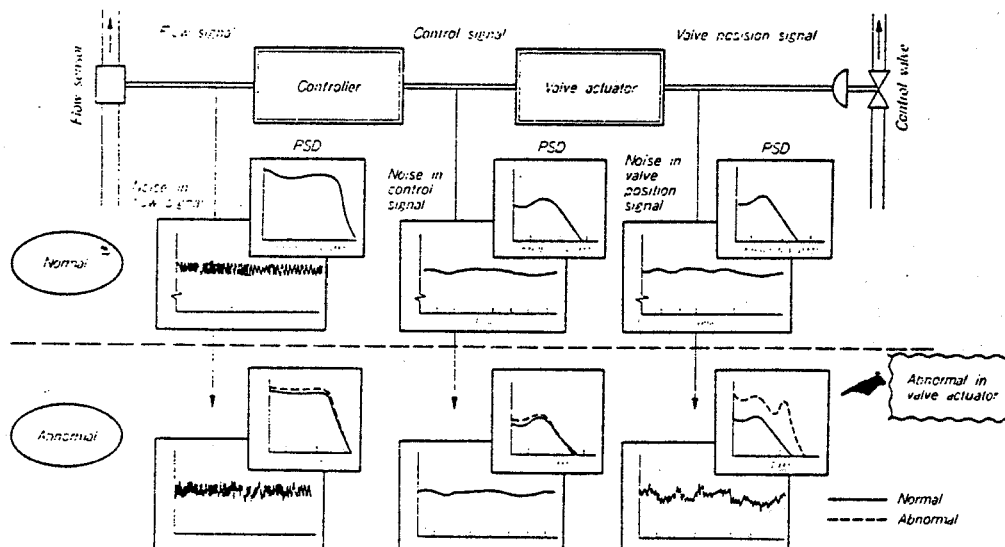


Fig. 2. Diagnostic method conceptual illustration by noise analysis

- (1) Frequency analysis of noise (Noise analysis = much information) → Early detection of anomaly
 → Much information for identifying the cause of anomaly
 → Diagnosis of dynamics without artificial disturbance
- (2) Diagnosis by the comparison with normal data → Diagnosis of unmodeled complicated systems
 → Diagnosis of each part in the whole system
- (3) Know noise source in BWR core → Noise analysis is accurate for diagnosis of BWR core.
- (4) Noise analysis technique for diagnosis is studying in many fields and countries → Utilization of many results in other fields and countries

Fig. 8. Advantage of BWR plant diagnosis by noise analysis

Table 1. Diagnosis Items

	Diagnosis Items	Diagnosis Significance
Core Section	Core Reactivity Stability	Avoidance of bad influence on fuel by power oscillation
	Channel Stability	Extension of operating boundary
	Channel Blockage	Prevention of fuel damage
	Channel Flow Distribution	Channel flow estimation based on experimental data
	LPRM Vibration Diagnosis	Channel-box damage prevention
	Channel-Box Damage Diagnosis	Fuel damage prevention
	LPRM Position Confirmation	LPRM position confirmation
Jet-Pump Section	Jet-Pump Vibration Diagnosis	Prevention of damage by vibration

Recirculation Flow Control Section	Main Controller Operating Characteristics	Early detection of troubles in control systems ↓ Prevention of scram Prevention of accidents
	Velocity Controller Operating Characteristics	
	Scoop-Tube Operating Characteristics	
	M-G Set Operating Characteristics	
Recirculation Pump Section	Recirculation Pump Operating Characteristics	Early detection of troubles in control systems ↓ Prevention of scram Prevention of accidents
	Recirculation Flow Control System Stability	
	Main Controller Operating Characteristics	
	Flow Control Valve Actuator Operating Characteristics	
Feed Water Control Section	Flow Control Valve Operating Characteristics	Early detection of troubles in control systems ↓ Prevention of scram Prevention of accidents
	Motor Governor Unit Operating Characteristics	
	Turbine Control Operating Characteristics	
	Feed Water Control System Stability	
Pressure Control Section	IPR Operating Characteristics	Early detection of troubles in control systems ↓ Prevention of scram Prevention of accidents
	Turbine Control Valve Operating Characteristics	
	Turbine By-Pass Valve Operating Characteristics	
	Pressure Control System Stability	

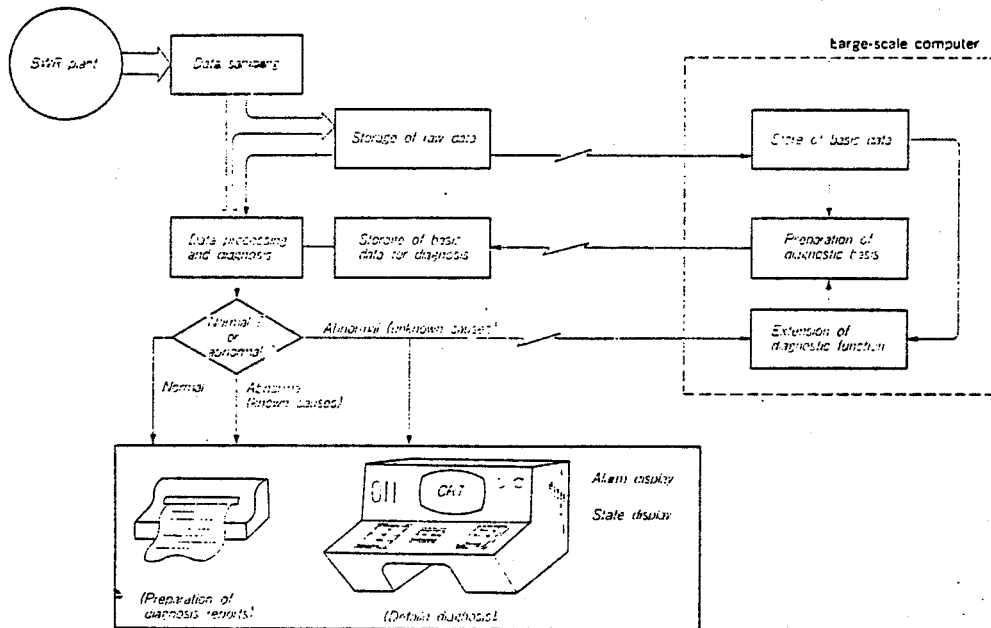


Fig. 9. BWR plant diagnostic system conceptual illustration

LOAD FOLLOWING OPERATION SYSTEM

Load following operation of nuclear power plants seems to be a real necessity in near future. The nuclear power generation in Japan has increased such that its capacity exceeded 10% of the total grid power generating capacity; this proportion is larger at night than day time. According to a current estimation, this proportion is expected to increase to about 50% (at night) in 1985.

In order to maintain the flexibility and reliability of electric power supply under such a situation, the need for the daily load following operation of nuclear power station will become much stronger.

Studies have been made on load following operation feasibilities of BWR nuclear power stations under thorough cooperation between a Japanese utility and the reactor power program controller has been developed to facilitate the automatic daily and weekly load following operation by recirculation flow control.

The reactor management system<4>, which has been developed for the purpose of more comprehensive and up-to-date analysis of the reactor operating state and reliable prediction of reactor behavior, is expected to further facilitate the BWR load following operation.

ASSESSMENT OF BWR LOAD FOLLOWING CAPABILITY

For planning the daily load following operation such as 14 hours high power operation at day time, 8 hours low power operation at night time and 1 hour transition period, an axial one dimensional core transient analysis model with Xenon and Iodine kinetics was developed. This model is adequate to describe the gross core behavior following with the recirculation flow control and fission product change. It can also give an approximate solution of core power distribution change due to the recirculation flow and xenon redistribution. In addition, it has an advantage of the ease of numerical calculation such that on-line predictational calculations are possible with the usage of the current reactor operating data as initial conditions and model parameters. This capability has been shown to greatly increase the accuracy of the predictational calculation compared with 3-D offline calculation with less accurate input data. Figure 10 shows an example of the calculational results with the 1-dimensional model for a typical daily load following operation. From this results, it is clear that the reactivity compensation for Xenon transient by recirculation flow is significant in the following two aspects; the first is the trajectory deviation from the allowable operating region in the power/core-flow map shown in Figure 11 and the second is the power distribution change due to the Xenon transient effect which may cause the pellet-clad interaction failure of the fuel elements, if the preconditioned envelope exceed during the transient.

Figure 12 shows an example of the power distribution change where the curve ①, shows the preconditioned envelope, the curve ②, the initial power distribution, and the curve ③, the maximum power distribution envelope during transient, the upper part of which is formed during high power, high flow, i.e., the larger Xenon poisoning period while the lower part is formed during high power, low flow, i.e., the smaller Xenon poisoning period.

Analysis using the one dimensional model has been performed for various daily and weekly load patterns which have different high and low power levels, different transition period and so on to assess the trajectory in the power/core-flow region and the extent of the necessary preconditioned envelope expansion.

From the above results we can conclude that the certain daily and weekly load following down to about 75% rated power is possible solely by recirculation flow control under adequate core management, i.e., preparation of the necessary preconditioned envelope and the control rod pattern.

The system is constructed by the mini-computer TOSBAC TM-40D and peripheral and has the data link between the existing process computer for core performance calculation. So the system can utilize the data base on the reactor core in the process computer. Nodal Xenon and Iodine densities are periodically updated by the RMS. RMS utilizes the axial one dimensional core model mentioned before for prediction of reactor core behavior under various maneuvers. When the core recirculation flow control is used, this model is quite adequate to predict the three dimensional power change $P(x,y,z,t)$ by the following approximation

$$P(x,y,z,t) = P(x,y,z,0) \frac{P^*(z,t)}{P^*(z,0)} \quad (1)$$

where $P^*(z,t)$ is the solution of the axial one dimensioned core model and $P(x,y,z,0)$ is the known initial power distribution from the process computer.

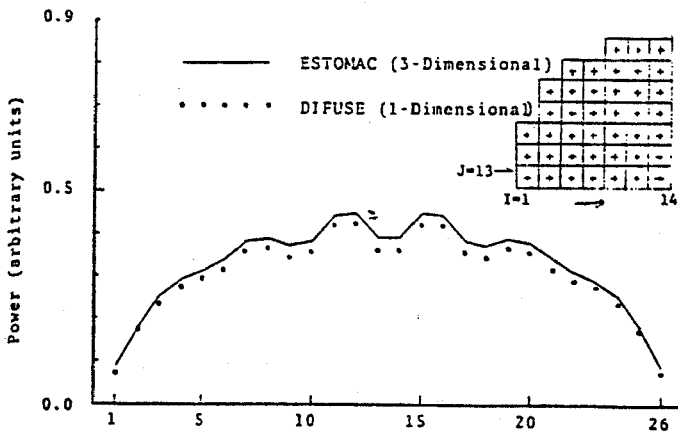
Figure 15 shows examples of this approximation where the results of the power distribution calculation by Eq.(1) for the fuel rods across horizontal lines at two axial line $k=13$ and 22 are compared with the exact 3-Dim. calculation. Fairly good agreement between the two is shown.

The RMS has the function of identification for local power distribution which uses the signals from LPRM (Local Power Range Monitor) string. This function also utilizes the axial one dimensional core model to interpolate and to extrapolate the signals from LPRM string to obtain local power distribution around the LPRM.

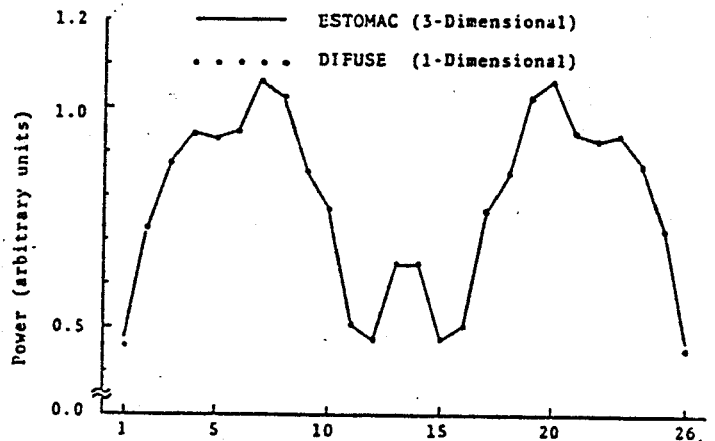
The application of RMS to load following operation is quite beneficial. The first is the predictability capability. Before the load following operation, RMS can simulate the core behavior under load following operation based upon the current state of the reactor core. If some violation of the operational constraint will be predicted, it is possible to adjust the load following pattern manually or even automatically. This prediction can be performed for the preselected load pattern of RPPC as well as the more general pattern, which adds the flexibility to the load following operation by the RPPC.

The second is the monitoring capability. The RMS's monitoring capability is faster and more comprehensive than the existing process computer because of the RMS's local nature of power distribution calculation and more detailed preconditioned envelope management. The proximity of the core operating state to any constraint can be detected earlier and necessary corrective actions such as power hold or power run back can easily be implemented.

The integration of RPPC and RMS is apparently the next step of the development for BWR load following operation.



[2] Radial Power Shape (core position: J=13, K=22)



[1] Radial Power Shape (core position: J=13, K=13)

Fig.10 Comparison between 1-D Approximation and 3-D Result.

REACTOR POWER PROGRAM CONTROLLER

To control the station electric power output, existing BWRs have the manual load setter in the turbine speed/load controls and the manual flow setter in the master controller of the recirculation flow control system. In performing the daily load following operation as shown in Figure 10, operators must perform continuous adjustment of the manual load setter or the manual flow setter not only during the transient period, but during constant power period.

In order to automate these operations and to exactly control the generator power, the reactor power program controller (RPPC) has been developed with due consideration for readiness of its installation in constructed BWRs.

The block diagram of the system is shown in Figure 13. It contains the load pattern generator and performs the feedback control of the generator power in accordance with the pre-selected load pattern. Its output is the demand signal to the existing load setter in the turbine speed/load controls.

In order to facilitate the operation, the system has the automatic initialization feature which enables the load reference, i.e., the load setter motor to quickly coincide in position with the initial value of the generated pattern when the system starts operation. The rate of change of the motor position is 15%/min at this case. After initialization the rate of change of the load setter is limited within 30%/hour to avoid the unnecessary power change in the load following operation.

The system is composed of the microprocessor based control unit, the operator console, the load pattern illustration panel, auxiliary relays and isolation amplifiers. The photo of the RPPC is shown in Figure 14.

The control unit stores the preselected load patterns of daily and weekly. Upon the request by the operator, the unit generates the operator selected load pattern according to the internal timer signal. The unit continuously monitors the reactor core, plant status and the functions of the unit itself. If an abnormality is found, alarm is generated and/or auto-reset of the RPPC function is taken place.

Major monitoring items are as follows:

- (1) Monitoring of core operational state by neutron flux signal and total jet pump flow signal.

The core operational state in the power/core-flow map is checked against the allowable operational region.

- (2) Monitoring of core operational constraint.

By communicating with the existing process computer, violation of the preconditioned envelope for each fuel node and of MCPR (Maximum Critical Power Ratio) limit are monitored.

- (3) Monitoring of the plant status.

Major transients by main plant components failure such as a trip of a recirculation pump, a trip of a feedwater pump and so on, are monitored in order to prevent scram with auto-resetting by RPPC function.

- (4) Self-diagnosis

Drive pulse of load setter motor, analog input signals, generator power output control function, power supply of the system and the system bus are monitored by the control unit.

APPLICATION OF REACTOR MANAGEMENT SYSTEM^{<5>}

The Reactor Management System (RMS) has been developed and tested. The objectives of this system are to perform more comprehensive and up-to-date analysis of current reactor state and to enable reliable prediction of core behavior under various maneuvers. The system first aimed at the operator aid for PCIOMR (Pre-Conditioning Interim Operating Management Recommendations) operation by monitoring PCIOMR violation, accurate prediction of target power in PCIOMR operation and so on^{<1>}.

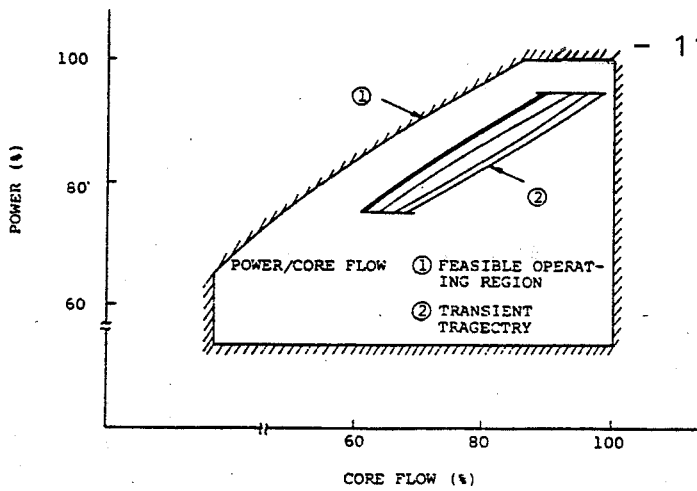


Fig. 11 Power/Core Flow Transient following 14-1-8-1 hr Power Demand Change

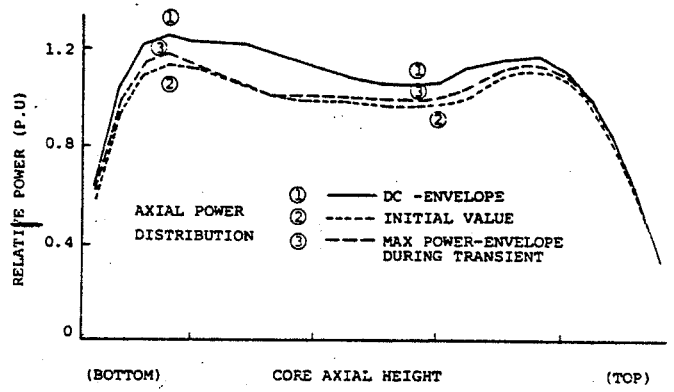


Fig. 12 Average Core Axial Power Distribution following 14-1-8-1 hr Power Demand Change

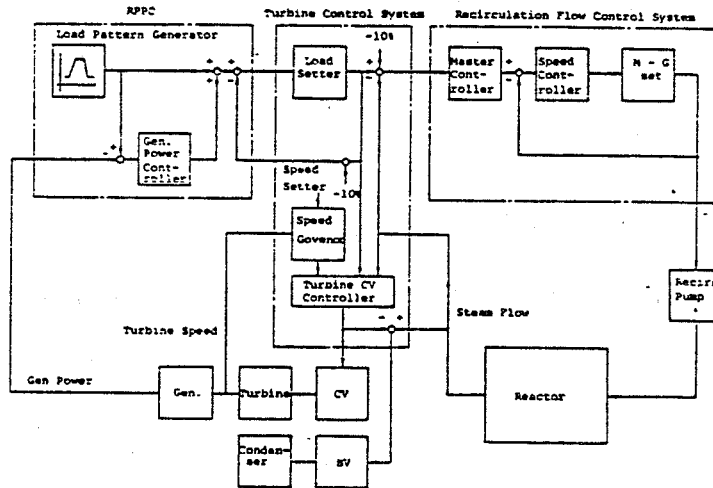


Fig. 13 Block Diagram of Reactor Power Control

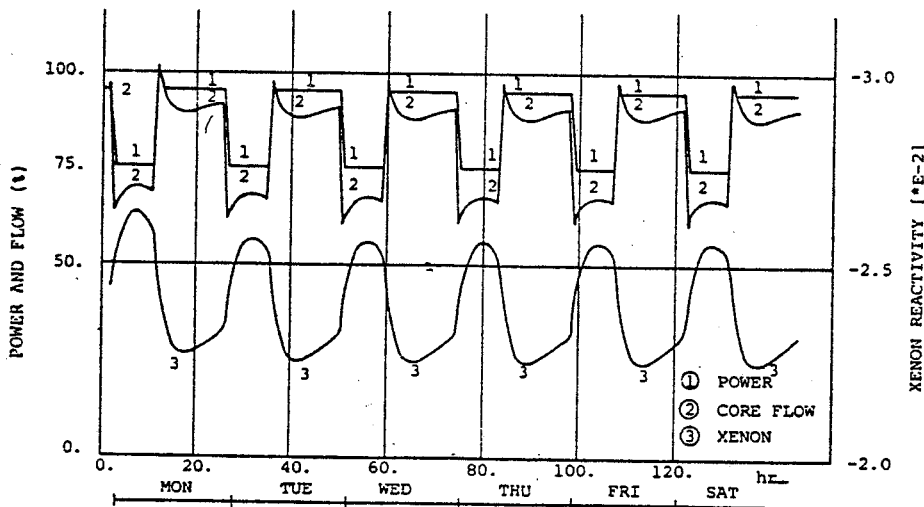


Fig. 15 Feactor Coreflow and Xe transients following 14-1-8-1 hr Power Demand Change

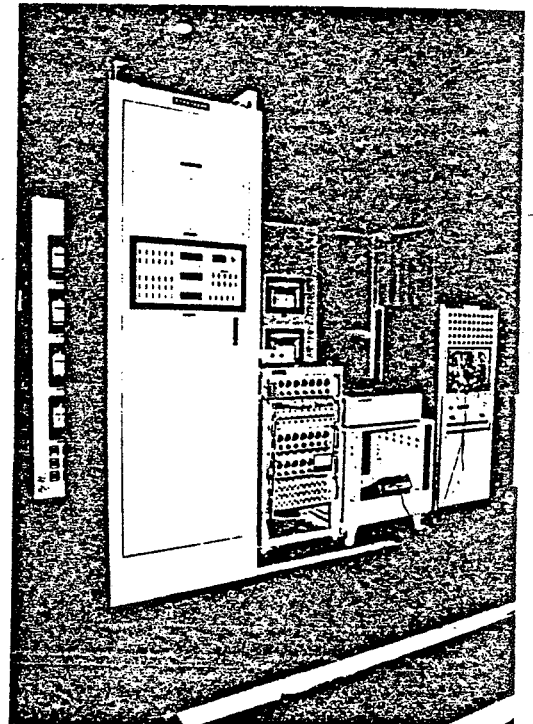


Fig. 14 Photo of RPPC (left pannel) (800W x 762D x 2286H)

CONCLUSION

After TMI-2 incident, human credit has been re-evaluated from the stand point of operator error reduction.

One of the most important implementation is speedy and complete monitoring of plant status during abnormal occurrence. And automatic operator action guide to prevent expanding the accident is also important.

Though, the systems described here have been developed before TMI-2 incident, some of TMI-2 Lessoned Learned are involved. However, we still continue to study improving these systems and developing new systems for the implementation of TMI-2 Lessoned Learned more completely.

REFERENCE

- <1> M. Kaneda, "The New Integrated Hierarchical Computer Complex in A BWR plant"
Paper, IFAC Symposium at New Delhi Aug. 1979.
- <2> R. Aoki et al. "BWR Centralized Monitor and Control System, PODIATM Development" Toshiba Review Int'l Ed., No.107, JAN-FEB 1977
- <3> M. Makino "An Application of the Process Computer and CRT Display System in BWR NPS"
Paper, IAEA Specialist meeting on Control Room Design, San Francisco July 1975
- <4> A. Tanabe et al. "Nuclear Power Plant Diagnostic System Using Noise Analysis " Toshiba Review Int'l Ed., No.112 NOV-DEC 1977
- <5> K. Makino et al. "Reactor Management System"
Paper, Enlarged Holden Program Group Meeting at Loen, June 1978

R.J. Conte

A MODEL SURVEILLANCE PROGRAM BASED ON REGULATORY EXPERIENCE

A Model Surveillance Program Based on Regulatory Experience

R.J. Conte, U.S. Nuclear Regulatory Commission,

King of Prussia, Pennsylvania 19406

ABSTRACT

A model surveillance program is presented based on regulatory experience. The program consists of three phases: Program Delineation, Data Acquisition and Data Analysis. Each phase is described in terms of key quality assurance elements and some current philosophies is the United States Licensing Program. Other topics include the application of these ideas to test equipment used in the surveillance program and audits of the established program.

Program Delineation discusses the establishment of administrative controls for organization and the description of responsibilities using the "Program Coordinator" concept, with assistance from Data Acquisition and Analysis Teams. Ideas regarding frequency of surveillance testing are also presented.

The Data Acquisition Phase discusses various methods for acquiring data including operator observations, test procedures, operator logs, and computer output, for trending equipment performance.

The Data Analysis Phase discusses the process for drawing conclusions regarding component/equipment service life, proper application, and generic problems through the use of trend analysis and failure rate data.

A Model Surveillance Program Based on Regulatory Experience

R. J. Conte, U.S. Nuclear Regulatory Commission, King of Prussia, Pennsylvania 19406

Introduction

Plant surveillance plays an important part in ensuring the safe operation of a Nuclear Power Plant. The necessity for having reliable components¹ is two-fold. First, from a safety consideration, the technology relies on redundant dependable equipment to properly function when called upon to mitigate analyzed transients. Second, from a power generation viewpoint, Plant Operators² desire to maintain dependable equipment to reduce the risk of sudden failures requiring costly plant off-line time.

In the United States Licensing Program, licensee event reports³ indicate that a majority of the events are recorded as due to component failure and/or malfunctions. Further, surveillance testing has been the primary means of identifying component problems. This testing program is heavily relied upon to judge the operability of equipment with respect to license conditions.

Presented herein are several key Quality Assurance aspects linked to a model surveillance program based on regulatory experience. This type of program should complement a good quality assurance program of design, construction and maintenance (reference 3).

¹Included in this term are groups of components/equipment required to function as a system.

²Plant operators are taken to include upper management staff.

³The Background Section includes a brief explanation of this system.

Background

The United States Nuclear Regulatory Commission (USNRC) requires periodic surveillance testing of safety components in Technical Specifications (TS) which are appended to the licensee. These requirements verify compliance with the TS Limiting Conditions for Operation (LCO). The TS, which have been standardized, are specific with respect to frequency but in most cases they are general in terms of parameter performance and how the test is to be performed.

Surveillance program requirements including general test procedural content are specified in an American National Standard (ANS) N18.7 (references 1 and 2) which are frequently used in U.S. Licensee Quality Assurance Programs. These standards call for the following key elements: schedules, procedures (along with format requirements), records, reporting and evaluation of test results (reference 2).

The TS also require the reporting of abnormal events termed "Reportable Occurrences" on a Licensee Event Report (LER) forms. A category of such an event is failure to meet a TS LCO or Surveillance Requirement. The form provides codes for computerization of pertinent information associated with the event.

Another reporting system that has been recently established is the Nuclear Plant Reliability Data System (NPRDS). This is also a computerized system which deals primarily with the categorization of component failures or malfunctions (reference 5).

The two systems (LER and NPRD) are distinguishable as follows. The LER System is mandatory from a regulatory viewpoint while the NPRD System is voluntary at this time. The NPRD System consists of a computerized component data base from initial voluntary input reports along with historical reports on component problems. The LER System is a file of events which have placed systems in a degraded condition. These events may be caused by human error, procedural problems, or external causes other than component failures.

Surveillance Program - General

The key elements or phases of any surveillance program consist of Program Delineation, Data Acquisition and Data Analysis. The Program Delineation includes the organization of personnel, associated duties/responsibilities, software and hardware to be utilized in the data acquisition and analysis phases. The Data Acquisition phase should assure the proper collection of useful and reliable information without degrading redundant operable components. The key phase, Data Analysis, should assure the timely review and evaluation of data along with the reporting and dissemination of results.

Surveillance Program Delineation

The program description can easily be accomplished through the establishment of a distinct written plant administrative control procedure. A Nuclear Plant Surveillance Program is considered significant enough to warrant its own administrative controls.

The personnel (by job position) along with associated duties and responsibilities needs to be specified in writing to avoid confusion. Confusion may arise because the model program normally includes the utilization of a variety of personnel with technical expertise having other direct line responsibilities.

A sample organization chart is provided in Figure 1. The ultimate program responsibility lies with the Plant Superintendent but one individual should be designated "Coordinator" with sole responsibilities for program effectiveness. The coordinator must interface with operations, maintenance, technical support and quality assurance staffs. Certain members may function on the data acquisition and analysis teams as well.

The data acquisition team should, in general, encompass operations department personnel to assure proper test procedure implementation and equipment operation. This does not preclude the use of other plant personnel such as a plant chemist, however, the established administrative control should address, before hand, types of personnel to be utilized in this effort.

The data analysis team relies on a combination of a variety of expertise. As resources permit the analysis team should be comprised of core personnel with project management experience and perhaps possessing a specific area of expertise. Where several experts are involved in an evaluation, the report should be the responsibility of a designated lead individual or project manager.

The complexity of a Nuclear Plant Surveillance Program dictates the use of detailed schedules to ensure that the program is properly administered. Computer technology has been extremely useful in this area and many U.S. licensees have adopted this approach. In this aspect however, experience has shown that application of the computer is dependent on the quality of the computer programming. This variable necessitates periodic auditing of the system to assure that schedules and information are being properly implemented.

The specification of frequency for surveillance tests in the program must have an adequate technical basis. Consideration needs to be given to component testing on too frequent an interval causing component degradation, while prolonged intervals between tests may not detect failure or abnormal trends toward failure. Vendor recommendations are a good starting point for initial program establishment, however, these frequencies should be subject to change depending on trend analysis results or experience.

For these reasons, surveillance test frequencies should not be specified as a licensee condition. The operator should have the flexibility (with proper administrative controls) to adjust test intervals with experience. Plans exist in the U.S. licensing program to remove surveillance requirements from the Technical Specifications, and permit operators to establish these requirements in an "Operation's Plan" that would be subject to approval by the licensing authority. Subsequent changes could be made to the program by the operator with reports of such changes to the licensing authority on a periodic basis.

Finally, the administrative controls should specify format and general content of procedures used to implement the program (references 1 and 2). Along these lines, the specification of logistics for processing completed procedures aides in the delineation of responsibilities (for example, assuring completed procedures along with data is forwarded to a member of the analysis team).

Data Acquisition

The Data Acquisition phase of the program can not be over emphasized because the quality of data analysis is closely associated with the quality of the data acquired which is representative of test conditions. It is imperative that the operators properly implement the established procedural controls. The most important aspect of this is the compliance with license conditions during the test and the restoration of the system/component to normal operation when the test is completed.

A good surveillance program also includes the data acquired as a result of the normal review of plant operations and the use of shift logs. This information is useful for trend analysis of significant normal operating parameters.

A key element in the review of normal operations is the shift operator. The shift operator is the first line of defense for detecting abnormal component conditions. The operator's duties should include a review of recorded operational parameters (routine observations). These observations should be performed with a "keen eye" for off-normal conditions. The use of the plant computer is important in this regard.

Plant computer surveillance is imperative. An additional aide to the operator could be a computer review of system status, such as a programmed versus actual valve lineup comparison to detect abnormal lineups (i.e., flow path valves isolated). This function should be supplemented by standard parameter alarm functions.

One assumption that has been made in this phase of the program is the reliability of the instrumentation used to collect data. Reliability is a function of proper calibration of the instrumentation with traceability to primary/national standards (reference 6). As a minimum for any test procedure, the serial number or designation of the test equipment (in-line or off-line) should be recorded for traceability. The maintenance of test equipment is addressed in a subsequent section.

Data Analysis

Data Analysis is the key element to the entire surveillance program. The objectives of the analysis should be: The determination of component service life status based on data input, verification of component application, and wide dissemination of generic problems associated with components.

The functions of the analysis teams should be: Verification of data in compliance with procedural acceptance criteria, trend analysis for significant normal operating parameters, trend analysis for test condition key parameters, and reporting of conclusions for corrective action to be taken, if warranted. Of particular interest here are the aspects of trend analysis for test condition parameters and reporting of results.

The data analysis team is not meant to usurp the responsibilities of the shift operators but they should complement the shift operator's function. In fact it is highly recommended that shift operators be members of that team. The data takers should conduct an initial review of data against the acceptance criteria to identify obvious problem areas (especially for simple tests). The data analysis team concept is valuable for the conduct of the more complicated/sophisticated testing with respect to test implementation participation and analysis of results.

Recently, the USNRC incorporated requirements for pump and valve testing into the standard TS. The requirements are specified in the American Society of Mechanical Engineers (ASME) Code (reference 7). Pump testing, for example, includes performance analysis using baseline data and trending. Alert and Action ranges are established for determining operability status and a threshold for the necessary maintenance (reference 6). This approach is recommended for all major equipment.

Documentation and reporting of analysis should not stop at upper management of the plant organization. Component problems sometimes have generic implications. Such information should be supplied to other organizations with similar equipment. The USNRC, through the LER System, generates Bulletins, Circulars and Information Notices for generic problems and these receive wide distribution throughout the United States. A Bulletin is significant enough to warrant a response from the licensee while the Circular and Information Notice are information type documents. However, in general, the LER System only "sees" events that have occurred because of some effect on the TS Limiting Condition for Operation (LCO). Many events involve component malfunctions/failures which would not be reported because it did not effect the TS LCO.

A more comprehensive idea developed recently is the Nuclear Plant Reliability Data System (NPRD). This voluntary computerized program is a consortium of utilities which input basic information on various plant components with subsequent reports on component malfunctions/failures (reference 5). This program, however, is relatively new and its effectiveness is still under review.

Test Equipment

The utilization of test equipment in a surveillance program must be backed up by an equally comprehensive surveillance (calibration) program. The elements addressed above apply to such a mini-surveillance program. Some exceptions are noted below.

A calibration procedure may not be warranted for each piece of equipment but generic procedures for types of equipment, such as pressure gages, should be developed to assure quality performance.

Trending of data need not be as extensive, however, careful reviews of repeated calibration check failures should warrant action for increased surveillance or equipment replacement. Along these lines a method should be established to trace the usage of test equipment that was found to be out of calibration (reference 5). Thus the effected surveillance tests can be redone with properly calibrated instrumentation to assure quality data.

Audits

With any comprehensive and extensive system affecting the quality of components, auditing of program requirements is a must to verify proper program implementation. If an audit system is not established through a Quality Assurance Program, the Surveillance Program should self impose such a system. In either case the audit should review the entire surveillance program including technical aspects.

Acknowledgement

The author wishes to acknowledge the United States Nuclear Regulatory Commission, Office of Inspection and Enforcement (Region I), King of Prussia, Pennsylvania for the opportunity to write this paper and the following individuals who assisted in the development of this work: H. Kister, U.S. Nuclear Regulatory Commission (Region I), King of Prussia, Pennsylvania and L. Prough, U.S. Nuclear Regulatory Commission (Three Mile Island), Middletown, Pennsylvania.

References

- (1) American National Standard Administrative Controls for Nuclear Power Plants N18.7-1972.
- (2) American National Standard Administrative Controls and Quality Assurance for the Operational Phase of Nuclear Power Plant N18.7-1976 (Revision of N18.7-1972).
- (3) Title 10, Code of Federal Regulations, Part 50, Licensing of Production and Utilization Facilities, Appendix B, Government Printing Office, Washington, D.C.

- (4) Instructions for Preparation of Data Entry Sheets for Licensee Event Report (LER) File, published by Office of Management Information and Program Control, U.S. Nuclear Regulatory Commission (July, 1977).
- (5) Reporting Procedures Manual for the Nuclear Plant Reliability Data System, prepared by Southwest Research Institute under the direction of ANSI Subcommittee N18-20 (April, 1974).
- (6) The Institute of Electrical and Electronics Engineers, Inc. Standard Installation, Inspection, and Testing Requirements for Instrumentation and Electric Equipment During the Construction of Nuclear Power Generating Stations IEEE Std 336-1971 (ANSI N45.2.4-1972).
- (7) American National Standard American Society of Mechanical Engineers (ASME) Boiler and Pressure Vessel Code (July 1974 Edition with Addenda through Spring 1976).

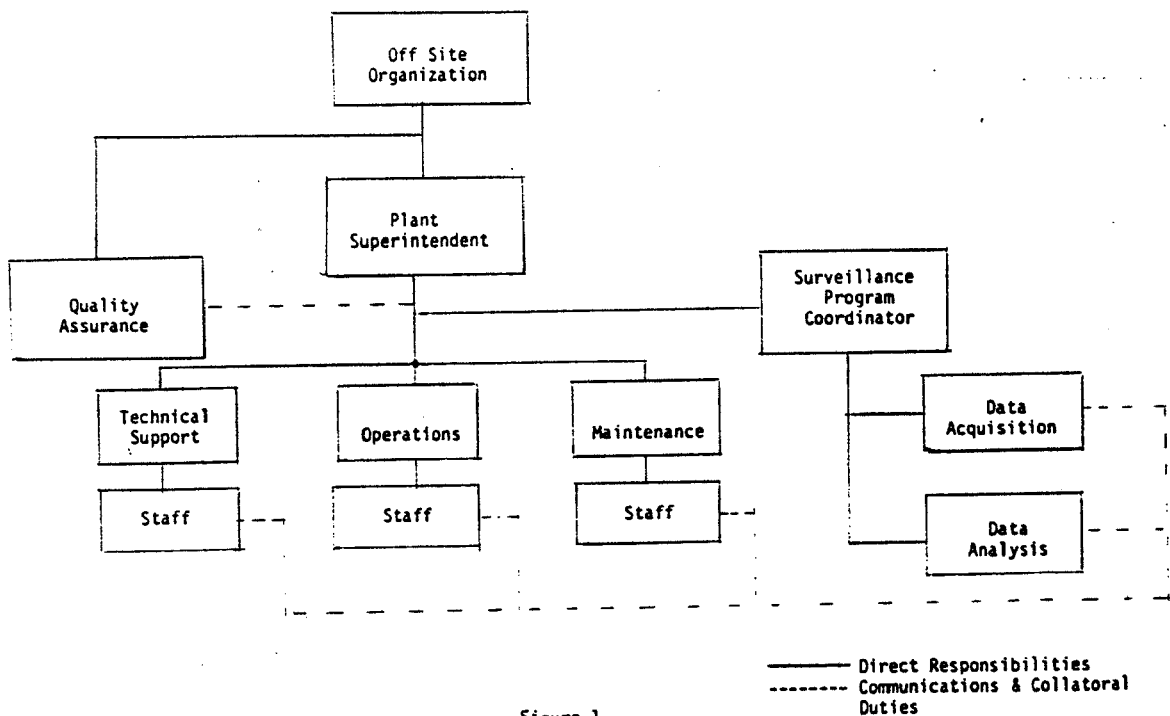


Figure 1

CONTENTS

Session II

TRAINING / SIMULATORS

Chairperson: R. Espefält

Secretary: D. Beraha

R. Espefält, D. Beraha SUMMARY OF SESSION II	131
G. Vaccarino ON THE DESIGN OF THE PEC REACTOR TRAINING SIMULATOR	137
A. Kameda, M. Sato, T. Sato, M. Sakuragi EVALUATION OF LIQUID METAL FAST BREEDER REACTOR OPERA- TOR TRAINING SIMULATOR	151
C.F. Gnospelius, P.E. Persson, R.I. Carlsson TRAINING OF POWER PLANT OPERATORS BY THE USE OF A SIMULATOR CLOSELY REPRODUCING ANOTHER PLANT	167
S. Kawashima BWR OPERATORS TRAINING EXPERIENCE USING SIMULATOR	179
J.F. Green, S. Birnie OPERATOR TRAINING FACILITIES FOR CEGB ADVANCED GAS COOLED REACTORS	197

R. Espefält, D. Beraha
SUMMARY OF SESSION II

R. Espefält, D. Beraha

SUMMARY OF SESSION II

The four papers presented in the session deal with the application of full-scale simulators to the operator training.

The first paper by Vaccarino describes the PEC simulator developed for a sodium cooled fast test reactor. In addition to operator training purposes, the simulator supports the development of operational and data acquisition procedures and aids the testing of control scheme changes. The simulator includes the operator's and instructor's desk, and the process computer on which real-time plant models are run. From the instructor's desk, the training can be monitored and recorded. Furthermore, the instructor interacts with the plant model to induce specific situations which include fault conditions.

Asked about the extent to which the simulator is used for training and for plant condition simulation respectively, the author replied that in the first two years before start-up of the plant, the simulator will mainly be used for operator training and procedure design. Afterwards, its main task will be to provide operational support.

In the next paper, Sato presented a simulator of a prototype liquid metal fast breeder reactor for operator training. To achieve effective training, it was found necessary to provide adequate accuracy in the simulation of the plant from cold start-up conditions up to the rated power output, especially w.r.t. the response time to operator actions and fault propagation. The simulator features different simulation modes (freeze, slow motion, speed-up, restart, step-back). The structure of the simulation model is outlined and the computing facilities are described.

Questions were posed regarding the function of the optional voice simulator. The author stated that voice simulators were already used in fossile power plants to establish efficient training schemes, by issuing operating instructions and trainer announcements. To the questions, if the total loss of electrical power is included in the simulation, and if the console is identical to the one in the plant, the author replied that the total electrical power loss was not yet simulated; the panel arrangement of the plant is still in the design stage, but the consoles will be identical.

The authors of the third paper were unable to attend the meeting. The paper was presented at the meeting as a written contribution.

Kawashima reported on the training experience gained in the BWR Training Center Fukushima - Ken, Japan. The trainees (over 400) included operators, supervisors, plant test engineers and designers from several plants. First, the training programs were described. They include programs for standard and intensive operator training, operator retraining and special advanced class operator training for trainees already working as operators, and family training for shift operator teams. Then, the training simulator features were outlined, stressing the wide range of malfunctions and multiple failures which can be simulated.

In the interchange with the audience, the speaker stated that Toshiba is in charge of the training center; the necessity for governmental examinations is being discussed, especially for senior operators; the training staff includes 29 persons, including 8 instructors and technicians; no difficulties were encountered up to now w.r.t differences between the design and control room layout of plant and simulator, since such differences are small.

The last presentation of the session by Green gave an overview of the Operator Training Facilities for C.E.G.B. Advanced Gas Cooled Reactors. The speaker stated that the necessity of improved operator training was recognized in the UK early after the Windscale incident. He continued with a description of the

training facilities. Three control desks which correspond to the desks of the three power stations involved are installed. The desks are linked to a computer through CAMAC interfaces. The training programs were outlined. As a suggestion for future control desk design, the speaker advocated increased parallel information display, suggesting a wall display of the whole plant instead of the restricted CRT diagrams.

The main themes of the animated discussion following this presentation are rendered by question and answer:

Q: How is the simulator kept up to date with plant changes?
How is the decision made as to what plant states are abnormal?
How is the feedback from the plant?

A: The training center is in personal contact with the three stations involved. Hardware changes are easy to introduce, the software and its checking present more difficulties. Abnormal states are defined according to the Plant Safety Report Incidents. Feedback from the plants is obtained by recruiting the Training Staff from people who have operated the plant.

Q: How about the alarm presentation and the reduction of alarms?

A: There is a danger of too much processing in the machine and too little information to the operator, especially in unforeseen situations when the alarm analysis might fail.

Q: Has the concept of a centralized training school been successful?

A: For initial training and in the given situation with similar plants, yes. If the number of sites is small with many plants at each site, local refreshing training might be better.

Q: Why display the whole plant if many detailed diagrams are available on CRT's?

A: A complete mimic may have advantages in team training, to provide information for more than one operator.

Q: Does a statistic of the quality of handling abnormal events exist?

A: There is not much statistical information. Also, the design of operational procedures may be wrong even if the operator performs correctly.

Q: Is an objective evaluation of operator performance possible?

A: An objective evaluation could only be attempted for some specific situations.

Q: Over the years, much information has been collected on operator response. Has the analysis thereof been considered?

A: No. Difficulties will arise since operators don't broadcast minor errors.

Q: Incidents may develop out of multiple minor accidents. Does the simulator represent the plant with the necessary accuracy to model such events?

A: The scope of the simulator is too restricted to account for these events.

Q: Since the operator is finally responsible, the judging capability should be trained.

A: The training is directed towards a thorough understanding of the plant, rather than towards check list procedures. This is most important in unforeseen situations.

G. Vaccarino

ON THE DESIGN OF THE PEC REACTOR TRAINING SIMULATOR

ON THE DESIGN OF THE PEC REACTOR TRAINING SIMULATOR

Giuseppe Vaccarino (+)

Comitato Nazionale per l'Energia Nucleare - D.R.V. BOLOGNA - ITALY

Synopsis

A summarized description of the PEC simulator, designed for operators' training and operational support, is given. The design choices as a result of the training and operational support requirements are discussed.

1. The PEC Reactor (1)

Pec is a 118 Mwt sodium cooled fast test reactor. The power produced in the core is lost in the air through a two loops sodium system whose final elements are sodium-air heat exchangers.(Fig.1)

A test facility - a 3 Mwt loop thermally and hydraulically insulated from the driver region - is installed in the core center. It contains a special fuel element whose power is lost in the air by a cooling system similar to the reactor one, but independent from it.(Fig.2)

The main purpose of the PEC reactor is to study the behaviour of fuel elements for fast reactor in thermal and neutronic conditions similar to those expected for commercial-size power fast reactors.

2. Simulator Functions

The PEC training simulator is one of the facilities devoted to training and operation support of the plant.

Its functions are the following: (2),(5),(6)

1. operator training, including response to plant faults;
2. development of operational procedures, particularly during plant operation;
3. test and development of data acquisition procedures;
4. test of changes of plant control schemes.

These functions have been defined on the basis of the plant operating requirements, its operation programme and the operation experience of simulators in similar power and research plants (3).

It is foreseen that only the first two years of the simulator life will be devoted mainly to training, whereas functions 2 and

(+) The author presently works as Sales Manager at SEL COMPUTER S.p.A.-Italy
Via Meravigli 12 - MILANO

3 will have a prominent role in the whole plant life (20 years).

Owing to the PEC exploitation programme, reactor operation is expected to be flexible; thus, operational procedures will change in the course of plant life according to the advances in fast reactor technology and related experimental requirements.

3. System Configuration (3)

To perform the functions listed at point 2, the simulator must duplicate the control room and simulate the reactor behaviour in order to supply the operators with the same responses as in the real plant.

The simulator is composed by four basic units linked as in the scheme of Fig.3.

- Operator's desk
- Instructor's desk
- Plant model and simulation computer
- Process computer

The radial structure has been chosen in order to get enough flexibility and simplicity in terms of information exchanges among different parts, and to make possible both the replacement of the different units and the simulator operation even without one unit.

The process computer is an independent unit and it is not integrated in the model computer.

3.1 Operator's Desk

The operator's desk is a full scale replica of the plant console. Its purpose is to put the operator in the same situations he faces during the real plant operation. It's equipped with all the instruments required for surveilling plant behaviour and with the controls for reactor operation.

The operator's desk is composed by main parts (Fig. 4):

- a) meters and controls for the nuclear part ;
- b) meters and controls for the reactor cooling loops;
- c) meters and controls for the test loop and the emergency cooling system;
- d) displays and conversational systems for the process computer.

3.2 Instructor's Desk

The instructor's desk is a free standing unit; it houses all the information systems and controls to enable the instructor to perform his functions ergonomically (Fig. 5).

The main instructor's functions, considered for the desk design, are: (3)

Exercise control : it allows the instructor to select the operating modes and to set the initial conditions and the operational constants for the simulation exercise.

Exercise Monitoring and Recording: the instructor can monitor the behaviour of the simulated plant in its response to the controls exercised by the operator stationed at the operator's desk.

He can also record plant variables from the simulated process for on/off-line processing. All the instructor's actions affecting the simulation, are recorded on a logging printer.

Performance Interaction: by means of CRT displays and coordinated computer programs the instructor can interact with the plant model to simulate fault conditions, control the state and level of ancillary signals, check and change any model variable.

The instructor can perform these functions through a set of controls grouped in a keyboard which is part of the instructor desk:

- a) Simulation control mode
- b) CRT display control
- c) Fault control
- d) Graph plotting controls.
- e) Variable storage and printer/plotter control
- f) Exercise record/replay control
- g) Fault sequence generation control

Each function is supported by a suitable software to enable the instructor to perform his actions and record them. A detailed description of the simulation control mode follows as an example of the instructor's function available. A group of three controls is available for Simulation Control Mode.

The main modes of simulator operation are "run" and "freeze".

In the "run" mode all the systems of the simulator are operational.

In the "freeze" mode all the calculation of the model equations are suspended and all the variables generated by the model are held at the values achieved when the "freeze"

state was selected.

The instructor can store the plant conditions achieved, or set different initial conditions to start a new simulation run.

In the "run" mode the instructor can select a "partial freezing" affecting some selected variables, in order to simulate mal functions or set special training situation.

3.3 Reactor Model

The reactor model is represented by a digital computer program which is able to react to commands coming from the instructor's and operator's desks. It must run in real time and its response must be similar to that of the real plant, within the defined accuracy limits. (6).

The model features has been chosen to get a wide and usefull exploitation of the simulator and to satisfy the training performances required.

The range of validity of the plant simulation is wide enough to evaluate the training performances even beyond the normal range of operation.

The accuracy of the simulation will allow the operator to get the true feeling of the real plant; it also ensures the fulfillment of all the functions defined in section 2.

The computing algorithms have been studied to get accurate and numerically stable results in real time.

They must also suit the performance targets based on an highly detailed reference model within a narrow range.

The model must be structured in order to allow the user to introduce the plant design modification easily, to test design changes in plant systems and operation, and to introduce new malfunctions.

To get these goals, the model design has been based on the following points:

The programming language used is a Fortran version optimized for real time use (e.g. SEL FORTRAN IV Extended).

The model has a modular structure; each model corresponding to a plant system or process is independent and connected to the main program through a suitable connection module.

The mathematical model is derived from the phisycal laws and its wide range of validity has been obtained adjusting the phisycal approach to the changing system conditions.

A set of model initial conditions are stored in the computer.

Initial conditions can be got either as final results of simulation runs (see "freeze" mode) or computed off-line through a suitable software and stored in a mass memory device.

An additional set of features has been incorporated in the model to enable the instructor to implement the action defined in Section 3.2.

The Instructor can access to any computer core location to read and/or change its content.

He can define groups of variables for recording, its form (on/off line, printout, graph, plotter) and parameters (start and stop time, frequency, etc.); a further group of variables can be selected for continuous display on the instructor desk CRT.

The model characteristics have been decided on the basis of the main simulator requirements.

In fact, the simulator will be operated for a quite long period, and mainly devoted to the design and analysis of plant operation and data acquisition procedures.

Therefore the software - its cost is about 60% of the whole simulator one - must be flexible and easy to modify.

The use of fortran in place of assembler and the modular structure allow an economic software maintenance by the user and possibility to update software and follow the changing plant situation without intervention of manufacturer's specialists.

Most of the users will be engineers and technicians without specific competence in computers; thus, all the design problems were solved from an engineering point of view rather than from a computer point of view.

A special effort has been done in the model specification to give to the instructor the maximum intervention capability on the simulator operation.

In fact, I believe that the simulator features, which are available for the instructor, play an important role either in the simulator, itself, either in suiting it to the specific plant, which the simulator has been constructed for.

3.4 Simulation Computer

The computer complex represents a key component of a simulator as its performances greatly affect the feasibility of the functional performances for the simulator system.

The main requirements for simulation computers are (4):

- Great computing power and high speed
- Memory capacity and expandibility
- Powerfull I/O for easy and fast communication with the operators and other equipments.
- Peripheral range for task required
- Available software (possibly application oriented)
- Service and support capability.

On the basis of the above mentioned characteristics a questionnaire was set and some computer models were selected. Benchmarks test were run to evaluate their performances for our particular application.

The final choice was for SEL 32/75 (Fig.6) which appeared to suit optimally our requirements.

A particular good evaluation got its powerfull and fast CPU, I/O structure, memory expansion capability and the R.T. oriented software.

After the choice extensive dedicated tests were made on SEL facility in Milan to get real performances and memory occupation for both computing and simulator management tasks in order to asses memory size requirements and CPU load for our project.

Tests confirmed our provisional evaluation on computer performances particularly for CPU and software.

3.5. Process computer

The process computer is a FOXBORO, FOX 2/30, with the configuration shown in Table 1. (7).

The computer performs several functions as data acquisition, alarms management, guidance in practical operation during start-up, shut-down and other plant transients, and off-line data processing whereas it does not perform any direct action on the process (DDC) due to safety reasons.

These functions are performed by the FOX 2/30 by means of its standard package for process control, IMPAC (Industrial Multi level Process Analysis and Control); it allows an easy and quick management of the process I/O and the execution of most of the required processing.

In other simulators the process computer has been simulated with a program allocated in the same computer used for the plant model. We chose a solution with two separate computers, because we thought to get a better experience in data acquisition problems in this way. In fact, with our radial configuration the computer receives the same signals reaching the operator's desk; these signals are similar to the real plant ones, within the accuracy limits.

Furthermore, we think this solution enables us to evaluate the adaptability of a general purpose process control package, as Impac, to the particular problems of a fast nuclear reactor.

4. Conclusion

The only purpose of this description was to present the results of the studies made during the simulator design.

We wish to stress that our simulator, due both to the peculiar reactor characteristics and its functions is different from most simulators presently in operation.

Particularly, with respect to the more immediate comparison with other power reactor simulators (for PWRs or BWRs), the PEC simulator is different, because it's quite likely that the plant and operating procedures in particular, will be modified during the plant life. Thus, the simulator should fit these changes and support this activity as a dynamic facility for the optimization of such changes.

This is the reason of most of the decisions about the model; they should ensure a very flexible and easy to modify simulator in all its parts.

Furthermore we wish to remind that a further target of the simulator implementation (besides the ones mentioned in point 2), is to qualify engineers in simulator technology (real-time simulation and programming, etc.) and in related fields as data acquisition, electronics, desk design, etc.

This last point has been taken in to account when we decided to adopt some solutions as, e.g., system structure, process computer type and configuration, operator desk and related systems implementation.

Table 1 - FOX 2/30 system configuration for PEC simulator

- CPU: DEC PDP-11/20 type with a 24 K word core memory and 16 bits/word.
- Mass memory: Drum, 991 K words, 87 milliseconds average access time, 118.200 word/second nominal transfer rate.
- H.S.P.T.R.: speed 300 character per second.
- H.S.P.T.P.: speed 60 character per second.
- System teletype: Teletype mod. ASR 35.
- Line printer: 132 characters/line, 8000 characters/minute.
- 2 - 12" CRT with alphanumeric keyboard, 24 lines, 80 characters/line
- 2 - 24" CRT, 24 lines, 80 characters/line.
- 224 analog inputs, 8 used for reference voltages.
- 12 analog outputs.
- 240 digital inputs.
- 48 digital outputs.

References:

1. Soc. NIRA - Reattore Veloce Prova Elementi Combustibile
PEC - Progetto d'Insieme - Genova 1975
2. G. VACCARINO- Specifiche del simulatore di addestramento del
PEC - CNEN Internal Doc. (1979)
3. G. VACCARINO- Specifiche della consolle di istruttore del si-
mulatore di addestramento del PEC - CNEN Inter-
nal Doc. (1979)
4. G. VACCARINO- Computer Characteristics for PEC reactor simula-
tor - CNEN Internal Doc. (1978)
5. C.H. ARTHORNE
ET ALT. The specification, implementation and use of
PFR simulator BNS Int. Conf. on fast reactor
power station - London 1974
6. E. TURRINI- Power Plant training simulator - EAI Internal
Doc. (1975)
7. FOXBORO - Fox 2/30 System equipment overview - AB 73 002GT
The Foxboro Company, 1975

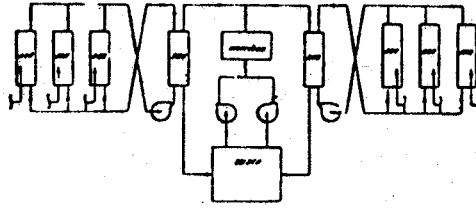


Fig.1-PEC reactor cooling system

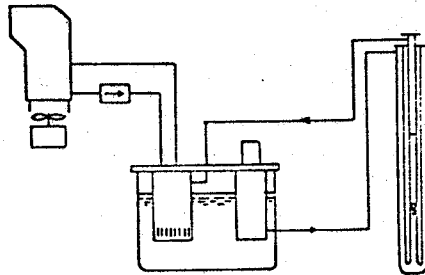


Fig.2- Test loop scheme

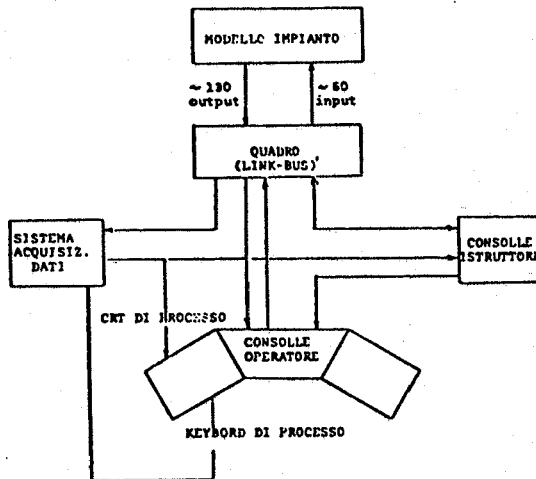


Fig.3- Simulator configuration



Fig.4. Operator's consolle

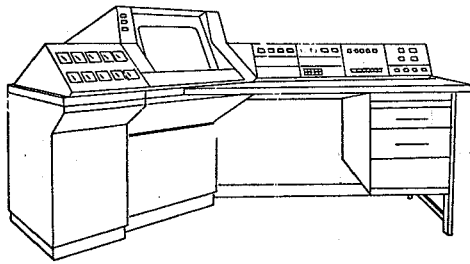


Fig.5. Instructor's desk

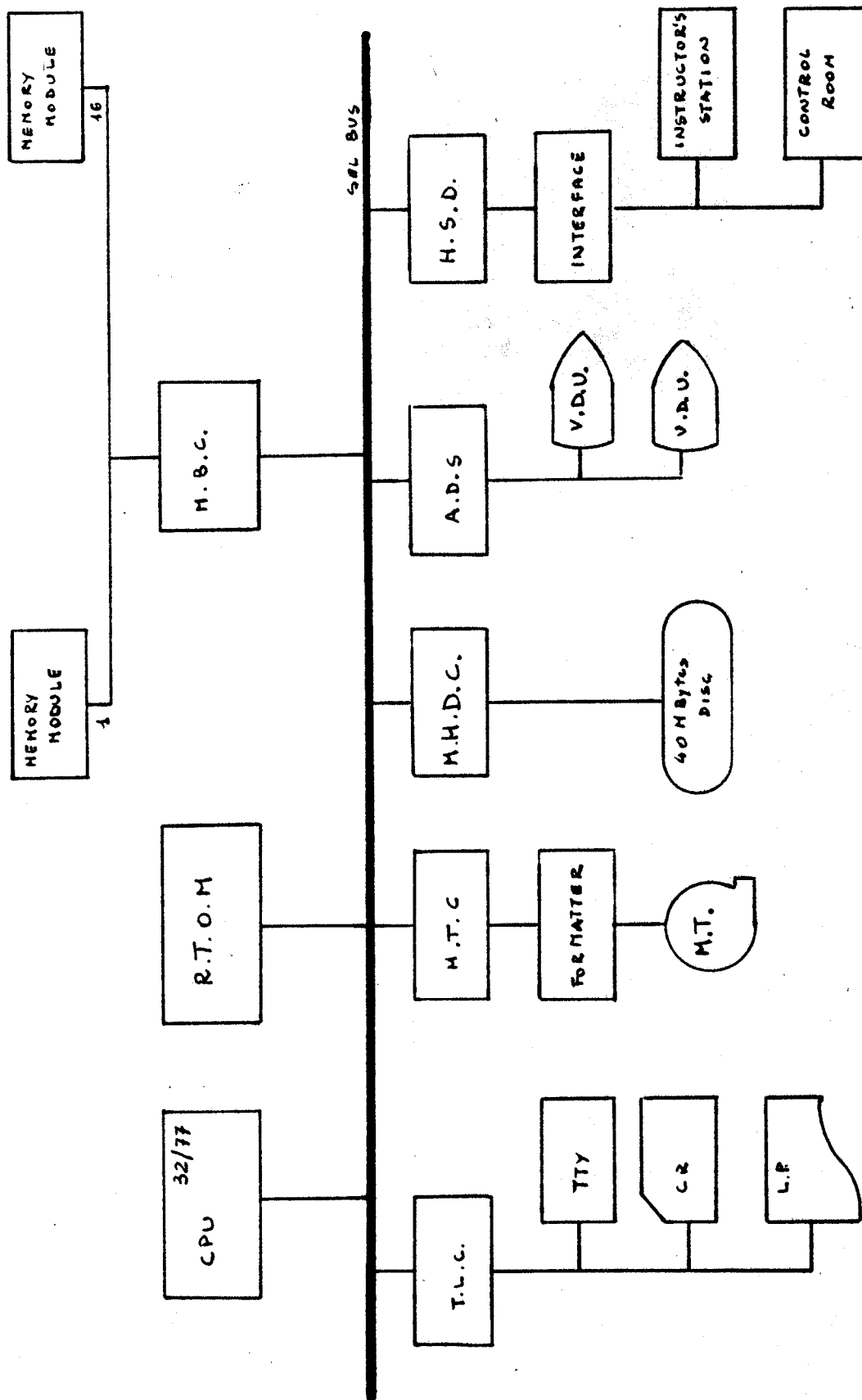


Fig.6 - SEL 32/77 computer complex for PEC reactor simulator

A. Kameda, M. Sato, T. Sato, M. Sakuragi
EVALUATION OF LIQUID METAL FAST BREEDER REACTOR OPERATOR
TRAINING SIMULATOR

IAEA/NPPCI Specialists' Meeting on Procedures and Systems for
Assisting an Operator During Normal and Anomalous Nuclear Plant
Operation Situations, Munich, Federal Republic of Germany, 5-7
December 1979

Evaluation of Liquid Metal Fast Breeder
Reactor Operator Training Simulator*

- A. KAMEDA, Advanced Reactor Engineering Department, Toshiba Corp.
- M. SATO, Advanced Reactor Engineering Department, Toshiba Corp.
- T. SATO, Fuchu Works, Toshiba Corp.
- M. SAKURAGI, NAIG Nuclear Research Laboratory, Nippon Atomic
Industry Group Co., Ltd.

* This work was performed under contracts between Power
Reactor and Nuclear Fuel Development Corporation and
Toshiba Corporation.

Abstract

Generally, the simulator can be classified according to its use as follows; operator training simulator, plant dynamics analyzing simulator, operating procedure evaluating simulator, plant designing simulator, etc..

Our study on simulator is aimed mainly for operator training.

As plant operation should be performed safely and efficiently, it is necessary for operator to train the plant operations that involve not only normal case but also abnormal case, and to improve his knowledge about the plant operation. For this purpose, the training simulator is the best tool to train the operator.

Based on the requirement described above, we have studied following items.

- 1) Evaluation of the general specification for the training simulator.
- 2) Evaluation of the simulation models.
- 3) Verification of the simulation models (dynamic models).
- 4) Evaluation of the equipments for the training simulator.
- 5) Investigation of the preceeded simulators.
- 6) Evaluation of the development schedule for this training simulator.

As the evaluation of the general specification for the training simulator, we evaluated the simulation range for each system and equipment. And the function for the training simulator was also evaluated. Such functions are consisted of freeze, slow motion, step back, start-up at appropriate modes, and malfunction, etc..

As for the evaluation of the simulation models, we evaluated the relation of the dynamic models and logic models.

As for verification of the simulation models, we improved plant dynamic analysis codes to be available in real time use.

As for the evaluation of the equipment for the training simulator process computer, control panels, instructor console and other components are evaluated. We have considered the computer system to be composed by the digital system. However hybrid system was also evaluated in comparison with digital system.

1. Introduction

The use of full scale LMFBR nuclear power plant simulators to train operators was attempted and has been built in some countries.

The need for large scale training simulators has been stressed along with construction of an increasing number of practical scale nuclear power plants and growing concern for the safety factors surrounding such plants. Especially for LMFBR, because of more systems and components than other reactor plants, operating procedures are complicated.

Our study on simulator is aimed mainly for operator training of Prototype LMFBR.

As plant operation should be performed safely and efficiently, it is necessary for the operators to train the plant operations which should involve not only normal conditions but also abnormal conditions, and to improve operator's knowledge about the plant operation. For this purpose, the training simulator is the best tool to train the operator especially for LMFBR plants.

2. Specification

2.1 Use of the simulator

The objectives of the LMFBR simulator are:

- (1) To train plant operators made familiar with the control, display, and alarm systems and not to make them misoperation and led to plant abnormal transients.
- (2) To provide an opportunity for operators to practice avoiding and recovering from fault situations.
- (3) To co-ordinate and evaluate proposed operational procedures and to check revised instrumentation and control systems.
- (4) To analyse plant incidents and check out the modified operational procedures.

And, in order to achieve above objectives, the following requirements are necessary.

- (1) The external appearance of the control console is designed identical with that of the referred plant's control console so as to exploit the training effect fully.
- (2) To make the simulator for training in operation capable of providing training with the same operating sense as the real plant, the contents and accuracy of the simulation model must be adequate, and the time from the control console operation to the responses of the equipment must be identical with the real plant within the range permissible as human sense.

Also, in order to exploit the training effect fully, the following functions are necessary.

- (3) Freeze operation
Ability to stop simulation at any time so an operator can see a transient or plant condition as it exists on all controls and indications.
- (4) Slow-motion operation

- (5) Restart at new operating conditions
Ability to start simulation at one of several plant state points.
- (6) Step-back operation
Ability to return the simulator to the conditions which existed at a previous point.
- (7) Initiate malfunctions.

2.2 Simulation range

While the simulation range must be compatible with the purpose of training, it is also necessary to make adequate study of the means of making best use of the features of the system used. For example, abridging of portions that are not necessarily important for training allows up levelling of the precession of simulation for the important parts. The basic simulation ranges of this simulator include the following.

- (1) With this simulator, training not only in regular operation of the plant but also in starting from the cold state and operation up to the rated output as well as in the shutdown of the plant can be provided.
- (2) The principal processing value of the plant is indicated and recorded by using the control panel identical with the real one. Also with respect to various protective functions, the equipments identical with that of the referred plant are simulated. When anything goes wrong alarm is annunciated, and the various protective functions are activated.
- (3) In case the operator executes an erroneous or abnormal operation, fault develops with the plant as in the real plant and the meters and alarm are activated.
- (4) Training in proper measures against erroneous operation and trouble that are likely to take place in the real equipment is to be made possible.

Fig. 1 displays the typical plant operation cycle and plant flow diagram of the model plant to which the operator must familiar.

The main process variables at the plant normal typical start-up schedules are shown in Fig. 2.

In this model plant, the operation blocks are divided into 1 to 15 as shown in Fig. 3 and 15 to 27 in the plant normal shutdown operation.

For the training of the plant fault condition, proposal events of plant accidents are considered as shown in Table 1 which led to the reactor trip. And, in this case, the operation blocks are divided into 28 to 35.

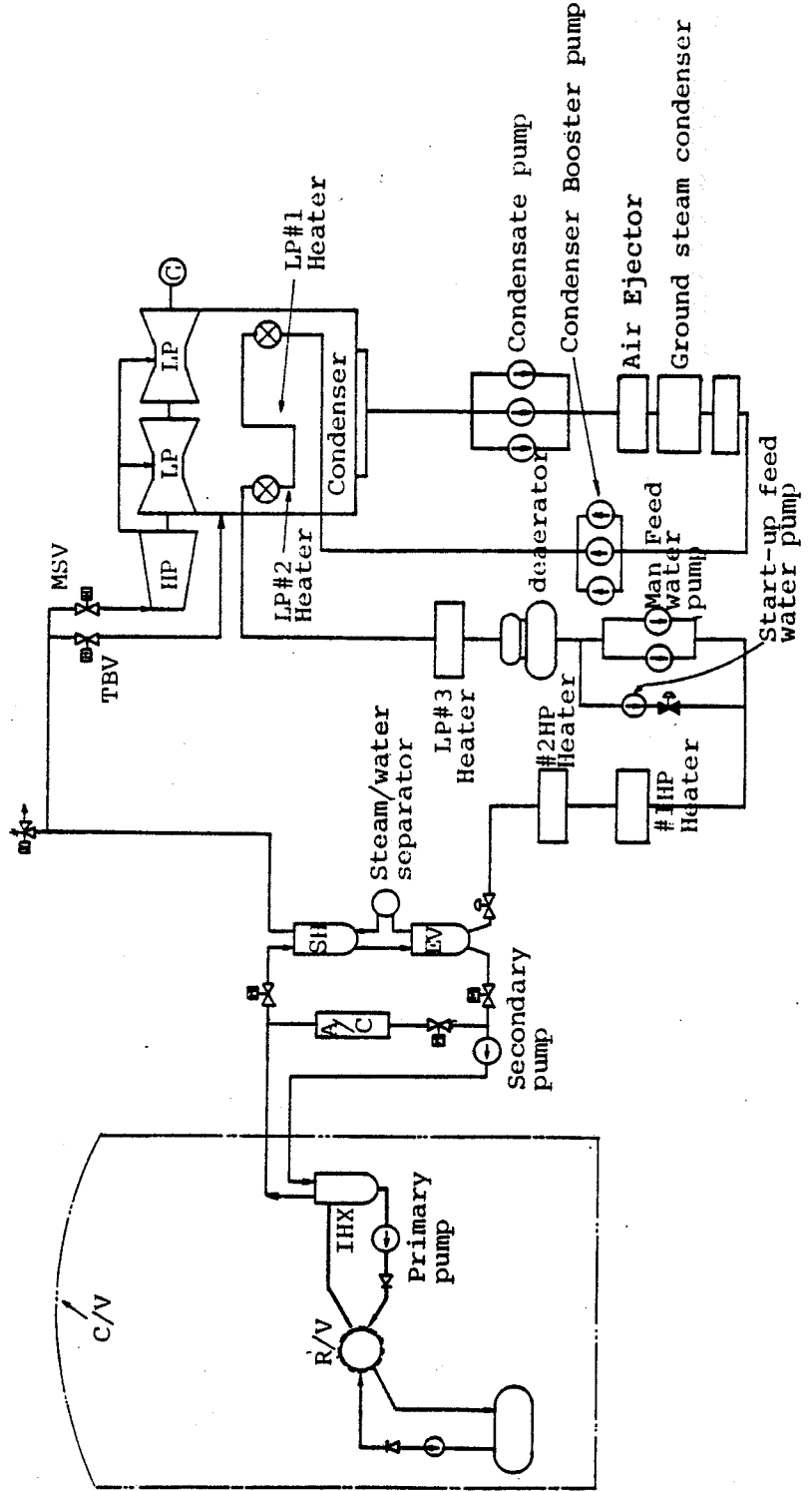
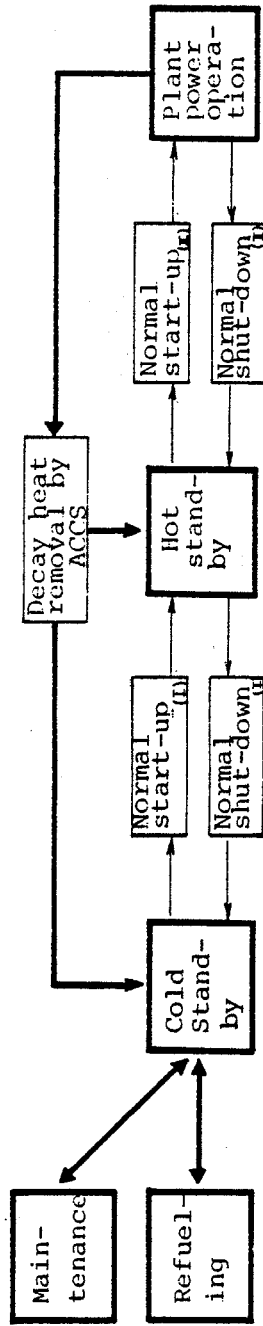
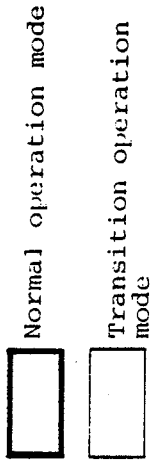


Fig. 1 Plant operation cycle and plant flow diagram

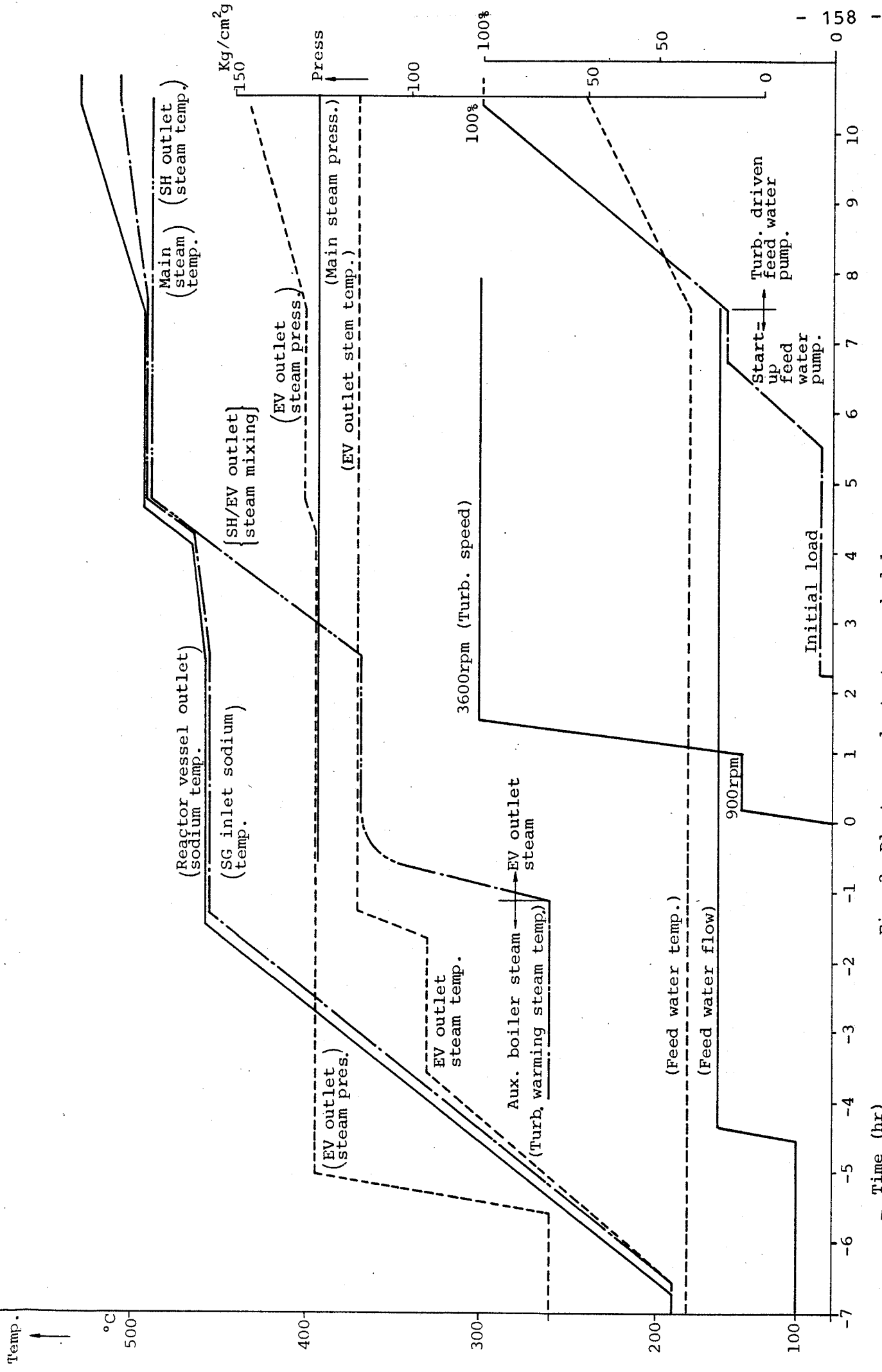


Fig. 2 Plant normal start up schedule

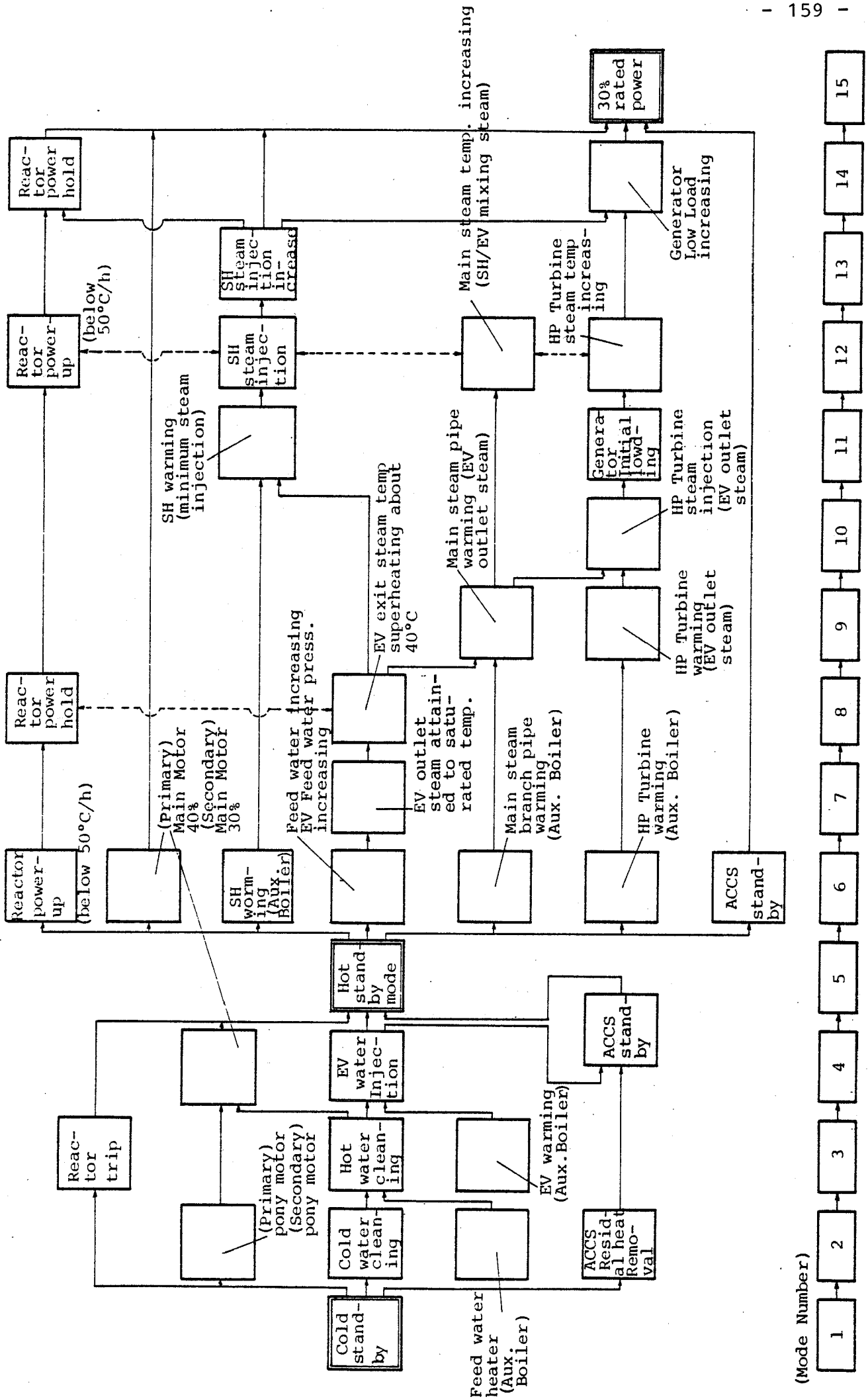


Fig. 3 Plant normal start up operation block

Table 1 Proposal events of plant accidents

No.	plant fault	No.	Plant fault
1	Reactor manual trip	20	Steam system safety valve open
2	Primary pump failure	21	Primary pump stick
3	Secondary pump failure	22	Secondary pump stick
4	Primary flow control failure	23	Main feed water pump stick
5	Secondary flow control failure	24	SG heater tube break
6	Control rod drop	25	Air cooler outlet sodium stop valve open
7	Control rod withdrawal (power operation.)	26	Main feed water pipe break
8	Control rod withdrawal (start-up)	27	EV inlet water pipe break
9	Turbine trip	28	Main steam pipe break
10	SG-Sodium stop valve open	29	SH outlet steam pipe break
11	Feed water control valve closing	30	Primary pipe break
12	SH inlet steam stop valve closing	31	Secondary pipe break
13	Main feed water pump trip	32	Loss of Normal on site power
14	Air-Cooler outlet sodium control valve closing	33	Loss of off-site power
15	SG heater tube small leak		
16	SH relief system misoperation		
17	Feed water control valve open		
18	Feed water pump speed control sys. failure		
19	Main steam magnetic relief valve open		

3. Simulation model

3.1 Software composition

Simulation models are generally divided into two parts such as Dynamic models and Logic model. As the simulator must be identical with the real plant within the range permissible as human sense, contradictory requirements; repletion of the substance of simulation and assurance of real time response, have been studied. In the software composition, function supervisory program for controlling the real time of simulation program has been provided, and the simulation programs are allocated to the basic packages, "Fast", "Medium" and "Slow". Fast is a simulation model requiring very fast response and process input-output routine and is executed once in about 500 msec.

Simulation programs other than those calculated with Fast are known as Medium and Slow, and are executed once in about 1 to 2 sec, and 5 sec, respectively.

The conceptual dynamic and logic models for this simulator are shown in Fig. 4.

3.2 Logic Model

The plant simulation models can be divided into logic models expressing plant interlock as typified by the relay sequence and the dynamic models indicating the nuclear, thermodynamic and hydrodynamic motion characteristics of the nuclear reactor, heat transport system, power generating system and auxiliary systems.

3.3 Dynamic Models

As shown in Fig. 5, the nuclear reactor system, heat transport system, steam generator system, turbine system, generator system, feedwater system, auxiliary system and the emergency system are divided into several small systems in this simulator, and for each system thermal, hydraulic, nuclear and electrical models are prepared.

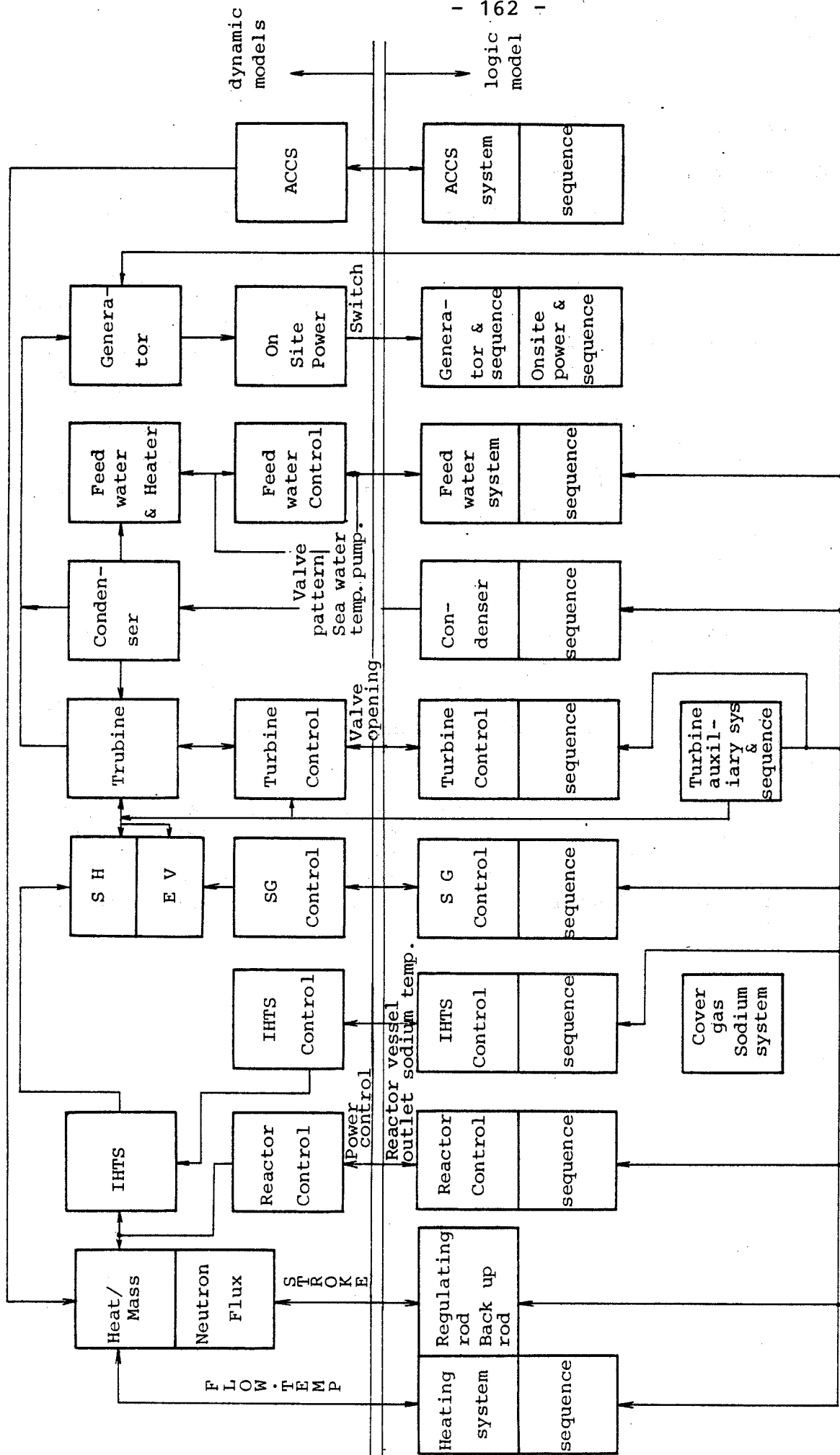


Fig. 4 Conceptual dynamic and logic models

- ϕ : Neutron Flux
- ρ : Control rod reactivity
- τ : Period
- W_1 : Primary sodium flow rate
- W_2 : Secondary sodium flow rate
- W_3 : ACCS sodium flow rate
- W_4 : Main feed water flow rate
- W_5 : Steam flow rate
- T_1 : Reactor vessel sodium level
- T_2 : Primary pump sodium level
- T_3 : Secondary pump sodium level
- T_4 : SH sodium level
- T_5 : EV sodium level
- P_1 : Feed water temp.
- P_2 : Main steam press.
- P_3 : Condenser press.
- T_1 : Reactor vessel outlet sodium temp.
- T_2 : IHX primary outlet sodium temp.
- T_3 : IHX secondary outlet sodium temp.
- T_4 : SH outlet sodium temp.
- T_5 : EV outlet sodium temp.
- T_6 : Feed water temp.
- T_7 : Main steam temp.
- T_8 : LP turbine exhausted steam temp.

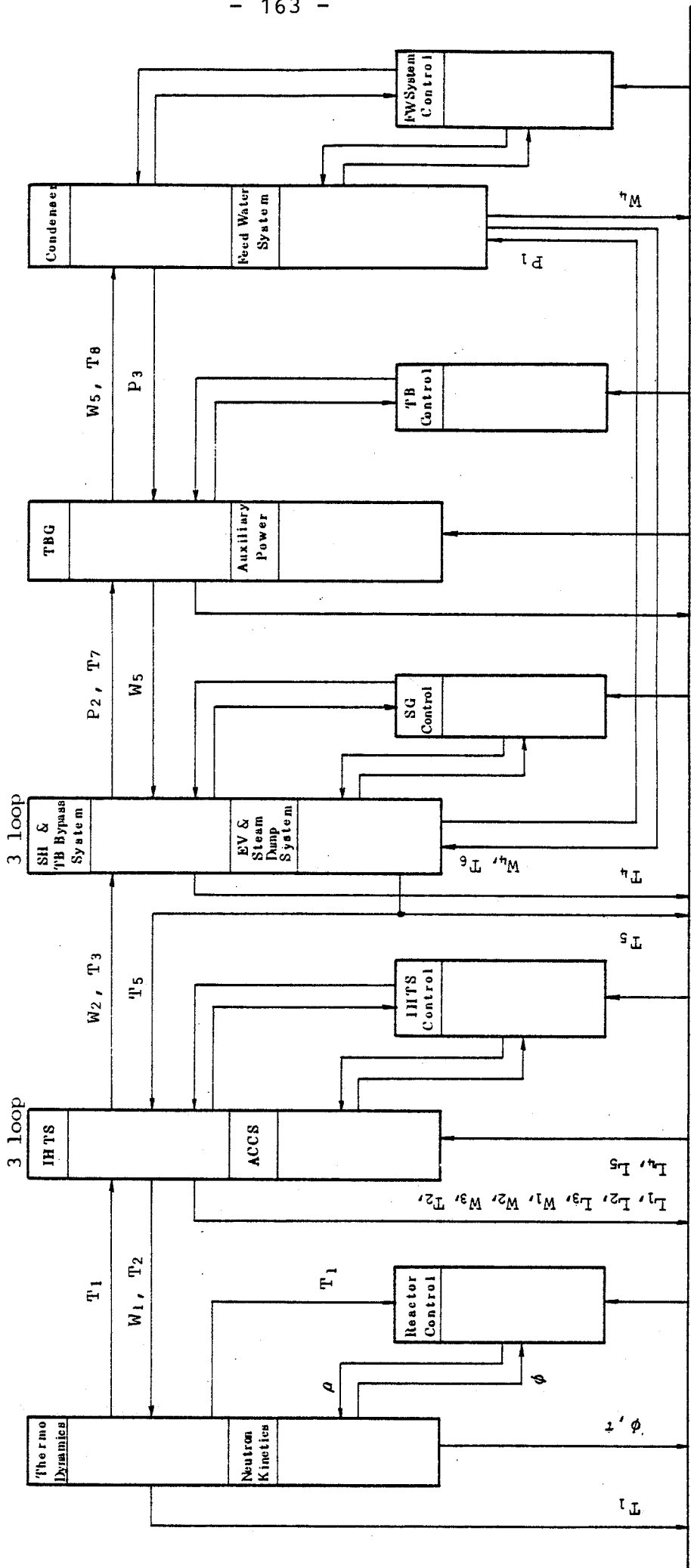


Fig. 5 Conceptual dynamic models

4. System composition

As shown in Fig. 6, this simulator is composed around the control console and the digital computer TOSBAC-7/70.

4.1 Control console

The control console is a bench board type control console for controlling and monitoring the nuclear reactor, heat transport system, steam generators, turbine and generator. It is designed identical in dimensions, coating color, configurations and arrangements of instruments and devices with the referred plant's control console so as to exploit the training effect fully.

4.2 Simulation computer

For the simulation computer, TOSBAC-7/70, a process computer has been considered. The real time response of a simulator is determined by the simulation computer performance and the following have been adopted:

Central Processing Unit

Word length: 32 bits

Core memory: 512KB (128kW)

Execution time (fixed decimal point):

Addition and subtraction: 0.36 μ s

Multiplication: 4.68 μ s

Floating decimal point provided

Disk memory unit

Capacity: 2MB (512K words)

Transfer speed: 625KB/sec

4.3 Instructor's console

This is the console for the instructor and equipped in the control room. This console is provided with selecting switches for the training modes. Selection of the mode in accordance with the training substance and purpose makes it possible to set the control console to the prescribed mode. It is possible to freeze and restart the simulation and also to repeat the same training. It is further capable of generating trouble or abnormal operation from time to time.

5. Conclusion

An outline of the Prototype LMFBR operator training simulator has been presented in the foregoing. It is expected that the simulator will be highly useful in training operators of LMFBR nuclear power plants in not only normal starting and shutdown operations but also in abnormal or troubled operating conditions.

In conclusion, we take this opportunity to express our profound appreciation for the cooperation and guidance provided by the Power Reactor and Nuclear Fuel Development Corp.

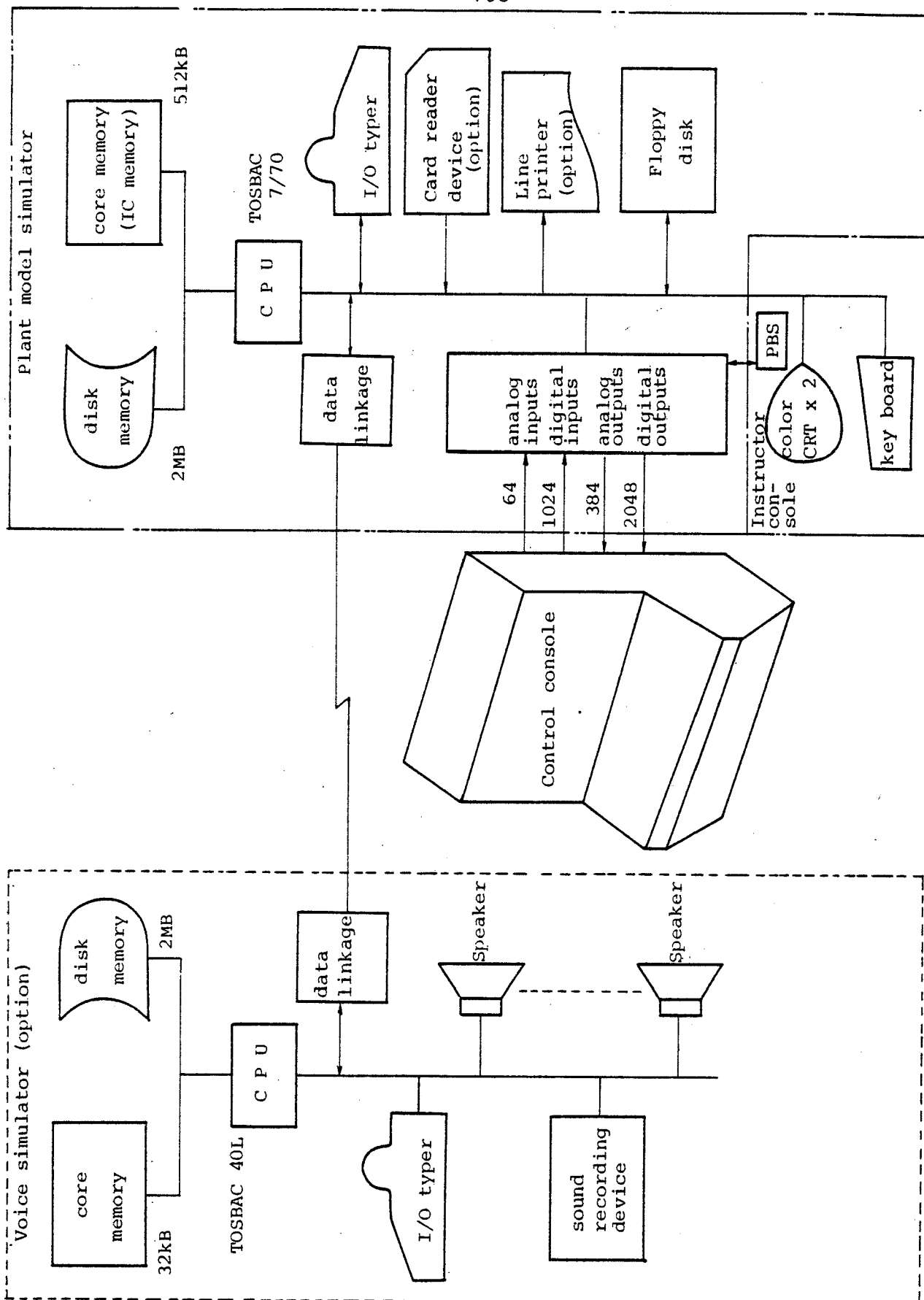


Fig. 6 System configuration of the model plant simulator

C.F. Gnospelius, P.E. Persson, R.I. Carlsson

TRAINING OF POWER PLANT OPERATORS BY THE USE OF A SIMULATOR
CLOSELY REPRODUCING ANOTHER PLANT

IAEA-NPPCI

Specialists meeting

5 – 7 December 1979

Training of Power Plant Operators

by the Use of a Simulator Closely Reproducing Another Plant

Authors:

**Carl F Gnospelius
Per E Persson
Rolf I Carlsson**

**Training of Power Plant Operators by the Use of a Simulator
Closely Reproducing Another Plant**

(1 attachment)

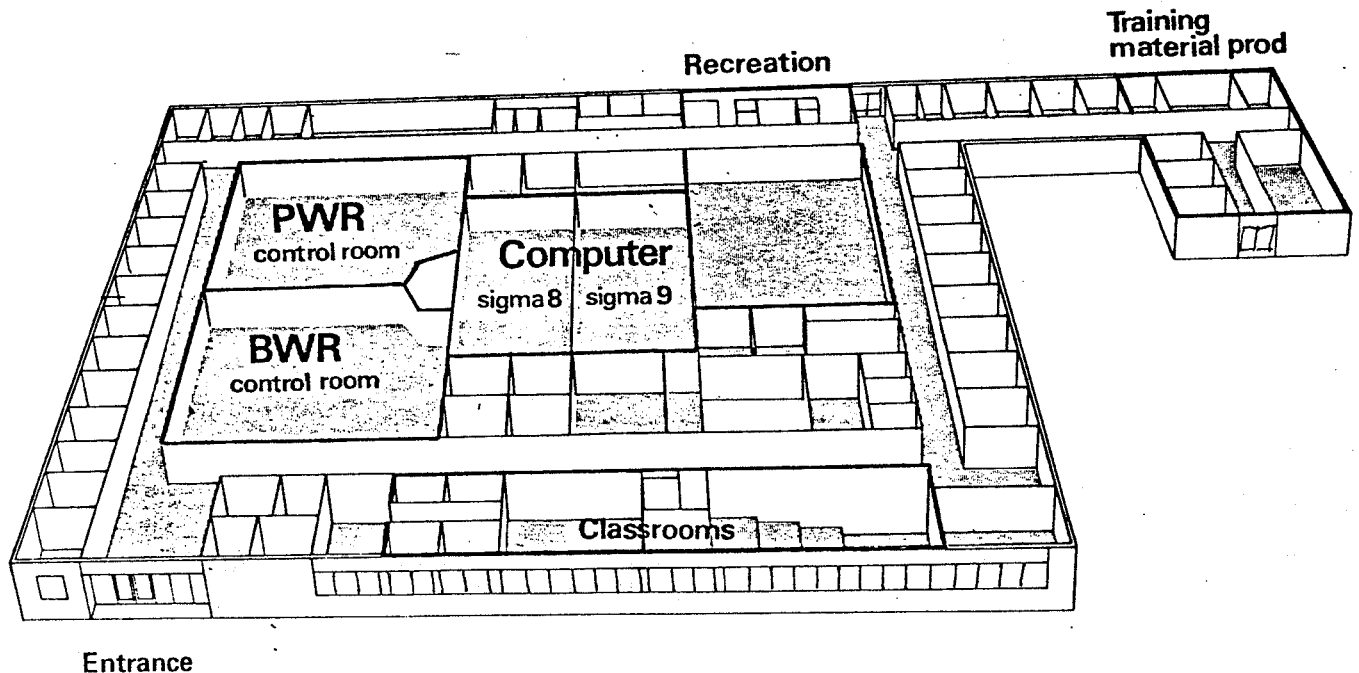
**DESCRIPTION OF THE TRAINING CENTER
(Nuclear Power Training Co).**

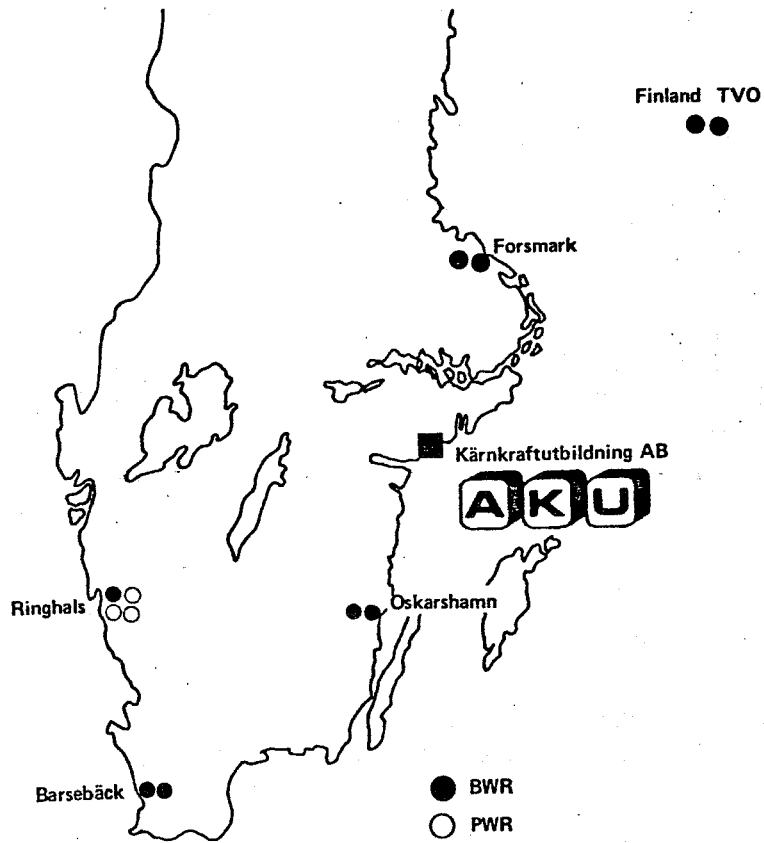
AKU was founded in 1972 by a consortium of the three Swedish utilities owning nuclear power plants. These are the Swedish State Power Board, holding 50% of the shares, Oskarshamn Power Group (OKG) and South Swedish Power Company holding 25% each.

AKU Nuclear Power Training Center is situated in the neighbourhood of the state-owned research station Studsvik 100 kilometers south of Stockholm at the Baltic coast. AKU's first simulator was taken into operation for training in November 1974.

There are now two full scope simulators at the Training Center, one for PWR- and one for BWR- operator training. Both this kind of light water reactors are represented in Scandinavia. AKU is providing training to ten existing light water reactor units in Sweden and also to the two BWR units in Finland.

In the Training Center there are also facilities like class rooms, equipment for the production training materials, and trainee recreation areas.





1979-12-03

DESCRIPTION OF THE SIMULATOR TRAINING

AKU is providing three types of simulator courses

Basic courses (5--6 weeks)
Retraining courses (1 week)
Special courses for nonoperators

Typically, one day consists of five hours at the simulator and three hours of class.

Before taking part in the basic simulator training the operators have had basic nuclear training and power plant technology courses at their own stations.

DIFFERENCES BETWEEN SIMULATOR AND REAL POWER PLANT UNIT

The PWR simulator is an exact copy of Ringhals' unit 3, and thus very similar to the other two PWR units (Ringhals 2 and 4).

The BWR simulator is a copy of Barsebäck 1. This simulator is used for training operators from nine BWR-units with differences compared with the simulator according to the following:

For two units there are no differences.

For one unit there is a very large difference in control room layout and instrumentation but the power plant process systems are identical with Barsebäck 1.

For four units there are some, but not severe, differences in control room layout and instrumentation and in plant design.

For two units, the oldest ones, there are big differences both in layout and instrumentation in the control rooms and in the basic design of the process systems.

There are generic differences in operating procedures and administrative routines between the different power stations as they are operated by different companies. Besides there are differences in language between Sweden and Finland.

1979-12-03

EXAMPLE OF DIFFERENCES

Control room layout

Manual control room switches are placed either in the control boards or in the panels of the cabinets placed behind the control boards. When placed in the control boards there are less possibilities for mimic diagrams according to the smaller surface area. In the modern units push bottom types of controllers and switches are used. Besides, the placing of the different devices in the control rooms differs quite a lot. Also operator aids like sequence of events recording or more or less advanced use of CRTs may differ from one plant to another.

Process system design

Some examples of differences between the simulated power plant and the other power plants are the following:

One turbogenerator compared to two turbogenerators in some units.

Manual control of the turbine compared to automatic control in some units.

One BWR has an emergency cooling condensor.

Later units have a 4-sub-divided electrical system while existing units have a 3-sub-division.

Some units have a steam pressure reducing system for the preheaters.

Different operational data, set point values etc.

Procedures

Operating and emergency procedures are different both principally and also in their layout.

1979-12-03

INVESTIGATION OF TRAINING PROBLEMS CAUSED BY THESE DIFFERENCES

The problems encountered by the operators during simulator training has been relieved through written and verbal enquires at the earlier training courses which were not adjusted to the different power plants but fully devoted towards training on the systems of the simulated unit. Out of this evaluation we found that in basic courses it is possible to go on treating only the simulated systems.

The retraining courses however have to be adjusted towards the operators' own units if there are large differences. We found in the enquires a succesively decreasing motivation of the operators to go to the training center and to learn large parts of another plant. This was especially pronounced when the discussions about licensing of the operators started in Sweden.

Action taken to reduce the problems of training operators from plants with differences.

It was decided to modify the retraining courses into different versions according to the operators' own plants:

Adjust the models and the control room to some extent

Adjust the training documentation

Use the operators' own procedures

Have the instructors study the differences in detail

Use a better pedagogic technique

Unit-tailored training implies that the simulator training is performed at operating modes and with malfunctions which directly can be translated into the operator's own station.

Adjusted s/w and control room

The simulator has been changed to small an extent, thus providing the possibility to use different computer program versions at different retraining courses. For instance, minor modifications have been made in the instrumentation including the exchange of certain setpoints. Besides, the instructor is able to give the operators their own alarm messages on the sequent of event recorder to aid them in taking the correct actions from their own plant's point of view.

All setpoints are shown as colored dots an the instrument scales of the simulator.

1979-12-03

For one of the older units we developed a simulator system version in which the representation of the core instrumentation makes possible the same manual actions during start-up as in the power plant. The ranges of the IRMs in the simulator are also in accordance with the older unit. As there are no automatic turbine supervision in this unit the turbine automatic control of the simulator is operated in manual mode during training of these operators.

Training documentation

The documentation used in the theoretical sessions in classrooms and when following up the malfunction sessions is describing the operators' own station. We also developed a special course book with register, from which the operator very quickly can find the analogue to an alarm of the simulator at his own power plant. There are also descriptions of actions normally taken in their own stations at different alarms of the simulator.

Operating procedures

The operators are using their own procedures "translated" to the corresponding simulated components of the simulator.

Instructors

In order to be able to give lessons to experienced operators about their own plant it is important for the instructors to be very well prepared. Instructors must have been out at the station for a long time (at least six weeks) before the retraining course is developed. At the training center the instructor must have the possibility to study the documentation of the power plant, in order to be fully familiar with each details.

Pedagogic technique

As the control rooms differ significantly it is important to have one instructor among the operators to help them to find and to translate alarms. A second instructor is operating the simulator, is performing local technicians tasks on call from the control room, and is supervising the training from the Instructor's Area.



1979-12-03

THE OUTCOME OF THIS TYPE OF SIMULATOR TRAINING

This type of adjusted simulator retraining has been performed to different degrees over the past year at the training center.

Some current experience is available from a tailored retraining session given to a team of operators which have had no opportunity to get such retraining before. Before going to the Training Center, the operators felt that simulator training was meaningless. These teams have after 6 one-weeks tailored retraining completely changed attitudes and are now very positive to further simulator training.

From the interviews with these operators after the end of the course it was showed that the change in attitude had been caused mainly by the possibility of using their own operating procedures, and of the fact that the theory has been concentrated around their unit. The arrangement with an instructor working with the operator and being able to guide him in his work in an unfamiliar control room has been succesful. The operators have also highly appreciated the changes made in the simulator and in the simulator's control room.

The attached summary of enquires reflects the opinions of the operators after this tailored retraining.

Consequently we will go on making mainly software modifications of the simulator, not only to make the device more realistic, but also in order to make it more similar to the units which are not represented by the original simulator.

REQUIREMENTS OF RESOURCES

In order to tailor simulator courses to different stations the following resources are required.

Programmers and system analysts for modifying the simulator

Instructors with close knowledge both of the simulated power plant and also of the operators own power plant

Teaching materials centered around the operators own power plant

At least two instructors performing the simulator training

We have seen that the personnel resources must be in parity with large effort required to prepare this type of courses. In order to make possible changes of the control rooms, in a simple way, more CRT-screens could be introduced in the simulator control room, for displaying alarms and systems layout representing the operators own power plant.



1979-12-04

Attitude inquiry

Summary of replies to inquiry given to 19 operators from an old BWR unit after having had 1 week of tailored retraining at the B1 simulator.

Have you received any new knowledge during the course about "your" plant?

Yes (19) No (0)

The theory going through "your" plant was

to theoretic (0) (16) (0) to elementary

The modifications made in the simulator refering to "your" plant have

made the (15) (4) (0) had none
training more importance
worth-while

What do you think about the difficulties concerning the adaption from "your" plant to the BWR-simulator's control room at this course compared to earlier retraining courses?

The diffi- (13) (6) (0) No difference
culties have
been reduced

LQn

S. Kawashima

BWR OPERATORS TRAINING EXPERINENCE USING SIMULATOR

IWG/NPPCI SPECIALISTS' MEETING

5-7 December 1979, Munich, Federal Republic of Germany

3. Man-Machine Communication

BWR OPERATORS TRAINING EXPERIENCE USING SIMULATOR

by

Syuzo Kawashima

BWR Operator Training Center, Ltd.

Fukushima-Ken, Japan

ABSTRACT

Since BWR Training Center received it's first class of trainees for Operator Retraining Course in 1974, many trainees including sub-operators, operators and supervisors were given highly abnormal and emergency situations which are not likely to occur in the actual control room.

This paper describes the standard training program established to prepare the operator to be proficient in BWR power plant operation and training experience including an example of the combined troubles.

1. Introduction

An improved and standardized BWR nuclear power plant is now under construction to aim for the security of safety and the furtherance of reliability, based on the accumulated experience of such erection and operation.

The rate of the operation of large-scale nuclear power plants and the supply of such electric power is growing year by year, so that the importance of operator responsibilities at such nuclear power stations is further increasing.

Particularly with an actual example of accident occurrence due to human errors as a turning-point, a strong claim is called for to enrich the operator education and training in Japan as well.

Among the operator trainings, a training course to use a simulator being carried out at the BWR operator training center since 1974, the trainees of more than about 400 have completed the courses of normal and abnormal operations by September, 1979, and are now working at their own BWR nuclear power stations. These trainees include the utility operators, sub-operators, supervisors, and plant test engineers and designers of the plant manufacturers.

The BWR simulator is modeled on the main control room in Fukushima Dai-ichi Nuclear Power Station Unit 3 (784 MWe) of Tokyo Electric Power Company and the training center is located near to the nuclear power station.

This simulation model has been attempted to increase the accuracy by adding periodic improvements on both the software and the hardware in due course of training execution.

Such important systems concerning the operations of simulator control room as the control switches to represent the systems and pictures of the panels are improved to be installed on the back of simulator control panels so as to make it available to grasp the interrelationship among the front panel, back panel and local operations.

As a cooperative operation between the main control room operations and the local operations occupies an important factor in the simulator trainings, a sub-instructor is at present assigned to assume the duties of local operations, based on the experience of initial training methods in which an instructor covers all the responsibilities.

The advantage of executing such training method lies in the point

that the instructor can concretely follow up and advise to such trainees' operations and manipulations as a guidance on their timely operations and manipulations, pointing-out of their maloperations, etc.

An occurrence of abnormal situation in the simulator training course must be designed likely available for the trainees to pursue the causes of such abnormalities, properly to take measures and to maintain the plant at a safety condition.

Particularly, in respect to the response not only to a single failure, but also to the combined malfunctions, it is quite important to verify such on the basis of analytical results and to set up an effective condition in the training.

This paper describes the contents of BWR operator training programs and the training experience including an example of combined malfunctions.

2. BWR Operator Training Programs

With reviews made on the desires and comments given by the trainees' dispatching organizations since the commencement of such trainings in 1974, the training courses as shown in Table I are set up as the BWR operator training programs.

These training courses are the ones extended to coincide with the operator training programs owned by each electric power company, in corresponding to an increase in construction of nuclear power stations and in number of personnel who have an operational experience in such stations.

The standard operator training course is the one of twelve weeks course for the operators at thermal power plants and the employees at other sections in the nuclear power stations than at the control room.

The intensive operator training course is designed for these personnel who have an operational experience at a nuclear power plant to get a qualification to become an operator and centered with the control room operations with lessened hours of the lectures.

The operator retraining course is designed for these personnel who are already working as an operator properly to take actions on an abnormal and emergency situation with which such trainees may seldom experience with the actual reactors.

The specially advanced class operator training course aims to provide a training course for these operators and senior operators who have already completed all the above training courses.

The family training course aims to train a shift operator team to make the team members acquired in a day a necessary theme raised among them.

An examination shall be executed after completion of each of standard, intensive and retraining courses, and the resulting evaluation of each trainee shall be sent to the respective dispatching body.

Table I: BWR Operator Training Programs

Training Course	Description	Training Hour
1. Standard Operator Training (8/class)	Teaches operating skills and techniques necessary to maintain stable operation of nuclear power plant.	12 weeks Control Room Operation: 128 Hours
2. Intensive Operator Training (4/class)	Gives intensive Control Room Operation training to those who already have operation experience in nuclear power plant and its system operation.	3 weeks Control Room Operation: 80 Hours
3. Operator Retraining (4/class)	Gives training in abnormal and emergency situations of nuclear power plant to further upgrade operator's proficiency.	9 days
4. Special Advanced Class Operator Training (1 team/class)	Gives training to advanced class operator on special items.	5 days
5. Family Training (1 team/class)	Provides opportunity for utility operator training requirement.	1 day

2.1 Standard Operator Training Program⁽¹⁾

The standard operator training course is the program of twelve weeks course having been implemented since April, 1974, consisting of the class room lecture, simulator training, actual plant observation and examination.

A number of trainees who have completed this course till today count about 200 persons.

The purpose of this course is that all the trainees shall effectively learn by experience the normal operation, abnormal and emergency operation and BWR operational characteristics by utilizing a simulator and thus attempt to increase their operational techniques and skills.

The major items in this training course are a training of making much of the fundamental manners which should be possessed by a trainee himself of skills in the art as an operator and a training to acquire the applicable actions against an abnormal occurrence. These include such items as a recognition of importance of team work in the operations, operational characteristics of the plant, transient responses, proper judgement on an abnormal occurrence, grasp of correct operation, and the like.

The class room lectures of four weeks comprise of the basic theory for reactor operator, nuclear steam supply system, emergency core cooling system, radiation protection, normal operating procedure, reactor safety analysis and technical specifications.

Each lesson of the lectures is assigned with 2 - 4 hours.

In case that there are some differences between the model plant and the plants at each trainee's dispatching station, such as a complicated system, a comprehensive plant interlock system, --- for examples, condensate and feedwater system, turbine control system, RHR system, operating procedure and others --- a consideration is made for the trainees to be thoroughly familiarized with the model plant very quickly for the sake of receiving a simulator training, by further adding more training hours.

The control room operation (CRO) trainings are emphasized in the simulator trainings and are designed with the aims likely available to make the trainees learned thoroughly all the necessary techniques and skills of the plant operations within a short period of time.

Principally, on the basis of the learnings of normal operation, meanings of procedures, start-up, shutdown and manipulation by a team and the response characteristics of the plant which are all the fundamental matters of the plant operations, it aims to secure the plant safety with some emergency actions by a team.

The instructor and sub-instructor will provide the operational trainings in the control room in the first half of this course to make the trainees acquainted with the model plant to include the normal start-up, shutdown and surveillance tests.

In the next step, all the trainees shall be assigned to the duties of shift supervisor, reactor operator, turbine operator and auxiliary operator and thus the normal operation shall be executed by a team. In such a case, the instructor will generate a malfunction in order to provide trainings on an abnormal operation.

At the end of the normal operation trainings, it is planned that a training of real time start-up operation shall be carried out so as available to make the trainees comprehensively acquired the plant operations.

It takes about 12 hours in this training course from the start-up preparation to the full power operation.

The training hours not assigned to the control room operations can be spent for the actual plant observations and the class room lectures which also provide for the last half part of this course.

An examination on the operational manipulation of the trainees shall be carried out in between the normal operation training and the abnormal operation training to evaluate their rating of progress in learnings.

The abnormal operation trainings include the reactor scram recovery, turbine and generator trip, main steam isolation valve close, feedwater control system trouble and others, while the emergency operation trainings on the pipe rupture.

This training course aims such safety shutdown of having thoroughly been recognized the plant safety as a proper judgement on the plant key parameters, correct manipulations, multi-monitoring of instruments, prompt communications with all the sections involved.

After completion of the abnormal and emergency operation trainings,

a final complete operation training to go over the course thoroughly shall be taken place, in order to supplement the weak points of the trainees.

At the end of this training course, such examinations as in writing, in oral, and on the normal and abnormal operations shall be carried out.

The control room operation trainings of this course are outlined in the attached Table II.

2.2 Intensive Operator Training

The intensive operator training course is implemented since 1978 and designed concentratedly to train on the control room operations these people who have an operational experience and/or an experience of system operation in a nuclear power station.

Four teams of trainees have up to now completed this course.

The duration of this course is three weeks, consisting of the control room operations of 80 hours and the class room lectures of the remaining hours.

The control room operation trainings are condensed with the programs in the standard training course and divided into the normal operation and the abnormal operation trainings.

At the end of the normal operation trainings, an execution of real time start-up operation is planned, which is very reputable among the trainees in terms of a comprehensive experience of the plant operations, as they are unable to have any experience of it with an actual plant.

The class room lectures include the operating procedure, summary of facility description and technical specifications, and in addition, the reviews on the basic theory necessary to the plant operations shall be carried out by using a computer assisted instruction system.

An examination shall be executed on the operational manipulations and in oral, and the result be sent to a respective trainee's dispatching organization.

It takes about four hours in the operations and manipulations examination for three times under such separate theme as the duties of supervisor, reactor operator and turbine operator in regard to the abnormal situation.

The control room operation trainings of this course are outlined in the attached Table III.

2.3 Operator Retraining

The operator retraining course aims to maintain and/or promote the operational techniques and skills by providing a periodic training for these people who are already working as an operator. Basically, the major point lies upon the abnormal operation trainings.

The duration of this course is nine days, consisting of the class room lectures and the control room operation trainings.

The trainees of about 200 persons have up to now completed this course, including such persons who have completed three times in this course held since its commencement in 1974.

The class room lectures include the comprehensive plant interlock system, operating procedure, operating limited conditions, plant transient responses and basic theory.

The control room operation trainings can be divided into such two phases as the normal operation and the abnormal operation trainings.

The normal operation trainings aim to make the trainees thoroughly acquainted with the differences between the model plant and the plants at each trainee's dispatching station, familiarized with the model plant and reviewed the normal operation.

The abnormal operation trainings cover the following items.

- (1) Reactor scram recovery
- (2) Turbine and generator trip
- (3) Reactor scram with main steam isolation valve open and close
- (4) Reactor scram with loss of auxiliary power
- (5) Primary loop recirculation system failure

- (6) Condensate and feedwater system failure including loss of feedwater
- (7) Loss of coolant accident (pipe rupture inside and outside drywell, relief valve stuck open)
- (8) Review of abnormal operation
- (9) Miscellaneous malfunction including limiting condition of operation

2.4 Special Advanced Class Operator Training

This special course is designed for these people who are already working as an operator and have also completed the abovementioned training courses, and/or working as a senior operator.

The duration and programs of this course shall be determined in consulting with the trainees' dispatching organizations, but the abnormal and emergency trainings shall be carried out, particularly centering at the multiple failures, taking the Three Mile Island incident as a turning-point.

This sort of training contains such programs that the emphasis is to be placed upon a proper judgement, command, communication and protective actions upon occurrence of a plant abnormality and emergency to be made by such responsible officers as in the senior operator class.

The duration of this course is determined to be five days, consisting of the class room study of 4 hours a day and the control room operation training of the same hours.

The control room operation trainings shall be carried out to review the normal operation to include the cases under malfunctions and to be related with the abnormal and emergency operations hencefrom.

The abnormal and emergency operation trainings are set to include the following multiple failures.

- (1) Loss of feedwater and relief valve stuck open including HPCI system failure or RCIC system failure
- (2) Loss of coolant inside drywell
- (3) All main steam isolation valve close
- (4) Main steam high radiation
- (5) Seismic trip and loss of auxiliary power

- (6) Review of emergency operation
- (7) Discussion of emergency operation training

2.5 Family Training

The family training course is the one to train a shift operator team in a day and implemented since 1976, whose theme to be learned is not fixed in advanced and shall be determined among the team members then attended.

The major lessons to be learned are to be reviewed on the important operational procedures among the normal operations.

The refreshment course of operators and the same by a team to include sub-operators shall be carried out in respect to the abnormal operations.

3. Training Simulator⁽²⁾

The simulator is modeled on the main control room in Fukushima Dai-ichi Nuclear Power Station Unit 3 (784 MWe) of Tokyo Electric Power Company and simulated available to perform both the normal and abnormal operations.

As an initial operation mode, eighteen kinds of modes can be set up to include a normal start-up, power operation, shutdown and scram recovery.

In regard to the malfunctions to be applied for the abnormal operation trainings, approx. 120 kinds of modes are incorporated in the simulation model. Toshiba process computer, TOSBAC-7000/20, is used as a simulation computer.

The equipment and instruments in the simulator main control room are constituted as follows.

- 1 - Process radiation monitor panel
- 1 - Emergency core cooling system, reactor shutdown control panel
- 1 - Reactor water cleanup system, primary loop recirculation system, RCIC system control panel

- 1 - Reactor control panel
- 1 - Main steam, feedwater, condensate water, circulating water, cooling water system control panel
- 1 - Turbine and generator control panel
- 1 - Electrical system control panel
- 1 - Annunciator auxiliary panel
- 1 - Operator console
- 1 - Typewriter

4. Combination of Malfunctions

Approx. 120 kinds of plant malfunctions are incorporated in the simulator model, and the responses at the occurrence of such malfunctions shall demonstrate good coincidence with the analytical results given through the execution of a large-scale computer with various analytical codes.

Further, a warning alarm can independently be sounded with a generation of plant abnormality.

A setting up of conditions to generate at the same time the multiple failures by combining some of such malfunctions, may become a question in the execution of trainings, unless after completion of verification made on both the analytical results of the plant designs and the responses of simulation model.

Taking the Three Mile Island incident as a turning-point, the importance of trainings on the multiple failures has been recognized, and even though there are plenty of room in which the reviews should be made in respect to the conditional setting up of multiple failures, such trainings shall be carried out with the typical malfunctions shown in the attached Table IV as in the combinations of malfunctions which are available with the current simulation model.

The training programs in case of multiple failures shall differently be arranged, depending upon the trainees' level, experience, simulation range and others, but the major items currently being executed are included in the specially advanced class operator training course.

5. Conclusion

Based on the experience through the training having been executed till today at the BWR training center, the current programs of training courses have been described in this article, as well as the same for multiple failures and the typical malfunctions which generate the multiple failures.

At the age of claiming the completion of operator education and training, it is our aim to make our further increasing efforts to fill up the complete programs of training courses through the experience accumulated till today.

Finally, we would like to express our sincere and deep appreciation to such individuals of each electric power company who have rendered us an ever lasting cooperation and good guidance in respect to the operation of the simulator.

References:

- (1) Syuzo KAWASHIMA, "LWR OPERATORS TRAINING IN JAPAN"
The Second Pacific Basin Conference (Sept. 1978)
Transactions vol. 29, 1978 (pp. 318 - 323)
- (2) Mutsumi ITOH, et al., "Operator Training Simulator for BWR Nuclear Power Plant", Toshiba Review, vol. 29, No. 9, pp. 1006 - 1011 (1973)

Table II: Standard Operator Training Course - Control Room Operation

Normal operation training phase

CRO-1, 2	Startup preparation
CRO-3, 4	Reactor critical approach to reactor pressure 40 kg/cm ²
CRO-5, 6	Reactor pressure 40 kg/cm ² to turbine start
CRO-7, 8	Turbine rated speed to rated power
CRO-9, 10	Plant shutdown (Rated power to shutdown cooling)
CRO-11, 12	Reactor critical approach to reactor pressure 60 kg/cm ²
CRO-13, 14	Reactor pressure 60 kg/cm ² to 20% power
CRO-15, 16	20% reactor power to rated power
CRO-17	Review of normal operation (startup and shutdown)
CRO-18, 19	Real time startup to rated power

———— Half way operation examination

Abnormal and emergency operation training

CRO-20, 21	Reactor scram recovery
CRO-22	Main steam isolation valve close and loss of auxiliary power
CRO-23	Primary loop recirculation system failure and feedwater control system failure
CRO-24	Condensate and feedwater system failure including loss of feedwater
CRO-25	Turbine control system failure
CRO-26	Main steam pipe rupture outside drywell
CRO-27	Loss of coolant accident (pipe rupture inside drywell) ECCS automatic start and core cooling

Final complete operation phase

CRO-28, 29	Review of abnormal and emergency operation
CRO-30 ~ 32	Review of normal operation

Note (1) CRO-11 ~ 19 include the malfunctions.

(2) Surveillance test (Core spray, RHR torus cooling, RCIC, HPCI, Main steam isolation valve and Diesel generator) shall be made during the normal operation phase period.

Table III: Intensive Operator Training Course - Control Room Operation

Normal operation training phase

CRO-1	Startup preparation
CRO-2, 3	Reactor critical approach to reactor pressure 60 kg/cm ²
CRO-4, 5	Reactor pressure 60 kg/cm ² to 20% reactor power

CRO-6, 7 20% reactor power to rated power
CRO-8, 9 Rated power to plant shutdown
CRO-10, 11 Real time startup to rated power

Abnormal and emergency operation training phase

CRO-12 Reactor scram recovery
CRO-13 Main steam isolation valve close and loss of auxiliary power
CRO-14 Primary loop recirculation and feedwater control system failure
CRO-15 Condensate and feedwater system failure
CRO-16 Turbine control system failure
CRO-17 Relief valve stuck open and main steam pipe rupture outside drywell
CRO-18 Loss of coolant (pipe rupture inside drywell)
ECCS automatic start and core cooling

Final complete operation training phase

CRO-19, 20 Review of abnormal operation, and normal operation

Table IV: Typical Malfunction for Combination of Simultaneous Malfunctions

1. ECCS system
 - (1) Relief valve stuck open
 - (2) RHR shutdown cooling system failure
 - 1 - Pump trip and injection valve close
 - 1 - Sea water pump trip
 - (3) HPCI system isolation
 - (4) All main steam isolation valve close
 - (5) RCIC turbine trip
2. Reactor control and protection system
 - (1) Channel-A and B trip
 - (2) Seismic trip
 - (3) CRD pump trip
3. Primary loop recirculation system
 - (1) M-G set A and B trip
 - (2) Control system failure
4. Condensate and feedwater system
 - (1) Condenser vacuum low
 - (2) All feedwater pump trip
 - (3) Condenser hotwell level low (loss of feedwater)
 - (4) Feedwater control valve air fail lock
 - (5) Feedwater control system failure

5. Turbine and generator
 - (1) Turbine trip
 - (2) Generator trip
 - (3) Turbine bypass valve stuck open
 - (4) Turbine control system failure
6. Electrical system
 - (1) Loss of standby auxiliary power
 - (2) Network load loss
 - (3) Auxiliary power transformer failure
 - (4) 1 - Emergency diesel generator failure
7. Pipe rupture and release of radioactive materials
 - (1) Main steam pipe rupture inside and outside drywell
 - (2) Reactor coolant leak inside drywell
 - (3) Main steam high radiation
 - (4) Reactor and turbine building high radiation

J.F. Green, S. Birnie

OPERATOR TRAINING FACILITIES FOR CEGB ADVANCED GAS COOLED
REACTORS

INTERNATIONAL ATOMIC ENERGY AGENCY

SPECIALIST MEETING ON PROCEDURES AND SYSTEMS FOR
ASSISTING THE OPERATOR DURING NORMAL AND ANOMALOUS
NUCLEAR POWER PLANT OPERATION SITUATION.

MUNICH DECEMBER 1979

OPERATOR TRAINING FACILITIES FOR CEGB
ADVANCED GAS COOLED REACTORS.

BY

J.F. GREEN AND S. BIRNIE

SUMMARY

The facilities provided at the Nuclear Power Training Centre of the Central Electricity Generating Board for the training of operators of the Advanced Gas Cooled Reactors are described.

The simulator control desks are replicas of three AGR designs with, in addition, simulation of the Data Processing System for each station.

Three modes of operation are envisaged

- a. Demonstration where the simulator is used by the tutor to illustrate lecture on plant behaviour.
- b. Interaction where the student carries out normal procedures and experiences plant failure situations.
- c. Investigation where engineering staff use the simulator for validation of modified operational procedures, ergonomic studies etc.

INTRODUCTION

The design intentions for the AGR simulator were described at an IAEA specialist meeting held in Studsvik, Sweden in October 1976. (1) This paper updates our thinking and reports progress with the simulator. The simulator consists of replicas of the control desk at three of the CEGB Advanced Gas Cooled Reactors located at Oldbury, near Bristol and a computer model of the plant which runs in the CEGB Computer Centre in London.

SIMULATOR FACILITIES

The five Advanced Gas Cooled Reactor sites that are in operation and under construction in the UK are built by three different consortia. To provide simulator training on these different designs, replicas of the control desks at Hinkley Point, Dungeness B and Hartlepool are installed at the Nuclear Power Training Centre, Oldbury near Bristol. Only one of the three desks can be used for training at any one time as the computing system capacity is not sufficient to drive desks in parallel.

The switches and lamps on the desk are driven by a digital input - output system and the meters, recorders and setting potentiometers by an analogue input - output system. These are standard modules to the CAMAC standard and they provide the interface to the local computer. This is a DEC PDP 11/34 with 128K words of memory and a

Floating Point Processor. In addition to the desk servicing function this computer models the station data processing computer. It provides the alarm display and data formats to the visual display units on the desk. There are four monochrome tubes, three for alphanumeric data and one for alarm messages. In addition, there are four colour tubes which are used to present Graphical and Mimic diagram displays for tutorial purposes.

The status of all switches and other controls on the desk is relayed approximately 3 times per second to the Modelling Computer in London, via two 9600 baud telephone lines which return data on the temperatures, pressures, actuator positions etc. computed for the current time-step. The Modelling Computer is an IBM 370/168 in the Board's Computing Centre. The desk status block also contains the simulator mode control (RUN-HOLD-FREE-INITIALIZE) and the fault insertion data.

The model covers the reactor, either as eight elements or as an average point model, the gas circuit with 4 circulators, two once-through boilers - either modelled as 12 planes or as 4 planes, the steam mains with start-up vessel, Main turbine and Generator, Turbine and Electric Feed pumps and Feed Water regulating system. The plant model also covers the control systems for the plant items listed above. The modules of plant necessary for a particular exercise are selected by the tutor and are linked to give an equation set that can be integrated. The real time integration algorithm is a modified version of Gear's method, a variable step length process with pre-computed Jacobian matrices.

CURRENT STATUS

The programme of functional tests of each component of the system in an integrated fashion has now been completed. The individual items have performed satisfactorily but the response of systems when working together has needed further development.

Dynamic testing of the simulator has been carried out in the ranges from Hot Shutdown to 20MW and 150MW to full power. Computational difficulties with the Once Through Boilers and their feed control systems at low-load have delayed the testing of the intermediate range of Plant Start-up.

Our experience with simulator modelling in a very large computer at a remote site where there is also substantial work load from other computer users is disappointing. The technical problems have, we think, been overcome but human problems in communicating the needs of the simulator staff to the computer operators in London, and securing an adequate diagnostic service when problems occur has contributed to the continuing delays with the project.

Training with this simulator is scheduled to begin in January 1980.

SCHEME OF TRAINING

The staff for the control room at all CEGB nuclear stations is selected from candidates who already possess academic qualifications in engineering of graduate, professional engineer or equivalent level. For staff at the AGR stations there is a combination of courses at the Nuclear Power Training Centre and On Job training.

Firstly, for those without a nuclear background, is an 'Introduction to Nuclear Power' course, which covers Nuclear and Reactor Physics, Heat Transfer, Plant Kinetics, Health Physics, Legislation and Licencing etc. This is followed by a 4 week course on "AGR Technology". This course is for staff from all the AGR stations and is given by engineers from the Design and Construction Division and by Research Officers from the Nuclear Laboratories. All the major plant systems, fuel elements, fuel stringer, moderator, coolant, boilers, control systems, essential supplies systems, the turbine and generator are presented and their design limits and control philosophy are discussed.

During this course the simulator is used in a demonstration mode. The tutor uses the simulator to illustrate features of the plant dynamics that he wishes to emphasise. Particular use is made of the fact that temperature profiles in the reactor and the boilers are available in the computer, whereas the instrumentation of the plant does not provide corresponding data. The principal aim is to enhance the students understanding of the physical processes taking place.

Following a period of plant familiarisation the engineers return to the Centre for an "AGR Operations" course. Each course will be limited to staff from one of the AGR stations and will cover the operational procedures for that station. The students working in groups of two or three will work through the plant start-up and shut-down procedures under the supervision of a tutor. When familiarity with normal plant behaviour has been achieved the tutor will introduce some faults having first discussed the plant response expected with the student. On this course, the simulator is used as the tool for teaching the operator the correct procedures and the reasons why these procedures have been established. By illustrating major faults, we aim to improve his skills in diagnosis of the state of plant.

All operations engineers will return to the Centre at intervals for a revision course. This will, like the operations course, be based on the simulator. Since the students will be familiar with the normal operational procedures, the tutor will introduce instrument and other plant malfunctions during the procedures to exercise the students diagnosis of and response to abnormal situations. It is intended that this course should also include simulation and discussion of a major plant failure such as a loss of coolant accident. One of the most difficult decisions for an operator when faced with a plant malfunction is whether or not he should disengage auto control loops and take control on manual. The simulator enables him to experiment and build up some experience that he could not obtain readily from the plant. The use of the simulator, the investigation mode, has to be

used with caution since operation outside the range where the modelling equations are valid may lead to erroneous results.

CONCLUSION

The AGR simulator system described in this report is now operating in a restricted range. Development work to extend this range and Acceptance tests are still in progress.

Ref 1. Specialist Meeting on Simulators for Training of Nuclear Power Plant Operators and Technical Staff, Studsvik, Sweden, 27 - 29 October 1976.

The design of a simulator for the training of operating engineers in advanced gas cooled reactor stations (AGR)

CONTENTS

Session III

DISTURBANCE ANALYSIS

Chairperson: Ph. Freymeyer

Secretary: W. Ehrenberger

Ph. Freymeyer, W. Ehrenberger	
SUMMARY OF SESSION III	207
C.H. Meijer, B. Frogner, A.B. Long	
A DISTURBANCE ANALYSIS SYSTEM FOR ON-LINE POWER PLANT SURVEILLANCE AND DIAGNOSIS	213
K. Yamazaki et al.	
DEVELOPMENT OF PLANT OPERATION MONITORING SYSTEM FOR NUCLEAR POWER PLANTS	233
L. Bürger, E. Végh	
MAN-MACHINE COMMUNICATION IN EXPERIMENTAL REACTOR CONTROL SYSTEM	247
W.E. Büttner, L. Felkel, R. Grumbach, F. Øwre, B. Thomassen	
FUNCTIONS AND DESIGN CHARACTERISTICS OF THE STAR DISTURBANCE ANALYSIS SYSTEM	261
L. Felkel, R. Grumbach, A. Zapp, F. Øwre, J.K. Trengereid	
ANALYTICAL METHODS AND PERFORMANCE EVALUATION OF THE STAR APPLICATION IN THE GRAFENRHEINFELD NUCLEAR POWER PLANT	283

Ph. Freymeyer, W. Ehrenberger
SUMMARY OF SESSION III

Ph. Freymeyer, W. Ehrenberger

SUMMARY OF SESSION III

The following pages summarize the discussion on the individual papers of the session.

Paper of Meijer, Frogner, Long

The system is not based on a specific kind of mathematical evaluations, but on cause consequence diagrams. The underlying models have the form of trees.

The simulated environment of the system did not produce any noise. During on-line operation an appropriate filtering would be necessary.

So far it was not yet considered which data should be selected for the system.

The system comprises 16 to 17 models in total. They have been derived from the considered disturbances.

Further models will in the first place aim at the improvement of the plant availability; later on safety questions will become important.

Paper of Yamazaki, Kawai, Hashimoto, Suzuki, Jzumi, Kato, Kiguchi
Kobayashi, Yanai, Jida, Nakamura

In order to keep system availability high, four computers are being used. Normally three of these work and the fourth is in stand by mode.

The present system is of course only additional to the conventional systems for reactor control or protection. So, if the system breaks down, enough back-up is available. Problems occur only during plant start-up. Start-up requires the presence of this computer system.

Paper of Bürger, Végh

The system contains two kinds of DDC loops: nuclear loops with cycle times of 2 seconds and thermal loops with cycle times of 4 seconds. In addition to DDC manual control is possible. The time intervals are supervised by watchdog timers.

CRTs are automatically updated every 15 seconds. Intermediate updating can be ordered by means of a pushbutton.

It is difficult to say, whether the operators will use the alarm trees provided by the system.

Short presentation of Mr. Johansson

Each new system faces the problem of being accepted. This is a reliability problem to a considerable degree. It should be designed such that graceful degradation is possible; so it should be modular.

Paper of Felkel, Grumbach, Zapp, Øwre, Trengereid
and

Paper of Büttner, Felkel, Grumbach, Øwre, Thomassen

A display of the timely sequence of any event is not implemented yet. It can be included, if the operator wants it. The information can be retrieved from the data base, if the total amount of information should be handled, however, the system would be increased.

The cause consequence diagrams are only a rough representation of the technical process, but it turned out that they are sufficient. Another problem is, whether they are valid. This is difficult to say; it must be verified in the future. Because of the large amount of experience necessary to derive these diagrams, they have been constructed in cooperation with KWU.

At the moment a particular system qualification is not considered necessary, because the STAR deals only with a limited part of the plant - the feed water system, and it works only open loop; i.e.

it is planned to perform a formal verification of the STAR programs. This verification shall be done with the aid of a GRS developed program analyser for the process computer language PEARL, in which the new version will be developed. So system reliability is considered very important. On the other hand, however, it is not felt that redundant computers are necessary.

The STAR does not require any new instrumentation, but it uses all information from the currently available measuring points. In its current configuration it uses more digital than analog signals. Concerning the analog values, as a rule three steps must be distinguished: high, too high and much too high. The STAR computer is connected to one of the plant's dual computers and gets all its information from this computer. The information transfer is strictly one-directional: supervisory computer to STAR. In order to avoid interferences with the plant only a one-way channel was provided. Analysis of the plant status itself, however, could start from the original analog and digital values as well in a different system set-up.

The STAR is considered only one module for a new control room. Noise analysis would be another module. The STAR could use the results of a noise analysis.

Paper of Baldeweg

The aim of the diagnosis is to find the real state of the power plant and to give advice for further action. The aim of the system is to make a data bank on the disturbed and normal plant situations and on appropriate operator actions.

Summary of the discussion

All the methods presented were considered to be useful for improving the knowledge on disturbed nuclear power plants. Further effort is necessary, primarily towards

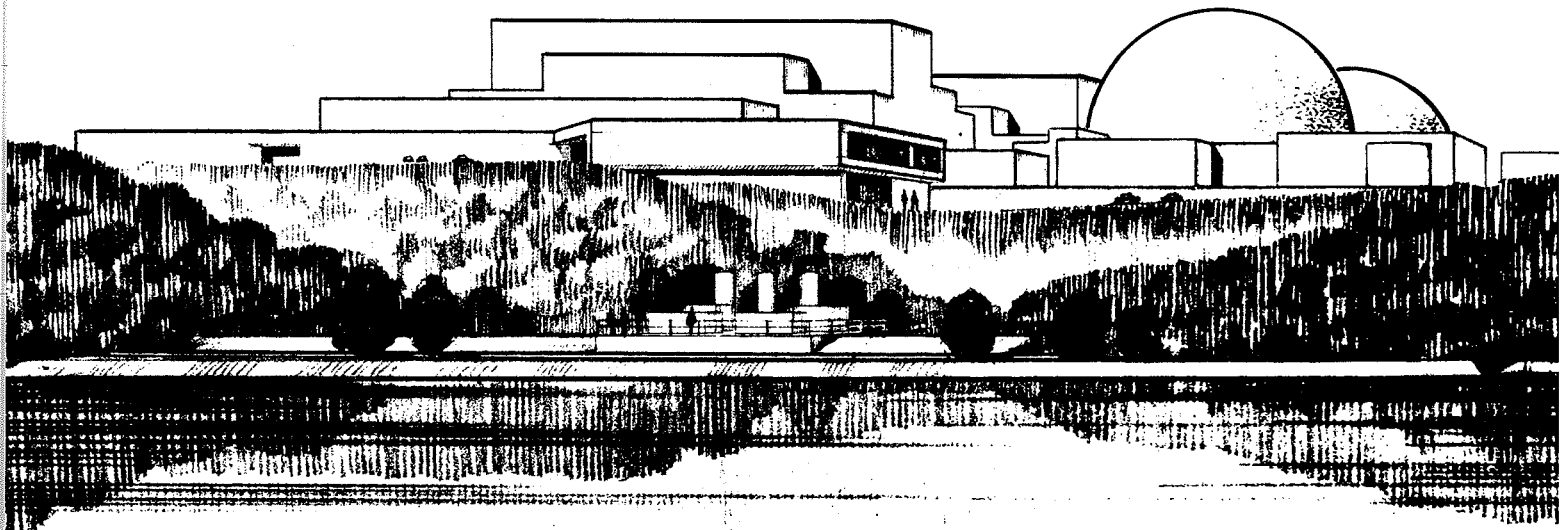
- enlarging available systems
- gaining operating experience.

There is no doubt that systems of this kind will increase in importance and will play a decisive role in future reactor control rooms.

C.H. Meijer, B. Frogner, A.B. Long

A DISTURBANCE ANALYSIS SYSTEM FOR ON-LINE POWER PLANT
SURVEILLANCE AND DIAGNOSIS

**A
DISTURBANCE ANALYSIS SYSTEM
for
ON-LINE POWER PLANT
SURVEILLANCE & DIAGNOSIS**



**C. H. MEIJER, MANAGER DEVELOPMENT
INSTRUMENTATION & CONTROLS ENGINEERING
NUCLEAR POWER SYSTEMS
COMBUSTION ENGINEERING, INC.
WINDSOR, CONNECTICUT**

**B. FROGNER, MANAGER
NUCLEAR SYSTEM PROGRAM
INDUSTRIAL SYSTEMS DIVISION
SYSTEMS CONTROL, INC.
PALO ALTO, CALIFORNIA**

**A. B. LONG, PROJECT MANAGER
NUCLEAR POWER, SAFETY & ANALYSIS DEPT.
ELECTRIC POWER RESEARCH INSTITUTE
PALO ALTO, CALIFORNIA**

**PRESENTED AT IAEA-NPPCI SPECIALIST MEETING ON PROCEDURES AND SYSTEMS
FOR ASSISTING AN OPERATOR DURING NORMAL AND ANOMALOUS NUCLEAR
POWER PLANT OPERATIONS SITUATIONS, MUNICH, DECEMBER 5-7, 1979.**

ABSTRACT

In a nuclear power generating station, a system providing on-line surveillance, early recognition, and diagnosis of disturbances could contribute not only to fewer station outages and therefore higher availability, but also to an improvement of the safety of the station.

This paper addresses a disturbance analysis system (DAS) for on-line power plant surveillance and diagnosis that allows operating personnel to assess in real-time occurring disturbances in terms of inherent character, cause, potential effect on the operational behaviour of the plant, and corrective actions. The system is computer-based and utilizes disturbance analysis algorithms based on information filtering, cause-consequence analysis and quantitative modeling techniques.

A prototype system operating on-line and in real-time was developed and demonstrated by Combustion Engineering Inc. (C-E) and Systems Control Inc. (SCI) under contract to the Electric Power Research Institute (EPRI). The demonstration utilized the C-E PWR Training Simulator and included the simulation and analysis of a selected number of disturbances in the feedwater and component cooling system, and some typical TMI-2 related events. An evaluation of the effectiveness of the DAS in terms of the performance of plant operating personnel in handling plant disturbances without and with the utilization of the DAS, is discussed in some detail.

Additional copies of this paper may be obtained by writing to Combustion Engineering, Inc., Communications Department 7021-1904, Windsor, CT. 06095, USA. Please mention the number (TIS-6349) that appears in the lower right hand corner of the front cover.

A DISTURBANCE ANALYSIS SYSTEM
FOR
ON-LINE POWER PLANT SURVEILLANCE AND DIAGNOSIS

INTRODUCTION AND SUMMARY

The Three Mile Island (TMI) accident has dramatically emphasized the importance of the man-machine interaction aspects within the control room of a nuclear power plant. The recently released Kemeny Report¹, documenting the results of a 6 month comprehensive study and investigation of this accident, concluded that in the TMI control room, "little attention has been paid to the interaction between human beings and machines under the rapidly changing and confusing circumstances of an accident". The report further concludes that the control room at TMI "showed little evidence of the impact of modern information technology", "information was presented in a manner which could confuse operating personnel", and "...the major factor that turned this incident into a serious accident was inappropriate operator action...".

From these conclusions, and also from those by others^{2,3}, it is apparent that the state-of-the-art of the man-machine interaction aspects in most nuclear power plants currently operating in the U.S. is less advanced than might be expected. One of the underlying reasons is that the design and implementation of control rooms in nuclear power plants has traditionally been in the way control rooms were built for fossil power plants. It has only been during the 1970's that the importance of more advanced human engineered control room concepts was recognized internationally⁴ by the nuclear industry. Such concepts are now penetrating the nuclear^{5,6} as well as the fossil⁷ power generating fields in the U.S. Universal application of the concepts is however not expected to materialize before the end of the 1980's. In particular, older plants and most of the plants currently in the construction phase will most likely have to be operated without a substantial benefit of many of the modern control room developments. Although selected control room improvements, to more involve the operating personnel as an integral part of the plant process, are being considered⁸, such involvement will still include many of the basic surveillance and diagnostic functions during the occurrence of plant disturbances.

An effective execution of these functions is often hampered by the lack of a universally accepted plant-wide alarm philosophy addressing such aspects as presentation, integration, prioritization, segregation,

grouping, suppression, shelving, etc. of alarms. A method or system that could analyze and integrate the alarm information generated for a given plant condition, could provide a significant contribution to the surveillance and diagnostic tasks of the plant operating personnel, and ultimately to the availability and safety of the plant.

This paper describes such a system in the form of an on-line power plant disturbance analysis system (DAS), which allows plant personnel to assess in real time, occurring plant disturbances. This assessment is performed by determining the cause of the disturbance, its potential consequence on the plant operational behavior, and the corrective or recovery action to be taken. The system is computer-based and utilizes disturbance analysis algorithms based on signal information filtering, cause-consequence analysis and quantitative modeling techniques.

A prototype system operating on-line and in real-time has been developed and demonstrated by Combustion Engineering, Inc. (C-E) and Systems Control, Inc. (SCI) under contract to the Electric Power Research Institute (EPRI). The demonstration utilized the C-E PWR Training Simulator and included simulation of a selected number of disturbances in the feedwater (FWS) and component cooling water system (CCWS) for this plant. In addition, some typical TMI related events were also simulated and analyzed to demonstrate how an effectively applied DAS could improve the safety of a plant.

In conclusion of the project, the performance of a representative group of nuclear plant operators was evaluated for a number of selected disturbances in terms of handling plant disturbances without and with the utilization of a DAS.

HISTORY

In England, it was recognized early in the 1960's that digital computers could be used for analysis of alarms beyond simple recording or annunciation. As a result, the Central Electricity Generating Board (CEGB) implemented a computer-based alarm-analysis system based on alarm fault trees at the Oldbury nuclear power station^{9,10} which was commissioned in 1968. Since then, similar alarm systems have been installed at Wylfa and Hinkley Point B. Being aware of the important improvements in man-machine interaction that can be achieved by a properly designed DAS, CEGB is continuing the development of

these systems. Plans are to install upgraded systems at the Dungeness B, Haysham, and Hartepool nuclear power stations.

Subsequently, research was initiated by the Institutt for Atomenergi (Halden, Norway) and the Gesellschaft für Reaktorsicherheit (Garching, Federal Republic of Germany) to develop disturbance analysis systems based upon cause-consequence diagrams^{11,12}. Preliminary tests during 1976 at the Halden research reactor demonstrated the technical feasibility of the approach¹³. Currently, both institutions, in conjunction with Kraftwerk Union and Bayernwerk, are implementing a prototypical system, named Störungs Analyse Rechner (STAR), at the Grafenrheinfeld plant¹⁴.

In power plants in the United States, most status information is still presented on a signal-by-signal basis with little integrated analysis. Often, hundreds to thousands of alarm annunciator windows are hardwired to individual process or control signals. Thousands of additional points are monitored by the plant process computer. Most filtering and analysis is also done on an individual signal basis. A first step toward providing more discriminating alarm information by analyzing selected variables was introduced by the industry in the form of Alarm Initiated Displays (AID)¹⁵.

The Electric Power Research Institute (EPRI) initiated in 1976 a research project with Combustion Engineering, Inc., and Systems Control, Inc., to develop a disturbance analysis system that could be demonstrated in a real-time simulated environment¹⁶.

FUNCTIONAL CONSIDERATIONS

In general terms, a disturbance analysis system should (1) incorporate a basic methodology for analyzing a wide variety of plant disturbances, (2) implement the plant specific design information in a data base, and (3) provide the results of its analysis in a precise format and on a timely basis to the operator for use in taking corrective action. The output results from the DAS may include the identity of the disturbance, time frame, possible consequences, and suggested corrective actions. At the discretion of the specific utility, and particularly the plant operational staff, it should be possible to vary the scope of the DAS implementation from selected disturbances in a given subsystem to a more plant-wide application using the same basic analysis methodology.

To achieve these objectives, the following general functional requirements were considered for the DAS:

- o Plant Interface: The DAS shall obtain plant status information directly from the plant's instrumentation and control systems or through the process computer. Additional sensors may be required; however, the benefits should justify the costs.
- o Operator Interface: The method for displaying the results from the DAS analysis shall be integrated into the control room design.
- o Timely Analysis: The DAS shall operate in real-time and present results within the time frame of the disturbance so that the operator can take corrective action.
- o Information Enhancement: The DAS shall enhance the quality and content of the information being displayed to the operator and reduce the number of secondary or extraneous alarms based upon the current mode of plant operation.
- o Disturbance Analysis: The DAS shall be capable of analyzing disturbances based upon a pre-established plant model stored in a data base. Once the DAS detects off-normal signals and analysis is initiated, the system shall be able to determine the nature, cause, consequence, and possible corrective actions.

MULTILEVEL ANALYSIS

Table 1 shows one way of classifying the problems associated with analysis of plant disturbances. The left-hand side of the table indicates the type of information needed to characterize the disturbances. The next three columns contain comments related to both the current and appropriate means of dealing with these types of problems.

TABLE 1
CLASSIFICATION OF THE PROBLEMS ASSOCIATED
WITH DISTURBANCE ANALYSIS

INFORMATION CHARACTERIZING THE DISTURBANCE	METHOD USED IN CONVENTIONAL SYSTEMS	REMARKS REGARDING CONVENTIONAL APPROACH	BEST MEANS OF DETERMINING APPROPRIATE MESSAGE
SINGLE CONDITION	600-1000 ANNUNCIATOR WINDOWS + METERS AND RECORDERS ON THE CONTROL BOARD COMPUTER ALARMS	ALARMING AND DISPLAYING EACH VARIABLE INDEPENDENTLY IS THE PRINCIPAL MEANS OF INFORMING THE OPERATOR ABOUT THE PLANT STATUS	SINGLE ENTRY TABLE LOOKUP
CLUSTER OF CONDITIONS	THE SUM OF SINGLE EVENT MESSAGES ARE DISPLAYED	IRRELEVANT AND SUPERFLUOUS INFORMATION IS OFTEN PRODUCED FOR THESE DISTURBANCES	MULTIPLE ENTRY TABLE LOOKUP
SEQUENCE OF EVENTS	SAME AS ABOVE + SEQUENCE OF ALARM LOGS AND "FIRST-OUT" ANNUNCIATOR SYSTEMS	CURRENT APPROACH IS OF LIMITED HELP IN DETERMINING THE UNDERLYING CAUSES FOR THESE DISTURBANCES	CAUSE-CONSEQUENCE ANALYSIS
QUANTITATIVE RELATIONS BETWEEN VARIABLES	STEADY STATE CALCULATIONS (THERMODYNAMICS, NEUTRONICS, ETC.) PERFORMED BY THE PROCESS COMPUTER	THE PROCESS COMPUTER IS CURRENTLY NOT REALLY PART OF THE ALARM SYSTEM	QUANTITATIVE EVALUATION OF PROCESS INFORMATION

To provide the best means of dealing with the four categories of disturbances in Table 1, the methodology developed for the actual disturbance analysis was

divided into three analysis modules or levels. The messages associated with single events and clusters of events are activated by Level 1, Level 2 involves analysis of sequence of events and/or complicated logic, and Level 3 deals with evaluation of quantitative models.

Level 1 analysis is a simple table lookup approach which is an efficient and simple means of analysis for a significant fraction of the commonly occurring plant disturbances. Also, this analysis module functions as an information filter which can prevent a large number of the disturbances from being subjected to the considerably more time-consuming and sophisticated analysis schemes represented by Levels 2 and 3 analysis modules.

Level 2 analysis is used to analyze disturbances which are characterized by complex logical relationships and/or sequence of events. The adopted method utilizes cause-consequence trees (CCTs) which are well-structured, easily implemented on a process-computer, and suitable for efficient on-line computer analysis. The method used for this analysis enables the implementation of new features that are unavailable in other alarm and diagnosis systems. The important features are:

- o Updating of the messages during the progress of a disturbance to keep the operator informed about the current status.
- o One step ahead prediction; i.e., the operator can be informed about the next message that is likely to be activated.
- o All the messages associated with each disturbance are grouped together.
- o Ability to correctly diagnose disturbances although some sensors may be malfunctioning.

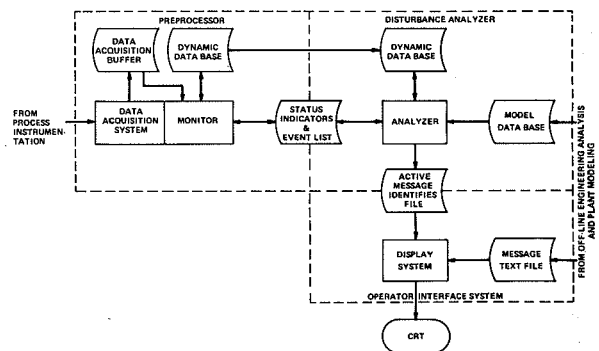
Level 3 analysis is intended for disturbances that must be analyzed by quantitative engineering type calculations. Sufficient flexibility has been incorporated into Level 3 to enable implementations of a wide variety of evaluations that cannot be fitted into the structured format associated with Levels 1 and 2.

FUNCTIONAL ORGANIZATION OF DAS

Figure 1 shows the main information flow in the DAS. The data acquisition system receives the

signals from the process instrumentation and converts the plant signals into the form needed for the disturbance analysis. The monitor compares the measured values with their high and low limits. An event is said to have occurred when a variable that previously was within its limits goes outside its limits, or a variable that previously was outside its limits goes inside its limits. A log is maintained of the time when the limit violations occur and the DAS analyzer is activated when one or more events have been registered. The messages resulting from the DAS analyzer are automatically displayed, and kept up-to-date, on a CRT.

FIGURE 1: SIMPLIFIED DIAGRAM OF THE INFORMATION FLOW IN THE DAS



Preprocessor

The data acquisition system and the DAS monitor are collectively denoted as the preprocessor. The activities of the preprocessor are performed sequentially and repeated every Δt seconds. The adjustable sampling frequency, Δt , is nominally set to 1 sec. The preprocessor tasks are executed asynchronously of the disturbance analysis. Thus, the DAS requires a multitask processor or (alternatively) two separate CPUs.

The data acquisition system is the interface between the instrumentation and the DAS. This system samples the input signals, checks for consistency (whenever multiple sensor readings are available) and sensor validity, performs low pass filtering, and converts the signals to engineering units. The data acquisition system is designed as a separate module to enable existing power plant data acquisition capabilities to be utilized in DAS implementations.

DAS Monitor

The DAS monitor activates and schedules the execution of the disturbance analysis. The monitor is activated as soon as the data acquisition buffer is updated. The monitor first communicates with the disturbance analyzer to determine the latest status of each process variable. Then the monitor updates user-defined derived variables and variable limits. Since the monitor has access to continuously updated plant signals, these variables can have any analytical expression including dynamic models if necessary.

The next activity of the monitor is to compare the variables with their specified (or derived) high and low limits to determine if any events have occurred since last sampling. Prior to activating the analyzer, the monitor gives the analyzer a copy of the relevant data. This copy of the data is kept fixed while it is used during the subsequent disturbance analysis.

Disturbance Analyzer

The DAS monitor schedules the execution of the disturbance analyzer. The disturbance analysis is then performed separately from the preprocessor so that the preprocessor can continue monitoring the process while the disturbance analysis is under way. The main functions of the disturbance analyzer are divided into three areas: (a) preparation, (b) multilevel analysis, and (c) post-processing.

The analyzer's copy of the process data may require some preparation before it is used for multilevel analysis. As an example, assume that an active message M1 is conditioned upon variables V1, V2, and V3 all being above their high limits. If analysis was activated because V1 just went back to its normal range, it is first necessary to deactivate M1, and then find the messages associated with V2 and V3 being HIGH. Therefore V2 and V3 must be subjected to a complete analysis.

Following completion of the multilevel analysis, it is necessary to perform a few cleanup functions (post-processing) before the analysis results can be presented to the operator interface system. So-called "second best" messages are attached to those events that the DAS was unable to adequately diagnose. Such messages may be used by the operators as supplementary information.

Operator Interface

This module translates the activated message identifiers into text strings that can be displayed on a CRT. Since these text strings are read by the operators, special attention must be given to the general layout of the information, choice of words, selection of colors, etc.

DATA BASES

The data bases have been divided into two broad classifications: (a) the dynamic data base and (b) the model data base. The first data base is updated each sampling interval by the data acquisition system and DAS monitor, while the other data base is entirely pre-established and fixed. The actual disturbance analysis consists of comparing the observed pattern of events as registered in the dynamic data base with the patterns for the disturbance models available in the model data base.

Dynamic Data Base

The dynamic data base contains two types of variables: (a) event variables and (b) auxiliary variables. The most important attributes associated with each event variable are as follows:

- o Name and value. The user assigns a unique name to each variable. The value is either obtained from the data acquisition system or computed by the DAS as a derived variable.
- o High and low limits are used as threshold values to determine when the disturbance analyzer should be activated. These limits are either fixed values or computed by the DAS.
- o Deadband is used to prevent small oscillations around the limits from being registered as events.
- o Priority is used to assure that important variables are analyzed expediently in case the analysis is unable to keep the pace with the stream of events. This feature has not been tested in this project; however, it is expected to become important in future developments and implementations of the DAS.
- o Second best messages contain the best information available in the case an event is registered for this variable and the DAS is unable to recognize the disturbance among its disturbance models.
- o Time of event is registered to enable the DAS to recognize sequence of events and to keep a record of when the event occurred.

- o Status Indicator is used as a key to guide the disturbance analysis. The status indicators are automatically updated by the DAS.

The auxiliary variables are only used as support information in engineering type of calculations and cannot initiate disturbance analysis by themselves. Thus, the only attributes associated with these variables are their names and values.

Model Data Base

This data base contains the information that represents the disturbance models of the plant. The model data base is divided into the following five groups:

- o Data base for Level 1 analysis
- o Data base for Level 2 analysis
- o Computational modules for Level 3 analysis
- o List of messages
- o Analysis directory for guidance of the multilevel analysis.

The first four groups of data must be developed by the user during implementation of the DAS while the analysis directory is generated automatically.

CAUSE-CONSEQUENCE ANALYSIS

Conventional fault tree and event tree analyses are performed on a function by function or system by system basis. Each function or system is addressed by hypothesizing failures and then studying how they impair performance. Cause-consequence trees used for on-line tracking and diagnosis of disturbances, are developed in a similar fashion except that it is necessary to account for the availability of process status information. Due to the large amount of experience available with fault tree and event tree analyses, it is natural to try to use modifications of these techniques for the on-line analysis. The cause-consequence tree (CCT) presented in this paper is such a modification.

A CCT is a formal representation of logical, causal, and temporal relationships. The tree can be considered as a "template" which can be compared to the detector readings of the process sensor states e.g., high, low, normal. Comparing the observed pattern of detector readings with the pre-established CCT enables the Level 2 analysis module to activate the

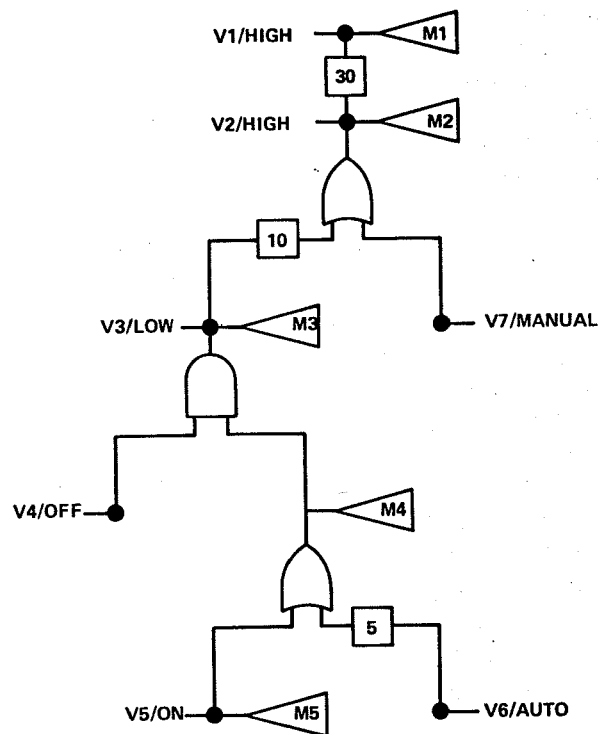
appropriate messages. Since the CCT is a model of how disturbances propagate, it is also possible to predict the future propagation of these disturbances.

Definition of the Cause-Consequence Tree

Figure 2 shows a hypothetical example of a CCT. The tree can be considered as nodes connected by arcs where each node is associated with one or more of the following attributes:

- o A variable identifier; e.g., V1, V2,...
- o A required condition for the variable; e.g., HIGH, LOW,...
- o A message identifier: e.g., M1, M2,...
- o A logical gate; e.g., AND, OR,...
- o A time delay; e.g., 5 sec., 10 sec.,...

FIGURE 2: A CONCEPTUAL EXAMPLE OF A CAUSE-CONSEQUENCE TREE



A node may be either observable or unobservable. An observable node is associated with a particular variable in the dynamic data base, while an unobservable node is not associated with any measured variable and its value can only be derived by deduction. The use of unobservable nodes provides a great deal of flexibility in construction of CCTs. Also, if there is a

modification in the instrumentations, e.g., addition or deletion of sensors, the CCT is easily modified by simply changing one attribute for the corresponding nodes.

For each observable node it is necessary to specify a required condition for the variable attached to this node. A node is said to be active if the required and observed conditions are equal and the part of the CCT below the node matches the plant observations. All the messages attached to active nodes are labeled as active messages.

The logical gates (AND, OR, or no logic gate) allow connection of the pieces of information required to diagnose the disturbances and to connect those disturbances that have common consequences.

Time delays are used to model the minimum time that is expected to elapse between events. If the observed time between two events is less than what it was modeled to be in a particular branch of the CCT, or if the observed sequence is opposite to the CCT, it is assumed that this branch does not correspond to the active disturbance. The modeling of the time delays therefore contributes to the unique identification of the disturbances and it prevents messages from being prematurely activated.

Time delays are also used to obtain what is called potentially active messages. In the case, the DAS determines that a node is not active for the single reason that enough time has not elapsed, the DAS will pick up the message associated with this node (if there is one) and label it as potentially active.

The objective of the on-line cause-consequence analysis is to find all the active and potentially active messages. Table 2 is an example of the activation of messages during the progress of a hypothetical disturbance.

It frequently occurs that several detectors do not respond as expected. This is a problem which the DAS deals with by making hypotheses about the detector readings. When it appears that an assumed value is consistent with a number of other observations, the result of the hypothesis is

that the detector reading is erroneous, or the sub-system from where the detector reading comes from, failed to respond as modeled. Let us assume that the analyzer finds a branch with several nodes which satisfy their required conditions but one (or a few) observation that does not correspond to the expected value. In this case the analyzer may assume that the node is active, label the node as a "hole", and continue the analysis. Holes must comply with the following rules:

- o Two sequential holes are unacceptable.
- o The number of holes in the active branch must be less than some specified number (recommended value: = 1).
- o Primary nodes cannot be holes.

TABLE 2
EXAMPLE OF A SEQUENCE OF EVENTS FOR THE
CCT IN FIGURE 2

TIME* IN SEC	EVENT	RESULT OF THE CAUSE- CONSEQUENCE ANALYSIS
0	V4 "s" OFF AND V5 "s" ON	M4 AND M5 ACTIVE M3 POTENTIALLY ACTIVE
1	V3 "s" LOW	M3, M4, AND M5 ACTIVE M2 POTENTIALLY ACTIVE
11	V2 "s" HIGH	M2, . . . , M5 ACTIVE M1 POTENTIALLY ACTIVE
41	V1 "s" HIGH	M1, . . . , M5 ACTIVE

*INITIAL CONDITIONS: V1 AND V2 ≠ HIGH, V3 ≠ LOW

In the example of Figure 2, assume that V6, V4, V3, and V1 satisfy the required conditions in sequence as required by the time delays while V2 is indicating a normal condition. In this case the DAS will label V2 as a hole and the entire branch between V1, V4, and V6 is considered active.

DEVELOPMENT OF DISTURBANCE MODELS

In order to perform its function, a DAS must include the appropriate models of the postulated plant disturbances to be analyzed. The models must be constructed in a form that accommodates the technique selected for the analysis system. The development of the models can be a significant effort. To minimize this effort, one should develop well formulated disturbance selection criteria. Such criteria must address e.g. which disturbance must be modeled for which plant system or

components, which plant mode of operation, the level of detail or the complexity of the models, etc. Existing results from previously performed failure mode and effects analyses (FMEA) or fault-tree analyses on the plant systems or components can provide an important contribution to the modeling effort.

The modeling process, mainly constituted the development of the model data base. This effort, was divided into five major activities:

- o Functional analysis of the selected subsystems
- o Cause-consequence analysis
- o Data base implementation and verification
- o Simulation and testing
- o Evaluation

The functional analysis included a detailed study of the design information of the two subsystems, the FWS and CCWS selected for this project. The study included an assessment of the functions of the subsystem, the means by which these functions are performed, the different modes of operation; e.g., automatic, manual, standby, etc., the operations of the actuators, information available from the instrumentation, and the dynamic behavior of the subsystem.

The cause-consequence analysis effort, transformed the general knowledge derived from the functional analysis into specific information associated with the disturbances that the DAS was expected to analyze.

The connotation of cause-consequence analysis is used in this paper to indicate that the primary emphasis is on determining cause of events that have occurred as well as predicting future consequences. This analysis has several similarities with fault-tree and event tree analysis; however, basic differences are bound to exist since the methods outlined in this paper are tailored to on-line tracking and diagnosis of disturbances using the detector readings as important pieces of information while the conventional fault-tree analysis is unrelated to the instrumentation.

To develop good CCTs, the analysis was initially performed according to a top-down approach. After specifying the system, one or more "top events" were defined. The following set of questions were then answered for

each event:

- o What is the sequence of events?
- o What are the minimum time delays between the various events?
- o What is the logic combination of these conditions?

The questions above were repeated for each of the events preceding the top event. The procedure is continued deductively until basic events and conditions have been reached or until further resolution of the events is of no interest.

A graphical representation (tree) can be then generated during the deductive reasoning process. The tree is so structured that the sequence of events leading to a particular condition is shown below the condition. The various events and conditions are logically related by AND and OR gates and time delays. The thought process involved and the graphical representation is similar to that commonly used for fault-trees.

If after the completion of the top-down analysis it was found that the basic events were unobservable, a unique set of observations, associated with a disturbance, were attached to a branch in the CCT. This method assured that this branch and the associated messages were only activated when the disturbance in question occurred.

After completion of the cause-consequence analysis, appropriate messages labeled by unique message identifiers were then formulated and attached to the appropriate nodes in the CCT. The next step in the modeling process included implementation and verification of the data base. Suitable coding forms and data base generator were hereby utilized to reduce the effort required. During the simulation process, the PWR simulator was used to evaluate the plant response for the disturbances to be diagnosed by the DAS, and to validate the adequacy of the disturbance models contained in the DAS data base. The simulator was further utilized to evaluate the overall performance of the DAS.

Table 3 summarizes the experience with the five steps involved in the data base development. Traditional (although time-consuming) problems such as debugging of software and hardware have been eliminated from the table since they are unrelated to the DAS per se, but rather associated with software and hardware development in general.

TABLE 3
SUMMARY OF EXPERIENCE WITH THE DATA BASE
DEVELOPMENT

ACTIVITY	MAIN PROBLEMS EXPERIENCED	IMPROVEMENTS THAT CAN BE MADE IN FUTURE PROJECTS	EXPERTISE REQUIRED IN PERFORMING THE TASK
FUNCTIONAL ANALYSIS	1. BEING ON A LEARNING CURVE 2. INCOMPLETE UNDERSTANDING OF THE SIMULATOR	1. IMPROVED FOCUS AND ACCURATE STATEMENT OF OBJECTIVE	1. GOOD UNDERSTANDING OF SUBSYSTEM 2. BACKGROUND IN CONTROL ANALYSIS, SIMULATION, OR MODELING IS ADVANTAGEOUS
CAUSE-CONSEQUENCE ANALYSIS	1. BEING ON A LEARNING CURVE	1. IMPROVED DESCRIPTION OF TECHNIQUE	1. BASIC UNDERSTANDING OF DAS FUNCTION 2. BACKGROUND IN RELIABILITY ANALYSIS IS ADVANTAGEOUS
DATA BASE IMPLEMENTATION & VERIFICATION	1. LIMITED SOFTWARE TOOLS FOR DEBUGGING	1. MORE ADVANCED DATA BASE GENERATOR	1. NO PARTICULAR
SIMULATION AND TESTING	1. INCONVENIENT ACCESS TO SIMULATOR 2. SLOW RESTART CAPABILITY	1. REGULAR ACCESS TO SIMULATOR (e.g. ONE HOUR EACH DAY DURING TESTING) 2. STREAMLINED TAPING OF DATA	1. KNOWLEDGE OF SIMULATOR TO DETERMINE THE APPROPRIATE WAY OF SIMULATING THE DISTURBANCES
EVALUATION	1. LIMITED SCOPE OF TEST 2. SMALL DATA BASE	1. COMPREHENSIVE TEST	1. HUMAN FACTORS BACKGROUND

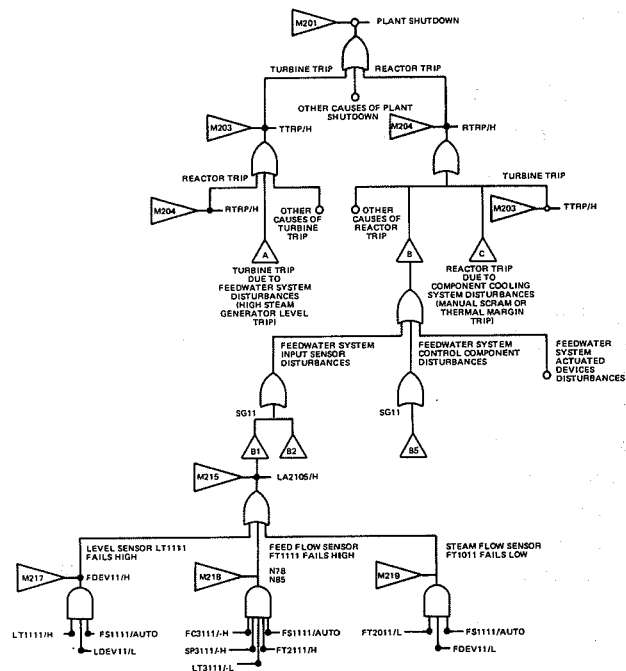
FWS & CCWS MODELING

A total of 54 system level disturbances were identified for a typical C-E PWR feedwater system (FWS) and 9 for the component cooling water system (CCWS), utilizing a failure or disturbance mode and effect analysis (DMEA) approach. Out of these 63 disturbances, 25 were modeled in the DAS. Figure 3 shows the CCT model for typical FWS input sensor disturbances. Out of the 25 modeled disturbances, a total of 9 (6 in the FWS and 3 in the CCWS), were thoroughly tested and evaluated on-line at the simulator for operator performance. This approach proved adequate to demonstrate the practicality of the developed methodology. Although modeling and implementation of all the disturbances identified by the DMEA would have yielded a larger data base, it was generally agreed upon that a considerable duplication of effort would have been necessary without a substantial contribution to the final results of the project. After the analysis methodology had been completed by SCI, implementation proceeded at C-E and SCI simultaneously. Utilizing an NSSS model, including a detailed model of the C-E steam generator, the methodology was debugged off-line on a PDP11/35 for several sample CCTs. C-E in the meanwhile implemented and debugged the methodology off-line on the Interdata 7/32, while proceeding with the modeling and data base development for 25 disturbances.

Upon completion of the debugging stage of the methodology, C-E then proceeded with on-line testing

of 9 disturbances on the simulator, one disturbance at a time. This testing phase proved to be invaluable specifically in terms of solving CCT interaction during the disturbance analysis process. The required effort of "tuning" the CCT's and methodology was considerably reduced by the availability of off-line testing capabilities, and a full scale plant simulator.

FIGURE 3: FWS INPUT SENSOR DISTURBANCES CCT



LEGEND

- FT1111 - SG1 FEED FLOW
- FT1011 - SG1 STEAM FLOW
- SP1111 - SG1 3-ELEMENT CONTROLLER WATER LEVEL SETPOINT
- M201 - PLANT SHUTDOWN
- M203 - TURBINE TRIP
- M204 - REACTOR TRIP
- M215 - FWS SG1 LO LVL ALRM
- M217 - FWS SG1 FF SF MISMATCH
- M218 - FWS SG1 FF SF MISMATCH
- M219 - FWS SG1 FF SF MISMATCH
- FC1111 - SG1 3-ELEMENT CONTROLLER MAIN FW VALVE POSITION DEMAND
- LT1105 - SG1 WATER LEVEL SENSOR 1
- LT1111 - SF1 WATER LEVEL SENSOR 2
- FS1111 - SG1 3-ELEMENT CONTROLLER MANUAL/AUTO STATUS
- LOEV11 - SG1 DIFFERENCE BETWEEN WATER LEVEL SENSORS LT1105, LT1111
- FC3111 - ADJUSTED LIMITS ON FC1111
- SP3111 - ADJUSTED LIMITS ON SP1111
- LT3111 - ADJUSTED LIMITS ON LT1111
- FT2111 - 30 SEC FIRST ORDER FILTER ON FT1111
- FT2011 - 30 SEC FIRST ORDER FILTER ON FT1011
- FDEV11 - SF1 STEAM FEED FLOW DIFFERENCE
- TTRP - TURBINE TRIP
- LA2105 - SG1 LOW WATER LEVEL ALARM, - 25 INCHES
- H - HIGH
- L - LOW
- SG - STEAM GENERATOR

Modeling the FWS was complicated by the presence of a number of feedback loops that makes it a highly coupled and complex dynamic system. The dynamic behavior during a disturbance depends upon:

- o Plant initial conditions prior to the disturbance
- o The way the failure occurred; e.g., sudden failure versus gradual failure
- o Plant mode of operations; e.g., controllers in manual

An additional complication arose due to the rather remote resemblance between a tree-structured model and the feedback dominated behavior of the FWS. Feedback loops cannot be explicitly modeled by a CCT. Dynamic models of the feedback loop are desirable in many cases. Modeling the CCWS proved to be much simpler than modeling the FWS although the engineer performing the analysis had much less prior understanding of the CCWS. Some of the important reasons for this situation are:

- o Feedback effects are of much less importance for the CCWS compared to the FWS.
- o The dynamic behavior of the CCWS disturbances do not depend upon as many parameters as the FWS.
- o To derive the information needed to implement the appropriate recovery action, the CCWS is well instrumented.

DEMONSTRATION SYSTEM

Figure 4 shows the hardware configuration for the DAS implemented in this project. The implementation was to a large extent constrained by existing hardware. An implementation at a power plant would most certainly be different from the setup discussed.

Ninety-eight signals were sampled in this implementation. The signals were obtained from the computer that drives the PWR Simulator. An Interdata 70 computer was used for implementation of the data acquisition software, and an Interdata 7/32 for the DAS monitor and analyzer software. This second computer was located about one mile away from the simulator.

Only raw digitized data were transmitted over the data link. A 1200 bit per second modem allowed adequate time for the data acquisition software to complete its activities and for the data to be transmitted within the 1-second sampling frequency.

The arrangement was good for a development project where debugging and testing were major activities. A typical debug session proceeded as follows. Signal data were received over the modem; the data were read by the DAS and also stored on magnetic tape for later off-line analysis; the disturbance analysis was activated; and the resulting message identifiers were transmitted over the modem while the test messages also were displayed on the CRT connected to the Interdata 7/32 computer.

FIGURE 4: DAS HARDWARE BLOCK DIAGRAM

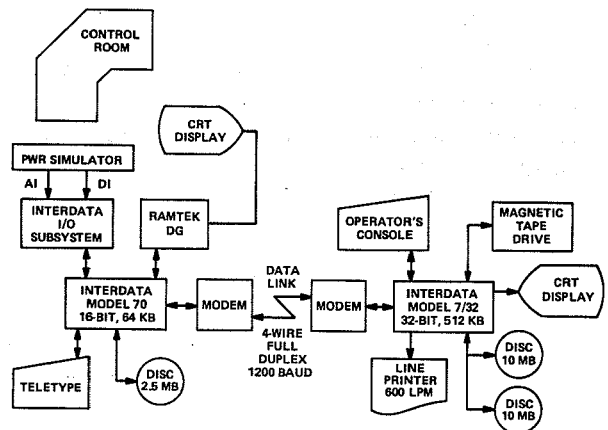


Table 4 shows the size of the major modules of the DAS. The data base generator was run as a separate program on the Interdata 7/32 as part of the initialization of the DAS. The data acquisition module, output display module, and message text files all resided in the Interdata 70 computer. The Interdata 7/32 accommodated the monitor (including a small module to transform the raw data into engineering values), analyzer, and the data base for the disturbance models. This is considered to be a modest storage requirement for a DAS.

TABLE 4
MEMORY REQUIREMENTS FOR IMPLEMENTATION OF DAS
ON INTERDATA COMPUTER

MODULE	REQUIRED MEMORY IN K BYTES
PRE-OFF-LINE DATA BASE GENERATOR	59
FRONT END	
DATA ACQUISITION MODULE	10
OUTPUT DISPLAY MODULE	11
+ MESSAGE TEST FILE	16
ON-LINE	
DAS MONITOR	32
DISTURBANCE ANALYZER	45
DATA FOR DISTURBANCE MODELS	42
TOTAL	215

During the DAS development, it was assumed that the DAS response time should be no more than approximately 2 seconds. This time is a function of the time required by each individual module of the system, e.g., monitor, analyzer, etc., to perform its function.

To interface the DAS with the plant operator, a single annunciator and a multicolor CRT display were chosen. An alarm annunciator "DAS Update" in the main control board of the PWR Simulator was used to alert the operators when the DAS was active and attention should be paid to the messages appearing on the CRT. The CRT was installed in the control panel of the simulator, next to the feedwater control panel.

The primary concern during the development of the display was the layout of the text messages on the CRT screen. Figure 5 shows an example of some of the messages. Each message is broken up into several fields as follows:

- o System where the disturbance originated
- o A brief description of the disturbance
- o Anticipated consequences if the disturbance is not arrested
- o Suggested recovery action
- o Cause of the disturbance.

This sequence of information display corresponds to the sequence of the diagnosis an operator would go through without having a DAS available.

The particular set of messages shown in Figure 5 is related to a steam generator level transmitter failing high. Initially, the first message is displayed

in yellow color to indicate that it is a "potentially active" message. The DAS detected that something was wrong but sufficient information was not available to firmly verify that the message was applicable. The message was given a cyan color (i.e., made "active") at the time when the feed flow/steam flow mismatch was sufficiently significant.

Reading the message from left to right, it can be noted that the feedwater system has been identified as the system where the disturbance occurred. The nature of the disturbance is a mismatch between feed flow and steam flow in steam generator #1. As a consequence of this disturbance a low level alarm condition is predicted to occur unless the operator manually opens the feedwater valve. The cause of the disturbance is that the level transmitter failed high.

FIGURE 5: AN EXAMPLE OF A DAS CRT MESSAGE DISPLAY

EPRI DISTURBANCE ANALYSIS SYSTEM				HR:MN:SS
SYS DISTURBANCE	CONSEQUENCE	ACTION	CAUSE	
FWS SG1 FF<SF MISMTCH	ALRM LO LVL	MC-OPEN FW VLV	LT11 FAIL HI	
FWS SG1 LO LVL ALARM	RT LO LVL			
FWS SG1 MAIN FW CTR OUT OF LMTS				
FWS SG1 FW VLV DP OUT OF LMTS				
	•			
	•			
	•			
	•			
UP TO 20 MESSAGES - 80 BYTES LONG MAX.				

Assuming that the operator does not take any corrective action, the second line of information will initially be displayed as a potentially active message whereupon it will change color when the low level alarm appears to indicate that it is an active message. This new message indicates that a reactor trip due to low level is imminent unless the operator implements corrective action.

The third and fourth lines of messages (in green color) are "second best" messages which contain supplementary information.

Various studies have been performed to determine the optimal use of colors for CRT displays and the ability of colors to convey information. Since a standard color code for industrial use has not yet been established, the color selections for the DAS display were chosen on the basis of C-E's experience^{17, 18} in this area.

PERFORMANCE EVALUATION

Upon completion of the debugging stage of the methodology, the DAS was tested on-line on the PWR Simulator for nine selected disturbances, six in the FWS and three in the CCWS, one disturbance at a time. Additional testing such as sensitivity with respect to initial power level, ability to diagnose two simultaneously occurring disturbances, ability to discriminate against power maneuvers, ability to diagnose disturbances during normal power maneuvers, and ability to diagnose failures that were not modeled, was carried out with varying degrees of success. In most of these cases, the DAS proved able to identify and correctly analyze the introduced disturbances.

In addition to the technical performance evaluation of the DAS, an effort was undertaken to determine the effectiveness of a DAS in the control room of a nuclear power plant. The steps involved in the evaluation were as follows:

- o Utilize C-E PWR Training Simulator
- o Run selected number of disturbances on simulator
- o Run disturbances during scheduled operator training sessions
- o Utilize operators from different utilities
- o Utilize operators with different training background
- o Quantify operator response to disturbances without and with DAS.

To allow proper evaluation of the performance by the operators in handling the test case disturbances, an evaluation form documenting time of disturbance initiation, time operator took action, training status of operator, etc., was utilized. The form was filled out by the simulator instructor during and immediately after each test case had been run. In addition to the form, the disturbance analysis monitoring capability of the DAS was utilized to record on magnetic tape such details as the sequence of events and dynamic behavior of disturbance related parameters. The information thus collected, was then reduced into graphs for the disturbance with superimposed timing events such as disturbance initialization, first message appearing on DAS monitor, control board annunciator actuation, operator action, etc.

Typical graphs are shown in Figures 6 and 7.

FIGURE 6: TYPICAL OPERATOR RESPONSES TO SG LEVEL (LEVEL TRANSMITTER) FAILED LOW, WITH AND WITHOUT DAS

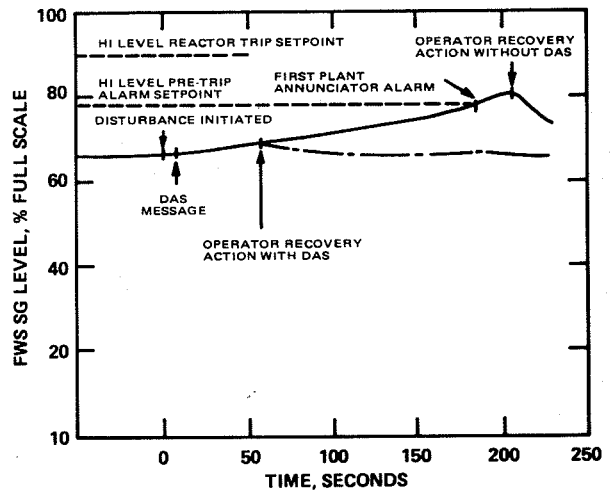
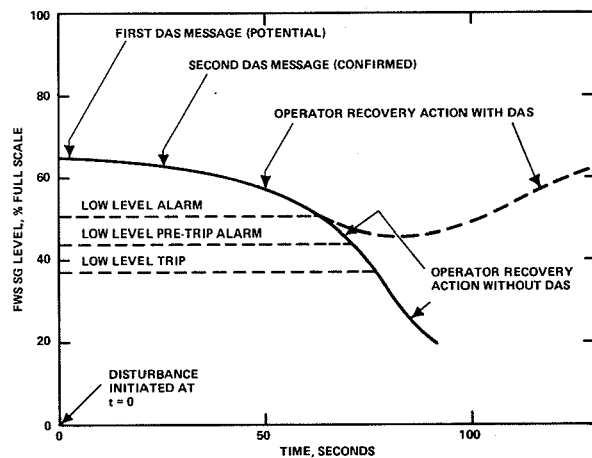


FIGURE 7: TYPICAL OPERATOR RESPONSE TO FEEDWATER PUMP SPEED CONTROL INPUT FAILED HIGH, WITH AND WITHOUT DAS



As can be observed from these graphs, the enhanced operator responses contributed to a reduction of plant perturbations as well as a reduction of challenges to the plant's protection system. Similar graphs

generated for other test cases yielded comparative results.

As expected, a wide scatter in proper operator response was observed. This scatter, as illustrated in Table 5, can be contributed to several factors such as operator training status, location of operator in control room at time of disturbance initiation, human factors aspects of the DAS monitor message displays, unique environment of the simulator control room, etc. However, taking these factors into account, the evaluation resulted in some significant conclusions as indicated in Table 6.

TABLE 5
SUMMARY OF RESULTS OF DAS EVALUATION EFFECTIVENESS

DISTURBANCE	EXISTING ALARM AT	TIME TO TRIP	DAS DIAGNOSTIC MESSAGE AT	OPER. DETECTS DISTURBANCE AT WITH/WITHOUT DAS	OPERATOR ACTION AT WITH/WITHOUT DAS
FEEDWATER SYSTEM (FWS)					
1. LEVEL TRANSMITTER LT1111/HIGH	25 SEC.	32 SEC.	5 SEC.	8/21 SEC.	21/80 SEC.
2. LEVEL TRANSMITTER LT1111/LOW	1 1/2 MIN.	4 3/4 MIN.	7 SEC.	7/78 SEC.	57/131 SEC.
3. LEVEL SETPOINT SP1111/HIGH	5 1/2 MIN.	18 MIN.	18 SEC.	5/73 SEC.	7/183 SEC.
4. LEVEL SETPOINT SP1111/LOW	25 SEC.	40 SEC.	18 SEC.	16/25 SEC.	22/30 SEC.
5. FLOW TRANSMITTER FT1111/LOW	-	-	2 MIN.	16/189 SEC.	20/105 SEC.
6. FEEDPUMP J.P TRANSMITTER (PD4516/HIGH)	72 SEC.	80 SEC.	37 SEC.	7/15 SEC.	7/25 SEC.
COMPONENT COOLING WATER SYSTEM (CCWS)					
7. COW PUMP 11 POWER OFF	20 SEC.	-	7 SEC.	7/28 SEC.	42/95 SEC.
8. COW HX11 OUTLET VALVE CV2824/CLOSED	10 SEC.	-	7 SEC.	7/4 SEC.	44/58 SEC.
9. COW HX11 SALTWATER COOLING VALVE H55296/CLOSED	2 MIN.	-	1 3/4 MIN.	137/150 SEC.	177/161 SEC.

* OPERATOR HAS 5 MINUTES TO RESTORE COW BEFORE PERMANENT EQUIPMENT DAMAGE WILL OCCUR.

DAS SIMULATION OF TMI EVENT

To evaluate the applicability of a DAS to the safety system of a plant, a TMI-type event was simulated on the C-E PWR Simulator. The approach taken in developing the logic was to identify the state of "key"

FIGURE 8: DAS CCTs FOR TYPICAL SIMULATED TMI EVENT

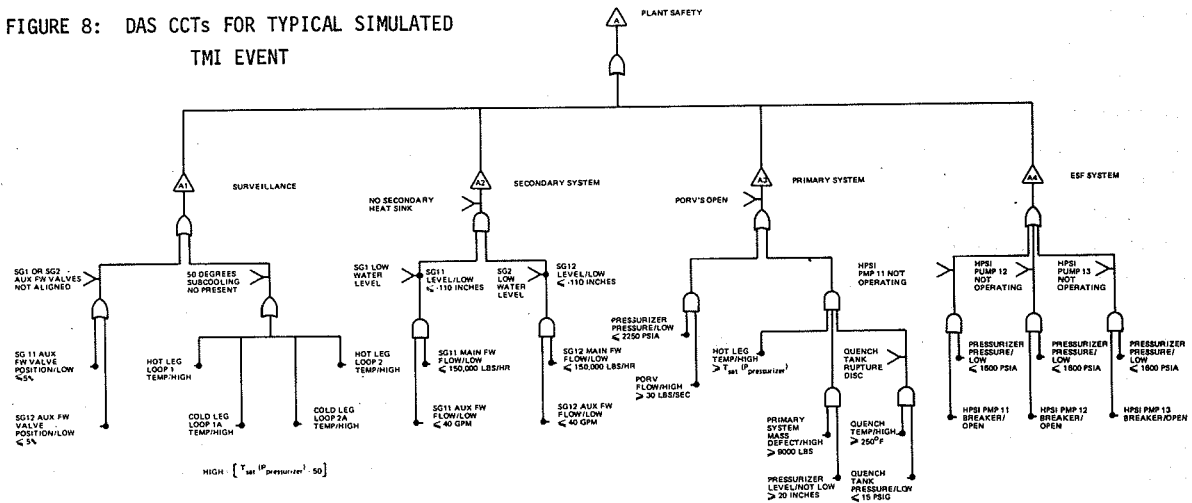


TABLE 6
CONCLUSIONS OF DAS EFFECTIVENESS EVALUATION

- A DAS WILL CONTRIBUTE TO LESS PLANT PERTURBATIONS FOR OCCURRING DISTURBANCES, THUS REDUCING THE CHALLENGES TO THE PLANT'S PROTECTION SYSTEM
- OPERATOR HAS EXTRA TIME TO RESPOND TO PLANT DISTURBANCES WITH DAS IN OPERATION
- EXTRA TIME IS IN RANGE OF:
SECONDS FOR RAPID TRANSIENTS (30 - 60 SEC. TO TRIP)
MINUTES FOR SLOW TRANSIENTS (5 - 8 MIN. TO TRIP)
- OPERATOR RESPONSE TO DISTURBANCES TYPICALLY OCCURS AT FIRST CONTROL BOARD AUDIBLE ALARM WITHOUT DAS
- DAS TYPICALLY PRODUCES FIRST AUDIBLE ALARM SOONER THAN EXISTING ALARM SYSTEM
- OPERATORS CONFIRM DAS MESSAGES WITH EXISTING CONTROL BOARD INDICATORS BEFORE TAKING CORRECTIVE ACTION
- CORRECTIVE ACTION MAY BE TAKEN SOONER WITH DAS IN OPERATION
- OPERATOR RESPONSE IMPROVES WITH MORE FREQUENT USE OF DAS
- OPERATORS WELCOME IN GENERAL RELIABLE DIAGNOSTIC INFORMATION
- DETAILED CORRECTIVE ACTION MESSAGES FOR COMPLEX DISTURBANCES ONLY
- CAUSATIVE MESSAGE INFORMATION IMPROVES EFFECTIVENESS OF DAS
- USE OF EXCESSIVE ACRONYMS AND SUPERFLUOUS MESSAGES TO BE AVOIDED
- FOR DISTURBANCES INTRODUCING SHORT-TERM TRANSIENTS MESSAGES TO BE AS SIMPLE AS POSSIBLE
- IN DYNAMIC SYSTEMS A DAS CAN DETECT DISTURBANCES WHICH COULD OTHERWISE GO UNNOTICED

safety functions. This included both system functions such as coolant inventory state and component functions such as operability of safety systems.

The initial phases of the TMI event were characterized by a loss of heat sink, primary coolant and the depressurization of the primary system at high temperature conditions. The DAS logic developed, included the capability to perform pre-accident surveillance (aux. feedwater system alignment), accident surveillance (secondary heat sink and saturation conditions) some causative surveillance (quench tank integrity and pressure operated relief valve (PORV) status) and surveillance of safety systems (high pressure safety injection (HPSI) pump status). The specific cause-consequence diagrams employed are illustrated in Figure 8.

The simulation of the TMI event on the simulator involved artificially defeating the low steam generator water level reactor trip and manually inducing a PORV failure at the point of a high pressurizer pressure trip. These changes were necessary to more closely simulate the time frame of the events experienced at TMI.

A typical scenario would proceed as follows:

- o Prior to the start of the accident, the auxiliary feedwater valves are mis-aligned and the HPSI pumps are rendered inoperative.
- o Main feedwater is isolated.
- o The steam generators dry-out.
- o Primary system temperatures and pressure rises rapidly.
- o A high pressure trip occurs and the PORV's are failed in the open position.
- o Primary coolant is discharged into the quench (drain) tank causing the rupture disk to fail.
- o The primary system begins to depressurize, causing the approach to saturation conditions.
- o The main feedwater is re-established causing a more rapid depressurization and approach to the HPSI actuation point.

The sequence of DAS messages up to this point in the scenario is shown in Table 7. Recovery from this condition can then commence and messages will be removed as the plant is stabilized. After recovery is complete the messages that remain on the screen are shown in Table 8.

TABLE 7
DAS SEQUENCE OF MESSAGES

FWS SG1, SG2 AUX FW VLVS NOT ALIGNED

SG1 LOW WATER LEVEL
SG2 LOW WATER LEVEL
NO SECONDARY HEAT SINK

REACTOR TRIP (ON HIGH PRESSURE)
TURBINE TRIP
PLANT SHUTDOWN

PORV STUCK OPEN
QUENCH TANK RUPTURE DISK

50° F SUBCOOLING NOT PRESENT

HPSI'S NOT OPERATING

TABLE 8
DAS MESSAGES AFTER RECOVERY

REACTOR TRIP
TURBINE TRIP
PLANT SHUTDOWN
QUENCH TANK RUPTURE DISK

ACHIEVEMENTS AND CONCLUSIONS

The accomplishments achieved during this work correlate well with the specific objectives set forth in the EPRI Project RP891-2 Interim Report.¹⁶ An effective methodology for performing on-line analysis of occurring disturbances in a nuclear power plant has been developed, implemented and demonstrated on a prototype system. Although the project was initially conceived to improve plant availability through improved man-machine interaction, a conducted simulated TMI related event has shown that a DAS could also provide an important contribution to the safety of the plant.

The main conclusions derived at during the project are summarized below:

- o Real-Time Operation: The DAS has successfully been tested in real-time analysis of disturbances on a PWR training simulator.
- o Timely Analysis: For all the disturbances that have been studied on the simulator, the DAS has provided more timely and precise indication of the problem before actuation of the conventional annunciator system occurred.
- o Plant Interface: By implementing the DAS on a training simulator, it was demonstrated that the DAS could function as an independent system which required only plant instrumentation signals as input.
- o Preprocessing: The DAS has its own preprocessing function as part of its data acquisition module. The extent of preprocessing that is required is dependent upon the particular implementation.
- o Plant Mode Detection: The DAS can determine

the plant mode by monitoring the input signals or information derived from the input signals. This feature was partly demonstrated by the analysis of disturbances at different power levels.

- o Disturbance Detection: The disturbances that can be diagnosed by the DAS are detected by the appearance of one or more discrete events. The actual disturbance analysis is activated and the diagnosis of the status of the disturbance is updated following each of the events. This a flexible and efficient approach for detecting those disturbances that have been investigated in this project.
- o Disturbance Analysis: An effective methodology for performing the disturbance analysis has been developed. A multilevel analysis approach has been derived, which provides three levels of modeling complexity for various types of disturbances. Fault tree analysis and related techniques have been molded into cause-consequence analysis methodology.
- o Sequency of Events Evaluation: This DAS feature has two aspects to it: a) recognize the sequence by which the events occur and use this as an additional piece of information in the diagnosis of the disturbances and b) update the messages on the CRT as soon as new information is available to give the operator an overview of the sequence of events, the current status, and predicted future consequences. Both of these capabilities have been demonstrated.
- o Enhancement of Information: The DAS has been demonstrated to improve the information content in alarms compared to the approach used for conventional annunciator systems.
- o Operator Interface: The DAS has been demonstrated to give the necessary information through CRT displays. The DAS operates automatically without operator assistance.
- o Data Base Modification: A first step toward a data base generator has been taken during this project.

- o System Implementation: A demonstration type DAS has been implemented on commonly available minicomputers and integrated with a PWR plant simulator. The hardware requirements are considered to be modest and implementation is fairly straightforward. Analysis time is less than a few (typically 2 or 3) seconds. Two representative plant subsystems have been analyzed and used for the testing. Some 25 disturbances have been modeled for the two plant subsystems and 9 of these disturbances have been the subject for extensive testing.
- o Cost of Implementation: The cost of a DAS will be determined by the scope of the system or its implementation environment. Never-the-less our experience suggests that model development is the most expensive portion of the process. However, this cost may be shared between several plants if the disturbance models are fairly similar for these plants. Furthermore, the off-line disturbance analysis may provide additional benefits since a thorough off-line disturbance modes and effects analysis can give valuable insight into the adequacy of the plant design from an operational point of view.
- o Performance Evaluation: The performance of the integrated version of the DAS coupled with C-E's PWR plant training simulator has been evaluated by using experienced as well as trainee operators. Although only gross indications were sought, very positive experience has been gathered which will be valuable for future DAS developments.

A more comprehensive assessment of the results and conclusions of this work has been delineated in the EPRI Project RPS91-2 Final Report.^{1,2}

FUTURE DEVELOPMENTS

After the TMI accident, disturbance analysis systems have been frequently cited^{1,2} as a potential means of improving the safety of nuclear power plants. EPRI and the US Department of Energy have initiated short-

term scoping and feasibility studies in this respect. If a satisfactory degree of industry consensus can be achieved, it is expected that an extensive development effort to develop a second generation Disturbance Analysis and Surveillance System (DASS), will be undertaken during 1980. As a minimum, such a system would include techniques for:

- o Proper interpretation and validation of key process measurements
- o Surveillance of subsystem configurations and margins to Technical Specification limits
- o Identification of plant mode of operation and the integrated display of necessary state information
- o Timely recognition of disturbances
- o Assistance in monitoring operational procedures
- o Evaluation of possible control actions prior to initiation.

In addition to a demonstration and well validated engineering methodology, the development of a DASS would include an on-line design which could be adapted by individual utilities to their specific plant design.

REFERENCES

1. John G. Kemeny, Final Report of the President's Commission on the Accident at Three Mile Island, (10/79).
2. TMI-2 Lessons Learned Task Force Final Report, NUREG-0585, (10/79).
3. J. L. Seminara, W. R. Gonzalez, and S. O. Parsons, Human Factors Review of Nuclear Power Plant Control Room Design, EPRI NP-309, (11/76).
4. Proceedings IAEA Specialist Meeting on Control Room Design, IEEE-75CH1065-2, (7/75).
5. J. E. Myers and J. W. Veirs, "An Advanced Control Center Design for Nuclear Power Plants", Proceedings American Power Conference, (4/75).
6. HPR-214, Proceedings Enlarged Halden Programme Group Meeting on Process Supervision and Control in Nuclear Power Plants, Fredrikstad, Norway, (6/77).
7. R. Hicks, "Power Plant DDC Computer with Distributed Multiplexed Plant Monitoring", Instrument Society of America, Power Instrumentation Symposium, Chicago, (5/78).
8. Nucleonics Week, Inside NRC Special Supplement, (10/22/79).
9. D. Welborne, "Alarm Analysis and Display at Wylfa Nuclear Power Station", Proceeding British IEE Vol. 115 #11, (11/68).
10. D. Patterson, "Application of a Computerized Alarm-Analysis System to a Nuclear Power Station", Proceedings British IEE Vol. 115 #12, (12/68).
11. R. Grumbach and K. Netland, "Plant Disturbance Analysis: A Survey of Essentials for a Consistent Design", Enlarged Halden Programme Meeting on Supervision and Control in Nuclear Plants, HPR-214, (6/77).
12. L. Felkel, R. Grumbach, E. Saedtler and D. Wach, "Treatment, Analysis and Presentation of Information about Faults and Plant Disturbances", Symposium in Nuclear Plant Control and Instrumentation: IAEA-SM-266/76, (4/78).
13. R. Grumbach, H. Hoermann, "Plant Disturbance Analysis by Process Computer Basic Development and Experimental Testing", Proc. of IAEA/NPPCI Specialist Meeting on Use of Computers for Plant Control and Safety, (6/76).
14. F.W. Owre and L. Felkel, "Functional Description of the Disturbance Analysis System for the Grafenrheinfeld Plant", Halden Program Meeting, (6/78).
15. J. N. Shukla and R. H. Wong, "Nuclenet Control Complex", Proceedings Specialist Meeting on Control Room Design, IEEE-75CH1065-2, San Francisco, (7/75).
16. B. Frogner and C. H. Meijer, "On-Line Power Plant Alarm and Disturbance Analysis System", EPRI Report NP-613, (2/78).
17. S. Dlugolenski et al, "Using Color in Industrial Graphics", Control Engineering, (7/79).
18. M. M. Danchak, "Alphanumeric Displays for the Man-Process Interface", C-E Publication TIS-5301.
19. B. Frogner and C. H. Meijer, "A Disturbance Analysis System for On-line Power Plant Diagnosis", Final Report EPRI Project RP891-2. (to be published).

ACKNOWLEDGEMENTS

The authors are indebted to J. P. Pasquenza (C-E), J. N. Lanzalotta (C-E), R. H. Brown (C-E), J. S. Katz (C-E), J. W. Pfeifer (C-E), F. M. Kessler (C-E), S. Dlugolenski (C-E), T. Dennis (C-E), S. Foster (SCI), K. Jeyarasasingam (SCI), B. Friedlander (SCI), H. S. Rao (SCI), and A. Ipaktchi (SCI) for their technical contributions to the project, to S. A. Morrey (C-E) for the artwork, and to S. A. Averill (C-E) and D. J. Brunelle (C-E) for typing the final manuscript.

K. Yamazaki et al.

DEVELOPMENT OF PLANT OPERATION MONITORING SYSTEM FOR NUCLEAR
POWER PLANTS

DEVELOPMENT OF PLANT OPERATION MONITORING SYSTEM FOR NUCLEAR POWER PLANTS

Kanji YAMAZAKI¹, Katsumi KAWAI¹, Yuji HASHIMOTO²,
Mitsuo SUZUKI³, Masayuki IZUMI⁴, Kanji KATO⁴,
Takashi KIGUCHI⁴, Setsuo KOBAYASHI⁴, Katsuya YANAI⁵,
Hiroshi IIDA⁵, and Hideo NAKAMURA⁶

1. Tokyo Electric Power Company
Chiyoda-ku, Tokyo 100 JAPAN
2. Chugoku Electric Power Company
Hiroshima-shi, Hiroshima-ken 732 JAPAN
3. Chubu Electric Power Company
Higashi-ku, Nagoya 461-91 JAPAN
4. Energy Research Laboratory, Hitachi Ltd.
Hitachi-shi, Ibaraki-ken 316 JAPAN
5. Omika Works, Hitachi Ltd.
Hitachi-shi, Ibaraki-ken 316 JAPAN
6. Power Generation & Transmission Group, Hitachi Ltd.
Hitachi-shi, Ibaraki-ken 316 JAPAN

1. Introduction

With the increasing size of nuclear power plants, the amount of indicators on the operating console has become larger, and the monitored information has become more complex.⁽¹⁾ Plant operators are required to have a greater skill to grasp the plant state accurately.

The NUCAMM-80 (Nuclear Power Plant Control Complex with Advanced Man-Machine Communication) has been developed to decrease operators' burden and to increase plant availability. In this paper, a Plant Operation Monitoring System by computer based console, which is one of functions in the NUCAMM-80, is mainly described. The aims of the Plant Operation Monitoring System are :

- (1) to detect anomalies of the plant at an early stage,
- (2) to give information on their causes or locations, and
- (3) to give information on corrective actions.

This system consists of five subsystems : summary status display, system status monitor⁽²⁾, plant diagnosis system⁽³⁾⁽⁴⁾, automatic information selection system⁽⁵⁾ and conversational data access system⁽⁶⁾, and works during power change operation and/or steady state operation.

The performance of the Plant Operation Monitoring System has been tested by using anomalous process signals which are generated by superimposing the output signals of a dynamic simulator on the process data at normal operation recorded at a commercial BWR plant. The results of the performance test show that it works well, and it is expected that the system is to be a useful implement for safe operation and to improve plant availability.

2. Outline of NUCAMM-80

In the NUCAMM-80 introduced are technologies about computer based console, automatic operations, plant diagnosis, core performance and monitoring advanced process computer system.

Photo. 1 shows the plant operator's console of the NUCAMM-80. The plant operator's console consists of the cleanup demineralizer system, the condensate-feedwater system, the primary loop recirculation system, the reactor core and the monitoring of operating conditions, the turbine-generator system, and the monitoring of core performance. The balance-of-plant (BOP) console and the reactor core cooling system's console are separated from the plant operator's console.

Table 1 shows the comparison between the conventional console and the NUCAMM-80. The plant operator's console of the NUCAMM-80 is a desk-top type by taking human engineering into consideration sufficiently.

The NUCAMM-80 uses six color CRTs (Cathode Ray Tubes) in addition to indicators and recorders for operators to grasp and to judge correctly and promptly the plant operating conditions. A display of intensive information on color CRTs is controlled by multi-computer system with four computers (one is a standby). The number of switches on the plant operator's console of the NUCAMM-80 are reduced to about 30% by introducing automatic operations.

3. Plant Operation Monitoring System by Computer Based Console

Figure 1 shows the functional diagram of the Plant Operation Monitoring System, which consists of five subsystems : Summary status display (SSD), system status monitor (SSM)⁽²⁾, plant diagnosis system (PDS)⁽³⁾⁽⁴⁾, automatic information selection (AIS) system⁽⁵⁾, and conversational data access (CDA) system.⁽⁶⁾

Main functions required for plant monitoring systems are to detect anomalies and give the information on the anomalies at an early stage in order to prevent the unscheduled plant outage, and, for the situations of reactor scram or accidents, to give the information on the plant situation to make the damage as small as possible. The Plant Operation Monitoring System presented in this paper has been designed mainly for offering the former function.

(1) Detection of anomalies

Anomalous situations could be classified into two categories :

- (A) slow aggravation of performance of plant components, and
- (B) rapid progress of anomalous situations.

The functions to detect the situations (A) are usually called "diagnosis". Some of the proposed methods of plant diagnosis are the model comparison method and the noise analysis method. In the Plant Operation Monitoring System, the model comparison method has been employed, which is suitable for on-line and real-time uses, as well as for identification of causes of anomalies. The PDS involves a set of linear dynamic models for each plant subsystems and is convenient for monitoring each plant subsystem. On the other hand, the SSD has the rather simple models describing the balance of whole plant state, and is designed for grasping the whole plant situation at a glance.

For the situations (B), the PDS and the SSD are, of course, useful implements, which monitor the performance of plant components. At the same time, it is important to maintain the process variables, such as feedwater pump speed, core pressure, etc., within the specified safety regions. An index representing the closeness of process variables to their alarm or scram levels has been introduced, so that the operators can get the information on the anomalies in advance of occurring of alarm or scram. The SSM has been developed for this purpose.

(2) Identification of anomalies and taking corrective actions

The man has the greater ability of intensive judgement, however, has the less capability of large data processing. The machine or computer, on the other hand, can process the larger amount of data at high speed, however, its decision is limited by algorithm prepared in advance. For the decision-making of identifying anomalies and taking corrective actions, it is important to introduce man-machine cooperation to maximize the both performances of man and machine.

The AIS and the CDA have been designed to realize the effective cooperation of man and machine. The AIS selects automatically the information, which might be helpful for operators to understand the plant situation and to take corrective actions, by the algorithms simulating the decision process of skillful operators. It is triggered by the PDS, the SSD and the SSM, as well as the conventional alarm system.

The CDA realizes the efficient man-machine communication, by which the operators can select the desired information for their decision-making by the conversational mode.

Some explanation of each subsystem is given in the following chapters.

Photo. 2 shows the computer based plant operation monitoring console developed in this study. The process computer system (HIDIC-80) with consolidated modular engineering technology is used for the Plant Operation Monitoring System, except for the SSD and the SSM, in which four micro-computers are used to process the data and to control the operation panel and the display.

3.1 Summary Status Display

The SSD monitors twelve process signals representing the whole plant state and displays the deviation of these measured values from the reference values as a pattern of bright spots with the upper and the lower limits. The operator can grasp easily the difference from a normal operating condition by monitoring the displayed pattern.

The standard signals to calculate the reference value are the main steam flow and the speed controller outputs of the primary loop recirculation pump. Table 2 shows the monitored signals and the method to calculate the reference values in the SSD. These are obtained by fitting the measured values at the steady state operating conditions of the various reactor power levels for a commercial BWR plant of 2381 MW core thermal power. The upper and the lower limits are set to aid operators to grasp the plant state and to detect an anomaly. These limits are determined from the fluctuation during the normal operating conditions and the alarm levels.

3.2 System Status Monitor (2)

The SSM monitors intensively the change of operating performance for each plant component, such as pumps, turbines, valves and so on.

Figure 2 shows the functional diagram of the SSM. The characteristic indices are used for monitoring, which are defined as the probability whether the component can be continued to operate or not. Each component has a few observable signals, such as temperature, pressure, flow rate, vibration and so on, each of which represents the operating performance of the component. The characteristic index is normalized by the level which the component can not be continued to operate.

A maximum characteristic index on a component is picked up through a maximum value gate. In order to make monitoring simple, another maximum characteristic index in a subsystem is detected through a next maximum value gate, and is displayed by a bar graph on CRT. When the characteristic index arrives at the trigger level which is a certain value between zero and unity, a trigger signal is sent to the automatic information selection system.

3.3 Plant Diagnosis System (3)(4)

The PDS detects anomalies of the plant components at an early stage and identifies their locations or causes.

Figure 3 shows the conceptual diagram of the PDS which has two processing stages. The first stage is to calculate the differences ϵ_i , called the error signals, between observed process variables and corresponding variables estimated by the linear dynamic models. The error signals are nearly equal to zero under the normal condition, assuming that the models are well adjusted to simulate the behavior of the plant subsystem. And one of the error signals, at least, becomes far from zero under an anomalous plant condition. At the second stage, the block monitoring index B_i is calculated by taking the minimum error signal. The performance change of plant components is indicated by change of the corresponding block monitoring index. In the PDS, sixteen error signals are calculated and twenty block monitoring indices, i.e. the subsystem are divided into twenty.

3.4 Automatic Information Selection System (5)

The AIS system is triggered by the SSD, the SSM, the PDS and the conventional alarm system and automatically selects the information helpful for the operators to identify the detected anomalies and to take corrective actions. Conceptual flow diagram of the AIS system is shown

in Fig. 4.

The AIS system selects the information which has the highest grade. The grade is determined, in advance, for each anomaly to be detected by the monitoring sub-systems or the conventional alarm system on the basis of the grade of damage to a plant. The anomalies are graded into four classes. The highest one is a reactor scram or an anomaly that simultaneously causes a reactor scram, such as a turbine trip. The second one is an anomaly that may cause a reactor scram without quick and exact corrective actions, such as a reactor feedwater pump trip. The third one is an anomaly that may bring main component trips without exact corrective actions, such as malfunction of component cooling pumps. The lowest one is an anomaly that proves a presage of a component malfunction, such as high temperature of a bearing. If the detected anomalies have the same grade, the AIS system selects the information about the anomaly which has the plant data nearest to the operation limit such as the alarm level or the trip level. The selected information for each anomaly is tabulated in advance from operation manuals, results of plant dynamic analysis and so on. For example, in the event of turbine trip, main process data such as turbine speed, reactor water level and reactor pressure are selected and displayed with the information about the conditions of main components: opening and closing of main isolation valves, relief valves or bypass valves. Furthermore, sequence of major events are also displayed: major events mean a turbine trip, a generator trip, a reactor scram and so on. The selected information is displayed on the color CRTs by system flow diagram, trend graph, bar chart, message or combination of these.

3.5 Conversational Data Access System⁽⁶⁾

In the conversational information display, the plant data access procedure is divided into three levels in a hierarchical structure, in accordance with process system and operational mode. The data access keyboards consist of the access procedure control button, the ten-keys for designating the desired information, and digital display demand buttons. The operators can access the desired data, and can grasp the plant condition at any time.

4. Performance Test

The performance of the Plant Operation Monitoring System has been tested by using anomalous process signals, which are generated by superimposing the output signals of a dynamic simulator on the process data at normal operation recorded at a commercial BWR plant.

The manual trip of the turbine driven reactor feedwater pump A (TDRFP-A) due to decrease of the suction flow and the automatic start of the motor driven reactor feedwater pumps A and B (MDRFP-A,B) were simulated at the performance test. Figure 5 shows the performance test results of the Plant Operation Monitoring System.

For decrease of the suction flow on the TDRFP-A, the PDS, the SSD and the SSM detected anomalies in order of sensitivity. Photo. 3 shows the display example for anomaly detection of the SSD. In the first request by the operator, the AIS system selected data set of the TDRFP-A related with the anomaly detection of the SSM, which was the highest grade. Photo. 4 and Photo. 5 show the display examples for data set of the TDRFP-A and anomaly detection of the SSM, respectively. The TDRFP-A was tripped manually by the operator from the displayed information selected by the AIS system. Then, in the SSM, the TDRFP-A was removed from monitored component, and the MDRFP-A,B were added to monitored components. The monitored result of the SSM and the feedwater flow in the SSD returned to its normal level after the MDRFP-A,B automatic start. The operator

selected data set of the MDRFP by the CDA system, and confirmed normal startup of the MDRFP-A,B. Photo. 6 shows the display example for data set of the MDRFP-A,B. Then, to take the information on causes, the operator selected the trend graph of various signals by the CDA system.

The Plant Operation Monitoring System detects anomalies immediately after the decrease of the TDRFP-A suction flow, and gives the operator the location which has the highest grade. Therefore, the operator was able to trip manually the TDRFP-A, and the MDRFP-A,B were started automatically at about 20 sec. As the results, the reactor water level was controlled to about 680 mm, and the reactor scram could be prevented.

If the only conventional monitors, such as alarm system, indicators and recorders were available, it might require more time to detect anomalies and to take corrective actions. When the manual trip of the TDRFP-A by the operator and the automatic start of the MDRFP-A,B were later than about 30 sec, the reactor might be scrambled because of the "reactor water level low" (the scram water level is 273 mm).

5. Conclusion

The Plant Operation Monitoring System by computer based console has been developed. The system consists of five subsystem : summary status display, system status monitor, plant diagnosis system, automatic information selection system and conversational data access system.

The performance of the Plant Operation Monitoring System has been tested by using anomalous process signals, which are generated by superimposing the output signals of a dynamic simulator on the process data at normal operation recorded at a commercial BWR plant. The results of the performance test showed that it works well.

It is expected that the system is to be a useful implement for safe operation and to improve plant availability.

Acknowledgement

A part of this study was conducted in the course of the joint research program of Tokyo Electric Power Company, Chubu Electric Power Company, Chugoku Electric Power Company and Hitachi, Ltd..

The authors would like to thank Drs.K. Taniguchi and S. Yamada of Energy Research Laboratory, Hitachi, Ltd., for their encouragement and support to this work. The authors also express their gratitude to Dr. K. Takumi of Power Generation & Transmission Group, Hitachi, Ltd., Messrs. H. Maruyama and H. Kitanosono of Omika Works, Hitachi, Ltd., for their constant support during the course of the research.

References

- (1) M. H. Raudenbush, "Human Engineering Factors in Control Board Design for Nuclear Power Plants", Nuclear Safety, 14(1), 21~26 (1976)
- (2) S. Kobayashi et al., "Experience with Computer Based Systems Applied to Boiling Water Reactor Power Plant", Preprint of Enlarged Halden Program Meeting (1977)
- (3) K. Kato et al., "Anomaly Detection System for Nuclear Power Plant", Symposium of Power Plant Dynamics, Control and Testing, held in Knoxville, Tennessee (1973)
- (4) F. Murata et al., "Development of a Diagnosis System for a Boiling Water Reactor", Nuclear Technology, 44, 104~117 (1979)
- (5) S. Kishi et al. "Plant Monitoring by Color CRT Displays for Boiling Water Reactor", Hitachi Review, 25 (8), 265~270 (1976)
- (6) S. Kishi et al., "A Conversational Data Access Procedure for CRT Operator Consoles" IEEE Trans. on Nuclear Science, NS-22 (1975)

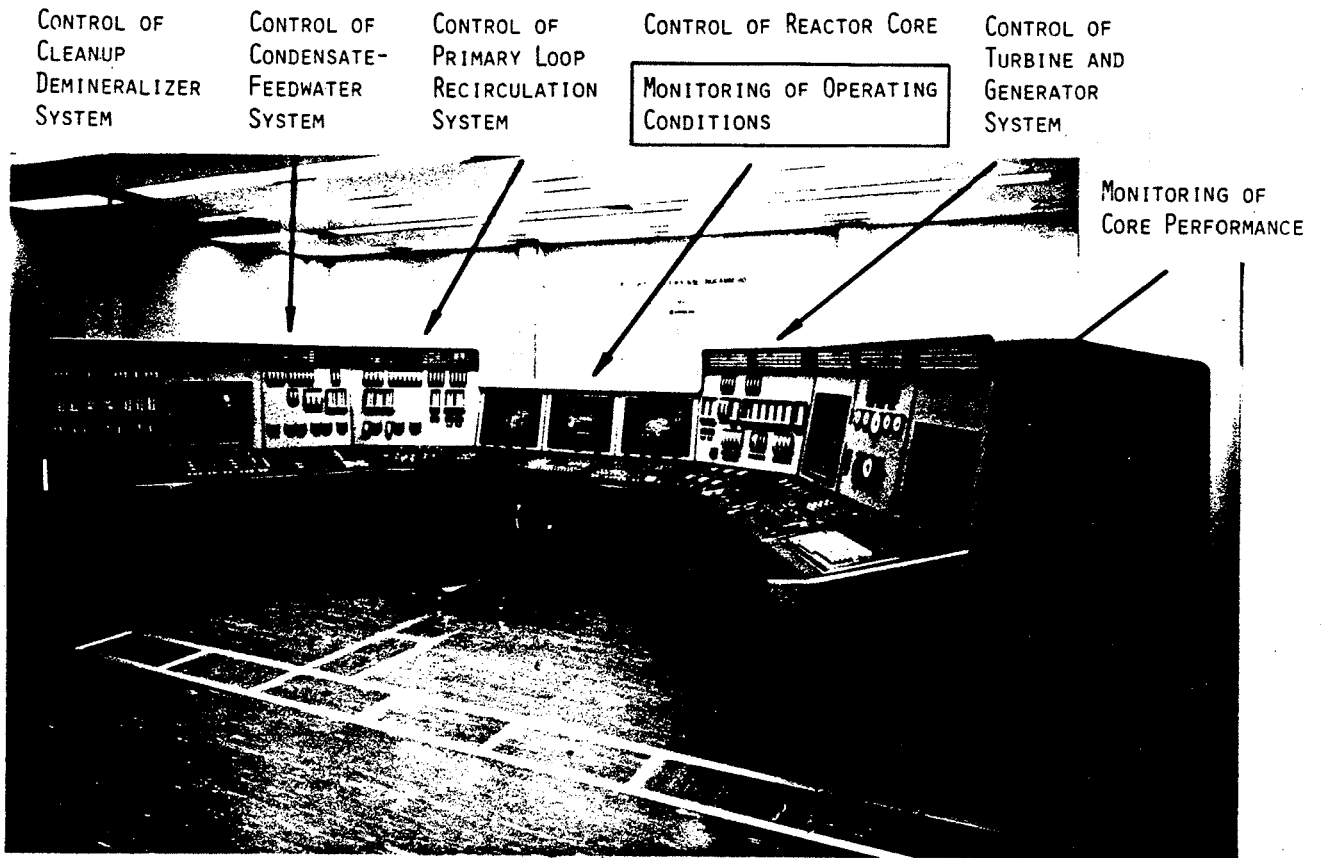


Photo. 1 Plant Operator's Console of NUCAMM-80

Table 1 Comparison between Conventional Console and NUCAMM-80

Item	Conventional Console	NUCAMM-80
Configuration	<p style="text-align: center;">Bench Board Type</p>	<p style="text-align: center;">Desk-Top Type</p>
Monitoring	<p>Instruments CRTs: 1-2 Indicators: 320 Recorders: 30</p> <p>Computers: 1 Core Performance Calculation</p>	<p>Instruments CRTs: 6 Indicators: 120 Recorders: 23</p> <p>Computers: 4 (Multi-Computer System) Core Performance Calculation Prediction of Power Distribution Plant Operation Monitoring (Display of Intensive Information)</p>
Operation	Switches: 600	Switches: 200 Automatic Startup and Shut-down

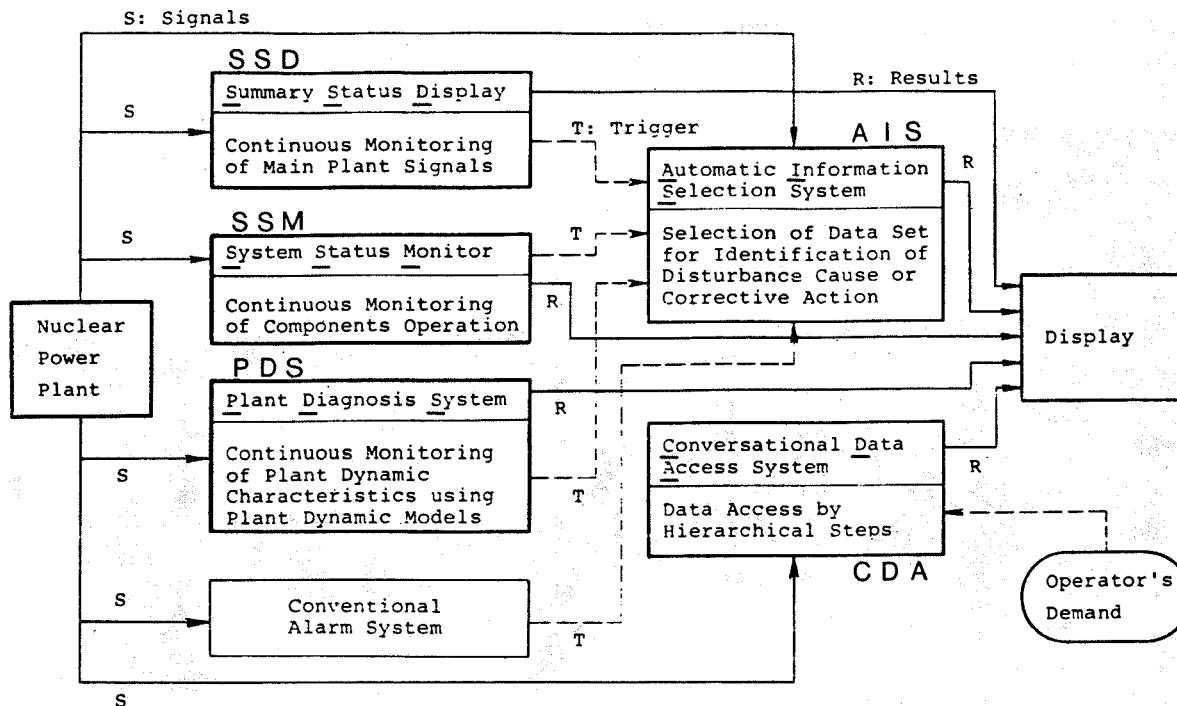


Fig. 1 Functional Diagram of Plant Operation Monitoring System by Computer Based Console



Photo. 2 Computer Based Plant Operation Monitoring Console

Table 2 Monitored Signals and Method to Calculate Reference Values

Signal	Reference Value	Unit
Main Steam Flow	Measured Value (W_{STM})	T/H
Reactor Pressure	Set Point + $0.0211 \times PWR + (0.0197 \times PWR)^2$	kg/cm ² g
Turbine Control Valve Position	$0.420 \times PWR - 4.00$	%
Turbine First Stage Pressure	$0.533 \times PWR - 2.87$	kg/cm ² g
Generator Power	PWR	%
Feedwater Temperature	$117.1 + 1.22 \times PWR - (0.0652 \times PWR)^2$	°C
Feedwater Flow	W_{STM}	T/H
Reactor Water Level	Set Point	mm
Reactor Power (APRM Reading)	PWR	%
Core Pressure Drop	$0.300 - 0.0650 \times W_T + (0.0583 \times W_T)^2$	kg/cm ² g
Core Flow	$5.60 \times W_D + 4100$	T/H
PLR Drive Flow	$22.1 \times (SP_A + SP_B) + 1282$	l/s

(Note) PWR : Core Thermal Power given by $0.0214 \times W_{STM} + 5.66$ (%)

$SP_{A,B}$: Measured Values of Speed Controller Output of PLR Pumps A and B (%)

W_D : Reference Value of PLR Drive Flow (l/s)

W_T : Reference Value of Core Flow (kt/H)

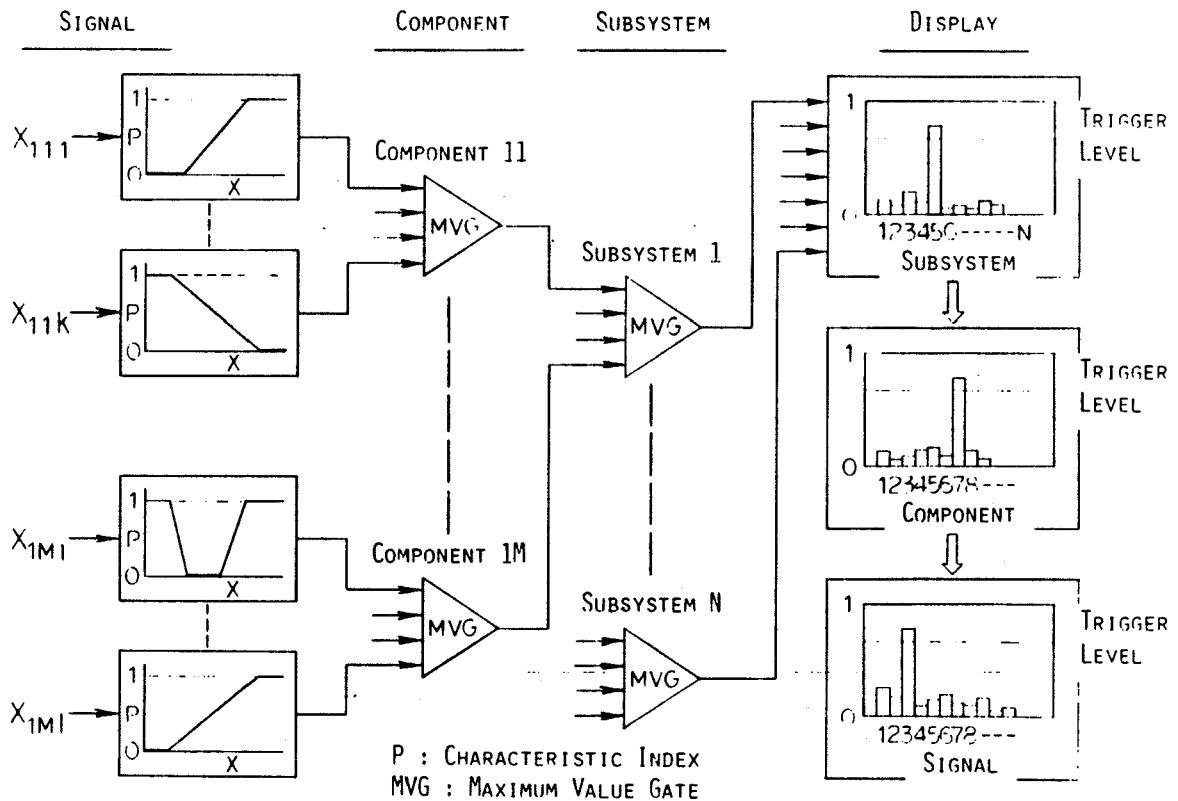


Fig. 2 Functional Diagram of System Status Monitor

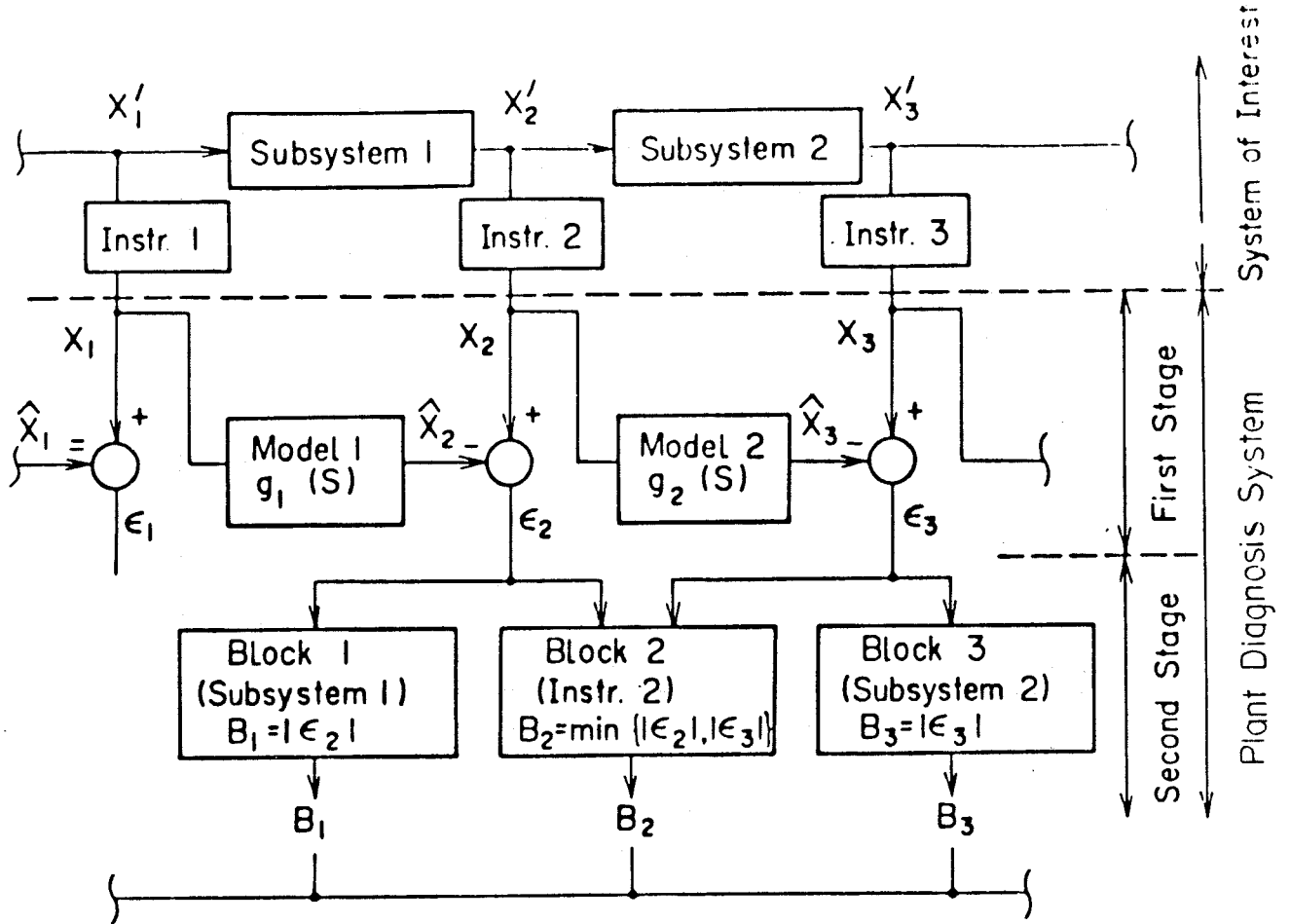
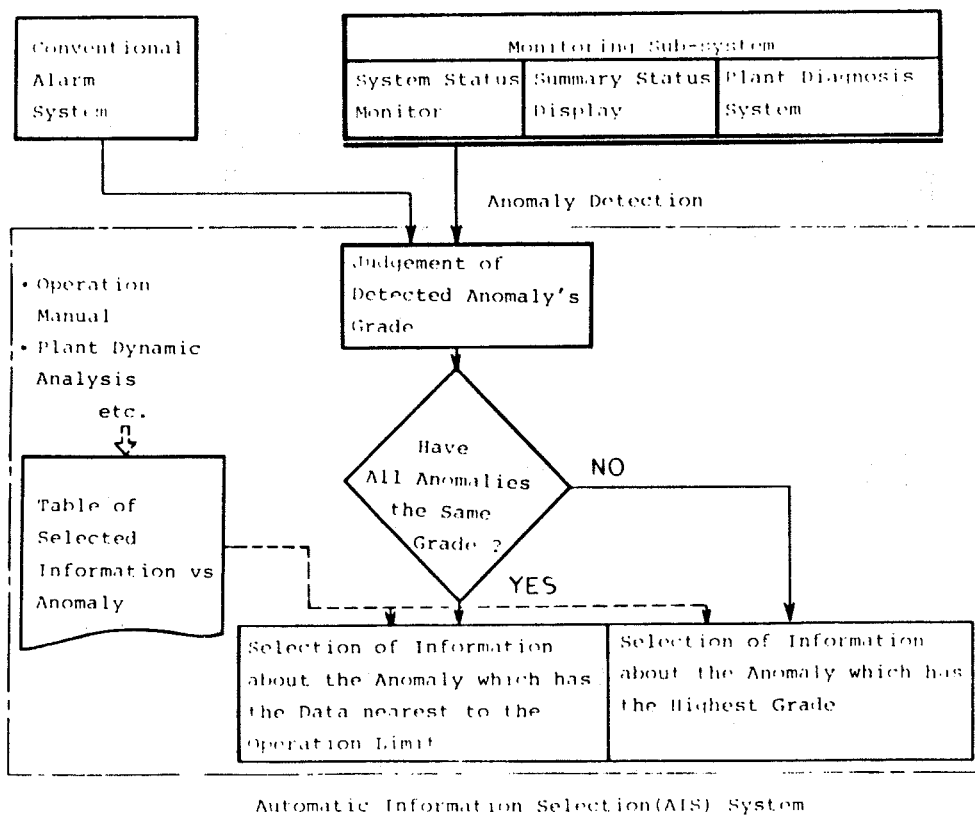


Fig. 3 Conceptual Diagram of Plant Diagnosis System



Automatic Information Selection(AIS) System

Fig. 4 Conceptual Flow Diagram of Automatic Information Selection System

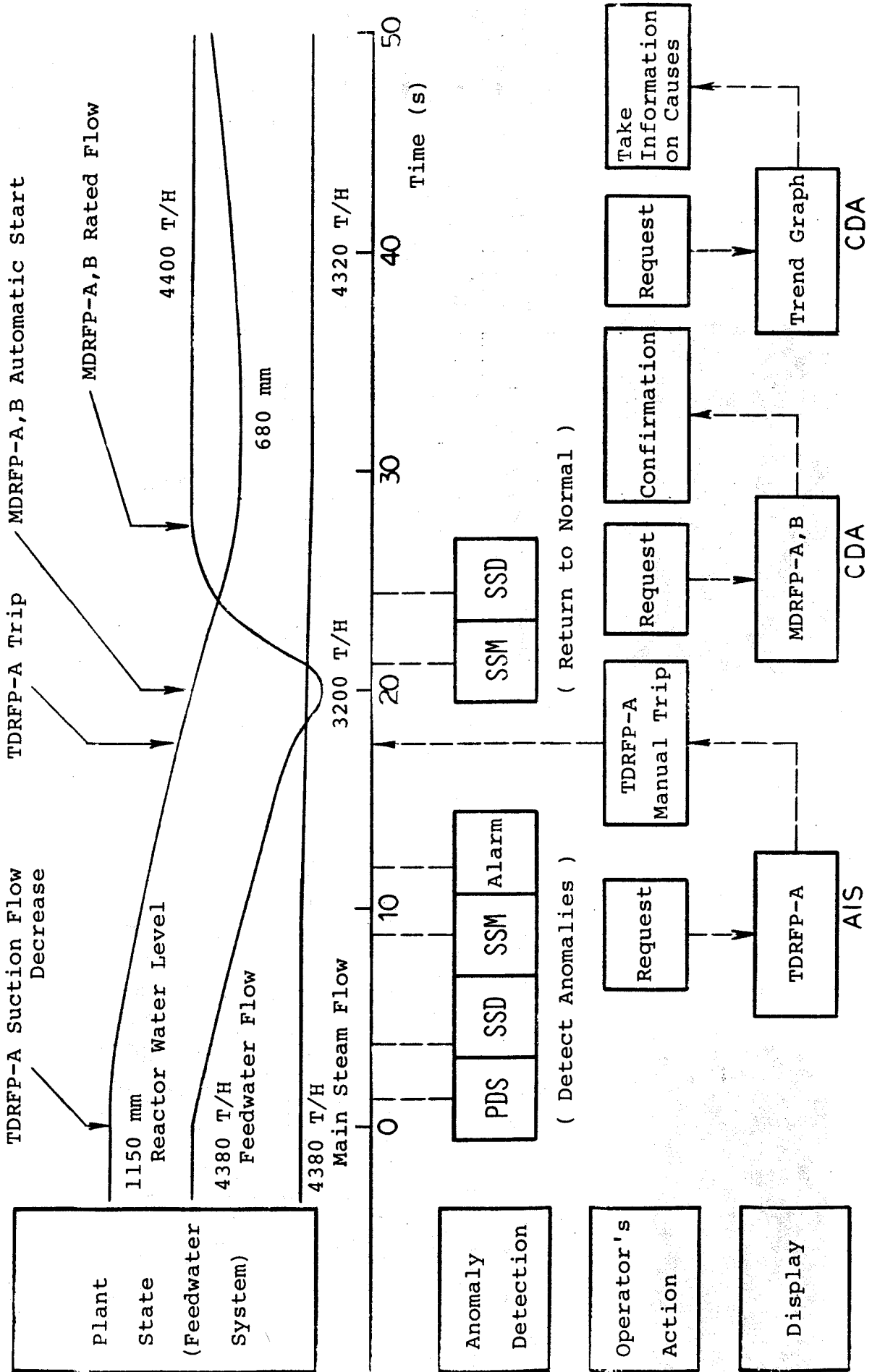


Fig. 5 Performance Test Results of Plant Operation Monitoring System

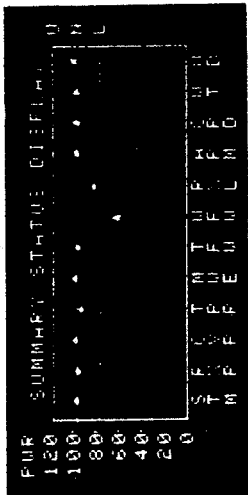


Photo. 3

Display Example
for Anomaly Detection
of SSD

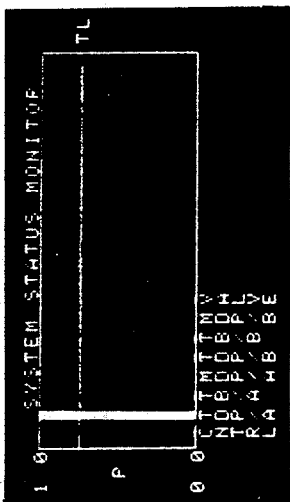


Photo. 5

Display Example
for Anomaly Detection
of SSM

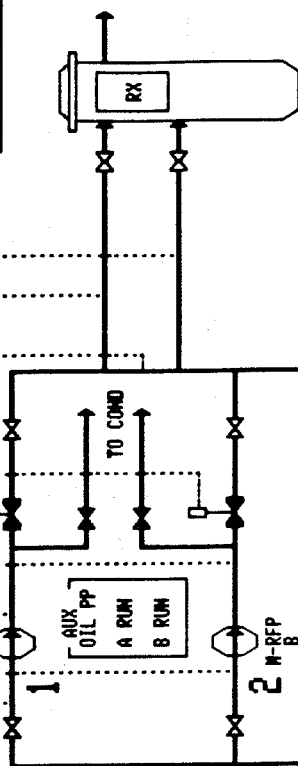
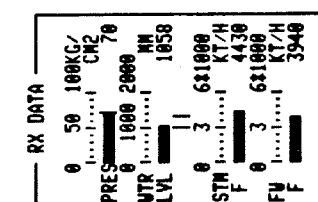
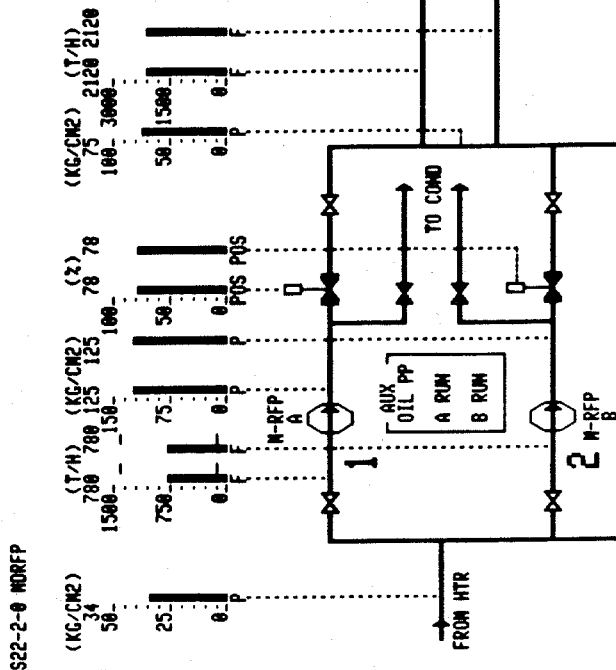
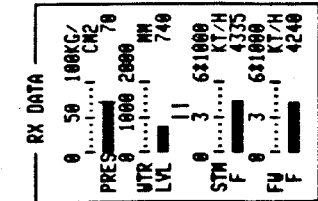
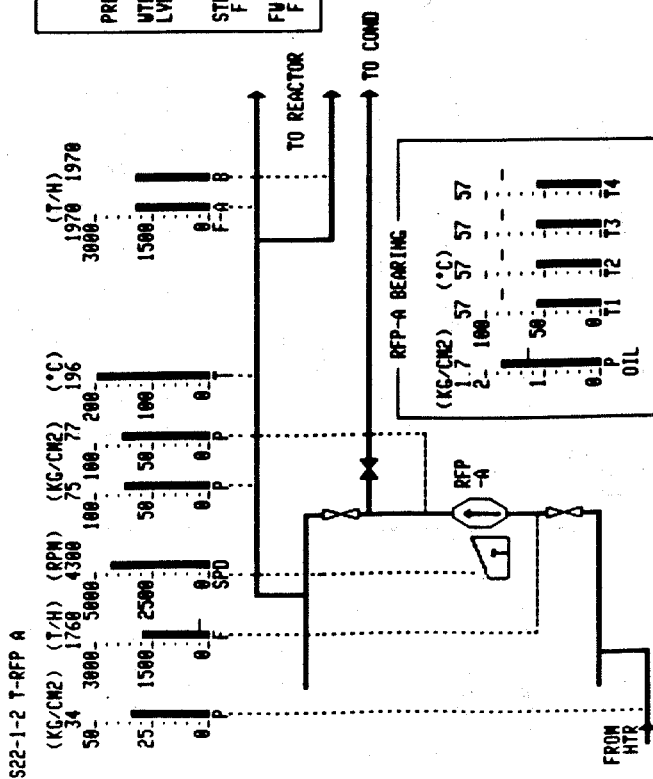


Photo. 4 Display Example for Data Set of TDRFP-A

Photo. 6 Display Example for Data Set of MDRFP-A,B

OF TDRFP-A

OF MDRFP-A,B

L. Bürger, E. Végh

MAN-MACHINE COMMUNICATION IN EXPERIMENTAL REACTOR CONTROL
SYSTEM

MAN-MACHINE COMMUNICATION IN
EXPERIMENTAL REACTOR CONTROL SYSTEM

L. BÜRGER, E. VÉGH

CENTRAL RESEARCH INSTITUTE FOR PHYSICS, BUDAPEST

INTRODUCTION

Man-machine communication plays a vital role in control systems because it is not enough just to measure and control a process, it is also essential that an operator always be well informed on the events within a short time. Here "short time" means an interval within the order of an operator's perception time.

This paper describes the man-machine interface of an experimental control system of a WWR-SM research reactor. This 5 MW reactor of the Central Research Institute for Physics, Budapest, has a computer system which has been operating for 3 years. The configuration began operating in 1976 as a data acquisition system /1, 2/ and it has been playing an active role since July 1978 /3/. In the control mode the computer controls in DDC regime the neutron level and the outlet temperature of the primary cooling circuit. The two DDC loops operate more or less independently under the supervision of a coordinator program which tunes their operation to the operator's requirements and to the actual state of the reactor /4/.

The configuration is based on an R-10 small computer which is the licenced Hungarian version of the French MITRA-15. The system needs 24 Kword core memory /16 bits word length/ and a fixed head disc with 800 Kbytes capacity. The used real-time operating system is the PROCESS-24K program package /5/.

This paper provides an overview of the man-machine interface of the system but it is mentioned that the colour display programs are not yet complete.

DATA STRUCTURES

The computer system must provide information on the instantaneous values of measured/calculated variables and alarms, moreover on the history of selected variables. These two types of data recording need two different data structures, namely

- a core resident data base where the instantaneous values and existing alarms can be accessed in a random way,
- a disc resident buffer with sequential organization for storing the history of the past.

The core resident memory is divided into two parts, viz.

- a primary data base stores the instantaneous values of the variables,
- a secondary data base reflects the results of the alarm analysis.

For practical reasons the primary data base is divided into pages of 256 bytes. Each page is assigned to a group which contains programs with the same starting condition. There is room for 48 variables on a page; each variable has a 4-byte long floating point value and a flag byte. The latter records the states of the variable, i.e. alarm limit violations, invalid measurements, etc. In the core resident data base there are 48 pages. The structure of a page can be seen in *Fig. 1*.

In the secondary data base a double word is assigned to every alarm event taking part in the alarm analysis. The structure of a double word is presented in *Fig. 2*. The first byte reflects if the alarm actually exists and if it is valid /it is possible that an alarm is invalid when, for example, the relevant measurement is inhibited/. The next byte points

to the first alarm tree on which the alarm event appears. The last two bytes store the identity code of the event. The secondary data base can store 640 alarm events.

When past events are required, the time resolution of the records depends on the age of the event in which the operator is interested. Our system has three memories for the past

- a short range memory with a time span of 15 minutes; a time resolution of 4 sec,
- a medium range memory with a time span of 1 hour; a time resolution of 20 sec,
- a long range memory with a time span of 4 hours; a time resolution of 60 sec.

All three of these memories are circular buffers, where the newest sample overwrites the older one. Every sample is one sector long /256 bytes/ and can store 48 variables. The first 4 variables to be recorded can be selected by the operator so their identity codes are stored in the sample. The other variables are system constants, they are stored in another table. The structure of a circular buffer is shown in *Fig. 3*.

The data transfer among the different memories is presented in *Fig. 4*. The primary processing /measuring, scaling, validity checking, alarm checking, etc./ produces a primary data base. When an alarm occurs, the alarm analysis program is activated and this reflects the actual state of alarms in the secondary data base.

A sample is composed every 4 seconds from the data of the primary data base and every sample is stored in the short range buffer, every 5th sample in the medium range buffer and every 15th in the long range one. Every half hour the last sample of the long range buffer is stored in a temporary, so called, "day" buffer. At midnight the contents of the day buffer /i.e. 48 samples/ are archived on magnetic tape.

The contents of the short range buffer are also recorded when a "post-mortem event" occurs. A program archives the short

range buffer 7 minutes after the "post-mortem event", in this way the 8 minutes preceding and the 7 minutes after the incident can be analysed later.

DATA PRESENTATION

Because people are generally visual types, the most convenient device for the presentation of data to operators is the CRT display. In our case there are three CRT's built into the control desk, two of them are alphanumeric, the third is a semigraphic colour device. Data-presentation supporting the operator's work in the normal reactor state is different from that in the abnormal state. In the normal state the data must be able to control the momentary values of the most important technological measurements and to give a general overview on the trend of the change of several very important variables. In abnormal operating states the presented data must give a complete image of the state of the plant and it must help the operator's decision. The first alphanumeric display serves to present data in normal states, the second one is the "alarm" display. The semigraphic CRT is used for trend and mimic diagrams.

DATA PRESENTATION IN NORMAL OPERATING STATE

The pictures presented in normal operating states are the following

- different kinds of technological logs on the first alphanumeric display, in tabulated form,
- mimic diagrams of the technology containing the relevant information and coloured according to the existing alarm state,
- trend diagrams: simultaneous plotting of 2 functions against time.

The last two diagrams are presented on the semigraphic colour display.

The technological logs contain

- data of different parts of the reactor /zone, primary and secondary coolant circuits, pumps, etc./,
- data necessary for certain procedures /start-up, change of power level by DDC control, etc./.

Ease of survey was our main point of view when constructing these logs therefore the actual values of the collected variables are presented in analogue /histogram/ and in numerical form. An example is shown in *Fig. 5*. The operator is able to select from these pictures by using a set of pushbuttons. The values of the picture will be updated automatically with a 15 sec cycle time. Updating is rapid because only those elements to be modified are sent to the display.

The mimic diagrams have a similar purpose to the technological logs, but in this case the values are shown only in numerical form written into the technological scheme of the relevant part of the reactor. *Fig. 6* is an example of this form of presentation.

The colour of the different elements on the scheme may change according to the operating state, e.g. the colour of a valve symbol is red if it is open, white if it is closed. The colour of a numerical value depends on its alarm state.

The method of picture selection and cyclical updating is the same as for technological logs.

The used colour display unit has a diagram plotter option which thereby enables it to plot 4 diagrams against time with different colours. The plotting occupies only a part of the CRT /256x256 points from the 448x288/, and it is possible to superpose it on a picture occupying the whole screen. The display hardware contains 4 separated memories /256 bytes/ to store the data of the 4 diagrams. The contents of the memory cells may be shifted when a new data item is sent into the last cell. In this way it is possible to represent the change of variables against time. Two kinds of trend logs may be presented on this display:

- a/ short trends of optional two variables selected by thumbwheel switches from the whole set of measurements,
- b/ short, medium, long or archive trends of two variables selected by thumbwheel switches from the group of variables whose previous values are stored in the circular buffers.

In case a/ the values of two selected variables are collected only in the display buffers. The loading of these buffers is independent of visualization, it is performed with 15 sec cycle time. Having requested the trend diagram, the operator sees the contents of these buffers, i.e. the values of the variables in the past 1 hour, approximately. After 15 sec new values will appear at the top positions of the diagrams and the other values will therefore move downwards on the screen.

In case b/ the operator may choose from among the different circular buffers. Then the data referring to two selected variables from the whole content of the chosen buffer is loaded from the disc into the display memory and presented on the screen. In this case there is no cyclical updating.

If the archive log was selected, the operator has to indicate the date of the archivations of the desired values. This can be done by another thumbwheel switch. The data of 5 days beginning with the given date are then loaded from the tape into the memory, and presented on the CRT. An example of the trend log presentation is given in *Fig. 7*.

It is possible to make a listing of the contents of the just presented trend logs on the line printer.

DATA PRESENTATION IN ABNORMAL OPERATING STATE

Three kind of data presentation support the operator's work in this case:

- the alarm list, containing all the variables which violated their limits and the deductions of the alarm analysis,

- the alarm-trees, showing the operator the "alarm patterns" from which the deductions were made,
- the post-mortem log, containing the values of the selected variables before and after the post-mortem event with 4 sec time resolution.

All the actual alarms are enumerated on the alarm list. Fresh alarms, which are not already acknowledged, are marked with a "+" sign. If the alarm analysis program analysing the actual alarm pattern finds the possible cause of the abnormal situation, it is presented in the alarm list as well. A hard copy is made from the contents of the list on the typewriter making the "event log".

Only 12 alarms can be presented on the screen of the "alarm" display. If the alarm list is longer, the operator can fold its pages in a forward or a backward direction.

The operator can see the logical construction from which the presented cause was deduced. On the CRT only the alarm trees containing actual alarms and deductions are presented. If the binary tree has more than four levels /15 nodes/ it is divided into parts and so presented. The operator is able to fold the pages of this book of alarm trees using pushbuttons.

In our system there are about 100 analogue measurements and approximately 100 digital state marks so the size of the alarm trees is generally not enormous, consequently the suppression of too many data from the analysis is not one of our problems.

The data collected just before and just after the post-mortem event are listed on the line printer only, they are then archived on magnetic tape for further analysis.

REFERENCES

- /1/ J. Péter, E. Végh: Data acquisition program for a nuclear research reactor. 2nd International Conference on Centralised Control System. London, 1978, IEE publ. No. 161, p. 131.
- /2/ L. Bürger, E. Zobor: On-line alarm analysis of the WWR-SM research reactor. International Symposium on Nuclear Power Plant Control and Instrumentation. Cannes, 1978.
- /3/ E. Zobor et al.: Direct digital control of the WWR-SM research reactor. European Nuclear Conference, Hamburg, 1979.
- /4/ E. Zobor et al.: Final Report on the IAEA Research Contracts No. 1194/RB, 1194/R1/RB and 1194/R2/RB. /In press/
- /5/ L. Bürger, E. Végh et al.: PROCESS-24K - an efficient process control system. Report KFKI-1978-17.

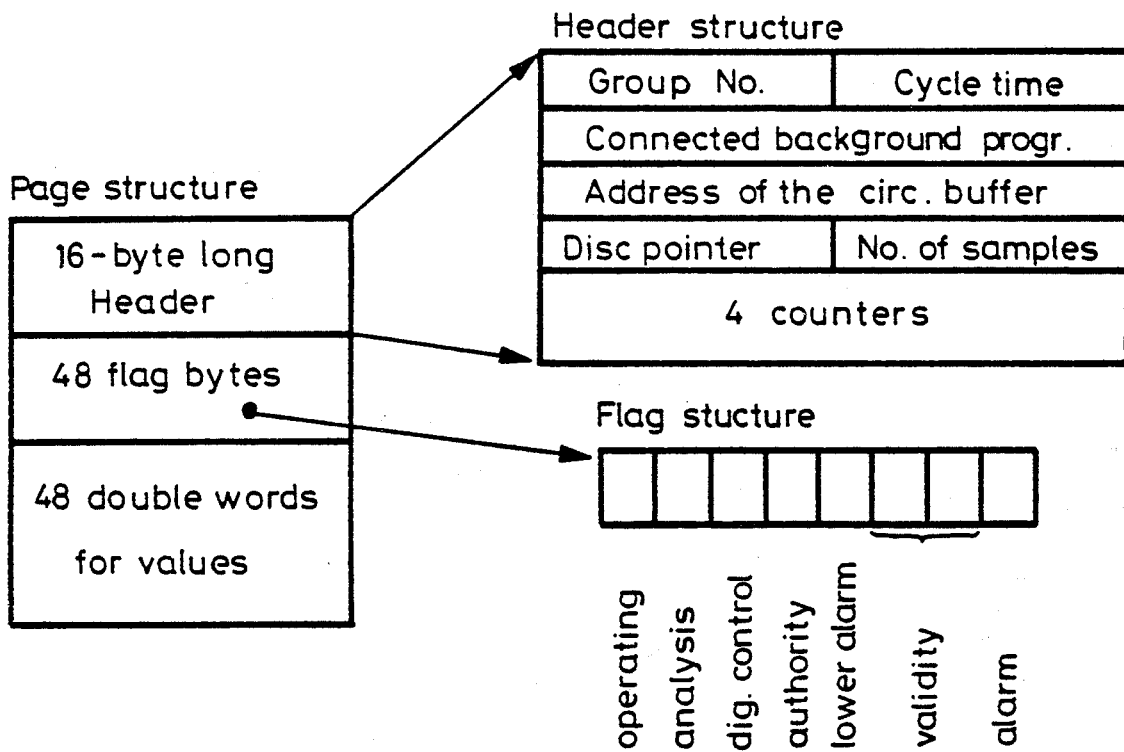


Fig. 1.
Organisation of the primary data base.

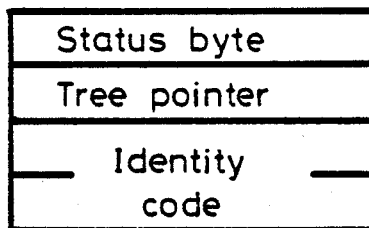


Fig. 2.
Structure of a secondary data base element.

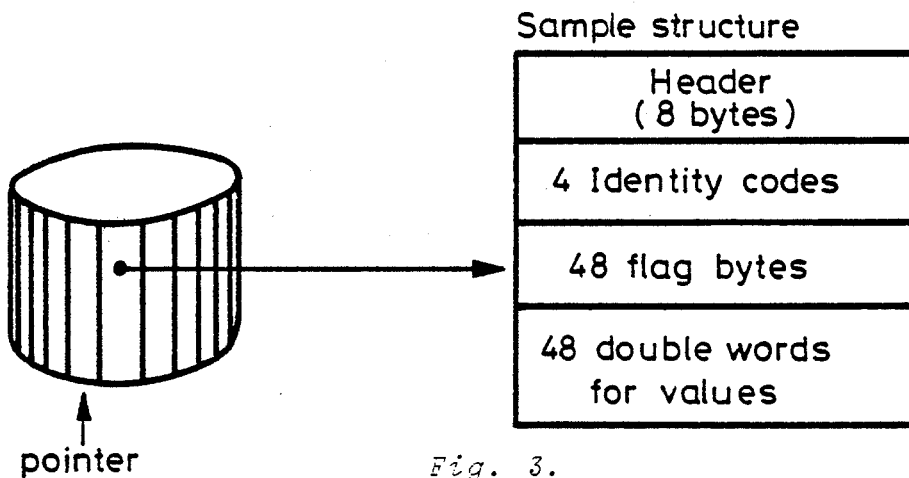


Fig. 3.
Structure of a circular buffer.

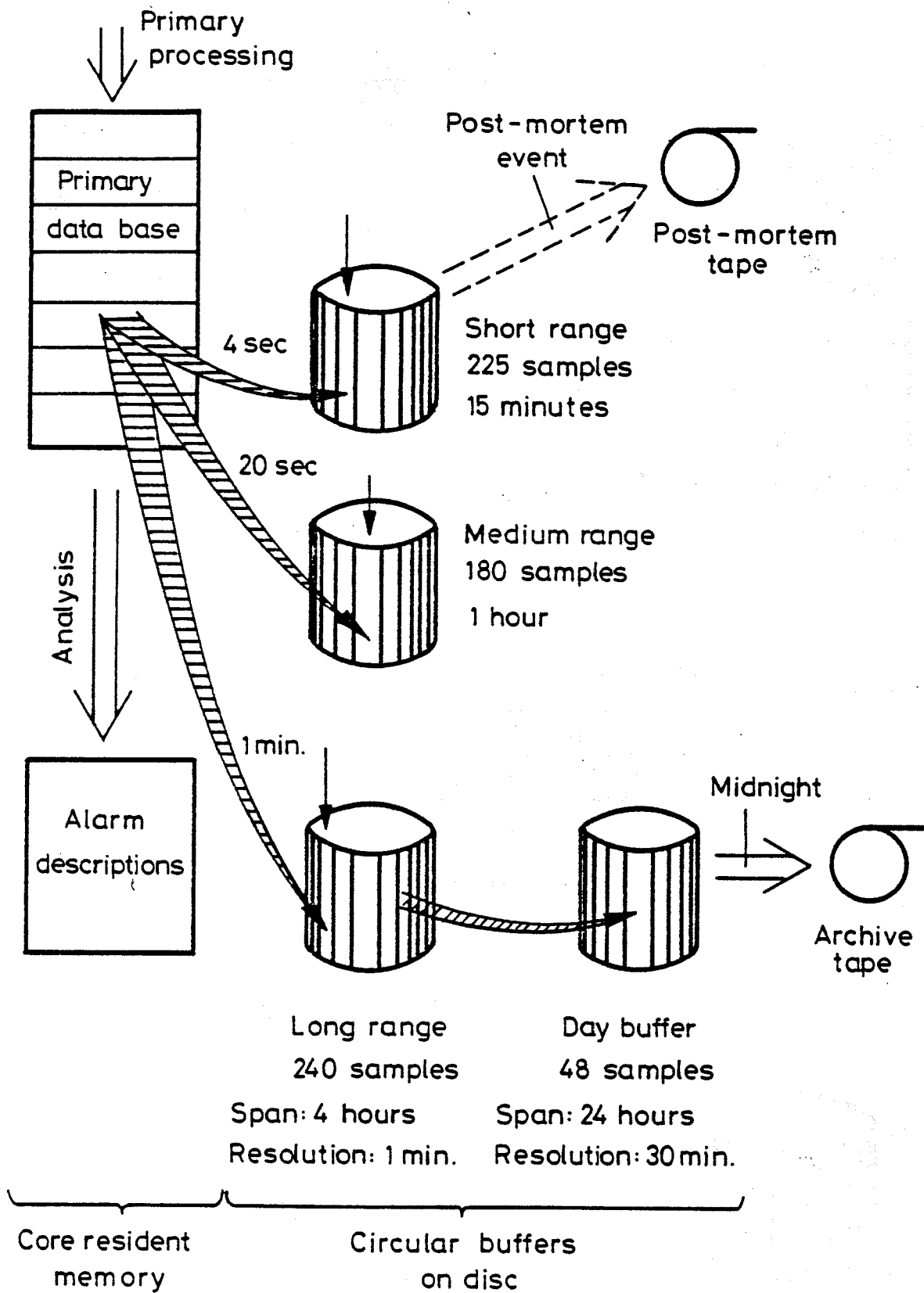


Fig. 4.

Data transfer among the memories.

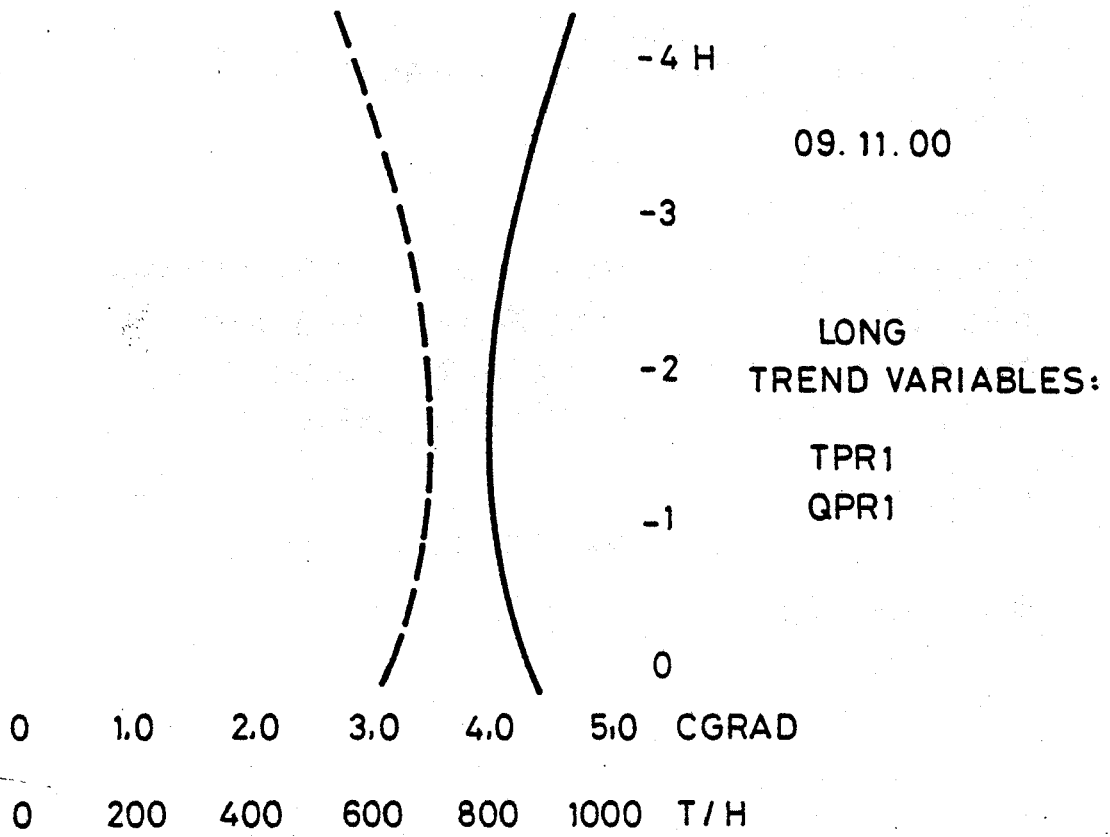


Fig. 7.
Trend log presentation.

W.E. Büttner, L. Felkel, R. Grumbach, F. Øwre, B. Thomassen
FUNCTIONS AND DESIGN CHARACTERISTICS OF THE STAR DISTURBANCE
ANALYSIS SYSTEM

FUNCTIONS AND DESIGN CHARACTERISTICS OF THE STAR
DISTURBANCE ANALYSIS SYSTEM

W.E. Büttner, L. Felkel, R. Grumbach†
Gesellschaft für Reaktorsicherheit (GRS) mbH
Garching, Germany F.R.
F. Owre, B. Thomassen
Institutt for Atomenergi
Halden, Norway

Abstract

The experimental version of the STAR system has been installed at the Grafenrheinfeld Nuclear Power Plant. This paper outlines the functional requirements and the functional layout of the state of the art disturbance analysis system. To supply some orientation for potential users, the minimum hardware equipment is shown for the on-line system. There are special time constraints imposed on the performance of the analysis. These are different for each plant subsystem to be analyzed. The paper also singles out those plant subsystems which are particularly apt for disturbance analysis. Another topic will be user aspects in handling the disturbance analysis system as well as ergonomic considerations.

A practical example of a plant system, a disturbance and the on-line analysis of this disturbance is presented. This example is also meant to inform the participants about a STAR demonstration which is planned at the end of this meeting.

†The authors are deeply moved by the sudden and unexpected death of their friend and colleague Dr. Rainer Grumbach.

1. Basic objectives and functional requirements

Owing to severe safety regulations in nuclear power plants, an extraordinary amount of instrumentation is necessary to guarantee a high safety standard. A large portion of the signals coming from the instrumentation is input to the reactor protection system and an even larger portion is available in the control room. The excessively large amount of information given to the operator in nuclear power plants is a consequence of quantitative upgrading control rooms of conventional power plants to meet the requirements in nuclear power plants, disregarding the fact that this might cause problems in the "man-machine-communication".

To improve the man-machine-communication interface, there are basically two problem areas to be investigated.

These are

- the development of computer based systems to assist the operators with processing the vast amount of information
- the development of an advanced control room concept which comprises and integrates modern systems for control and surveillance, to take full advantage of the operators capabilities and to optimize the operators performance/7/.

The STAR^{*} system the paper deals with can be considered to be one functional module in such a future control room. The STAR disturbance analysis system has been designed to improve both plant availability and plant safety.

Plant availability will be increased because the disturbance analysis system is to inform the operator about disturbances at their very beginning, so that he can take appropriate corrective action to prevent unnecessary shutdown. There is also a significant gain in reactor safety, since the disturbance analysis system may reduce thermal and mechanical stress on components and equipment, and because it is likely that disturbance situations may be recognised and precautions taken before they develop into severe incidents. TMI-2 serves as a good example here.

* Abbreviated from Störungsanalyserechner (disturbance analysis computer)

The objectives of the STAR disturbance analysis are:

- to recognise plant disturbances, depending on the plant mode of operation, as early as possible, determine the prime causes and the possible consequences, and provide information about the process status.
- If it is unambiguously possible, the best or suitable recovery action should be given to the operator.
- The operator must be involved in the analysis procedure, i.e. he must be able to select from the information available, rather than the information be forced upon him; the operator should also be able to supply information to the disturbance analysis system, which can not be assessed by instrumentation.
- The information about the process data and the disturbance should be supplied within a reasonable amount of time, i.e. the analysis must be performed much faster than the disturbance propagates.
- The quality of the information displayed to the operator should be improved by a disturbance analysis system, relieving the operator from nuisance information.
- Making extensive use of process computer resident data bases comprising a priori information about expected disturbance propagations, and operating and maintenance instructions.
- The disturbance models (cause-consequence diagrams) have to be sufficiently complex to properly represent the process and yet simple enough to be unambiguous and to be analysed quickly.
- The models should be flexible so that they can be extended or modified easily, which may be necessary due to experience gained.
- The methodology lying behind the models should be sufficiently general so that it can be applied to any kind of technological process.
- The models produced for similar plants should not contain significant differences to allow the transfer from one plant to another without excessive costs.

With the testing and the installation of the STAR disturbance analysis system in the Grafenrheinfeld Nuclear Power Plant it was shown that the above mentioned objectives and functional requirements were met. However, only a long-term performance evaluation /1/ will uncover whether or not the anticipated impact on safety and availability was justified.

2. Necessary hardware requirements

In the Grafenrheinfeld STAR system there are three computers used for performing all necessary functions. This, however, has a political rather than a technical background.

The on-line process data are obtained from the plants supervisory computer. This is because it was the simplest and cheapest way to connect a disturbance analysis system to a nuclear power plant under construction, where planning was completely independent of the application of a DAS. Furthermore, it was relatively easy to guarantee that there will be no backfittings from the DAS to the control system. For disturbance analysis there are two computers in Grafenrheinfeld. One is mainly concerned with the analysis, the other with communication and display functions. The reason for two computers is just owing to the cooperation between Institut für Atomenergie and Gesellschaft für Reaktorsicherheit, who have developed the ALKOM and ALSAN modules resp. quite independently. The result was a significant saving in development costs for the pilot project.

The actual system set-up is shown in detail in /1/. It is envisaged, that, to gain all the more experience with a DAS, the STAR system should be applied to another plant, of a similar type as the Grafenrheinfeld plant, but one which is operational. Since the ALKOM and ALSAN modules are completed by now, they will be integrated and implemented on one computer system.

The size of this process computer system will be in the range of 128 K words and a 10 MB disk unit. The computer will be connected to the plant instrumentation directly and thus does not need the data-base of the supervisory computer anymore. As in the present set-up two display controllers and two colour cathode ray tubes are considered sufficient for disturbance analysis.

The objectives of a second STAR application are not only to increase the amount of data about usefulness of a DAS but also to test new techniques concerning software validation. The ALSAN and ALKOM modules will be one integrated part and will be translated into the high level process language PEARL /6/. This will also ease transferability to other plants and

computer systems. Experience in the application of PEARL to problems of disturbance analysis is an anticipated and welcome by-product.

3. Plant systems analysis and plant models

The analysis of component failures and disturbances in nuclear power plants or at least parts of the plants by a process computer is achieved by examining cause-consequence diagrams which have been designed for the respective plant subsystems and which are on-line supplied with process signals. The cause-consequence diagrams can thus be considered models for possible disturbance propagations within a certain plant subsystem or disturbance propagations into other subsystems.

The construction of the cause-consequence diagram begins with a thorough systems analysis of those subsystems which are of particular interest to the objectives of disturbance analysis. Systems analysis must be carried out very carefully, since the results of the on-line disturbance analysis may crucially depend on a match between anticipated and occurred flow of events during a disturbance situation. Special attention is to be focused on the problem, that there must not be any erroneous information to the operators even in extraordinary process statuses, by analog or binary signal failures or during disturbances fading away.

Systems analysis is based on general knowledge of the behaviour of nuclear power plants like evaluation of reports on disturbances and results gained during the commissioning phase, knowledge of technical functions and characteristics of, say, pumps, turbine, generator etc., knowledge of the control system and experience gained in the construction of plant simulators. There is no "general purpose" plant model which could be used in all nuclear power plants, therefore, plant specific documents like system descriptions, function schemes and circuit diagrams are a necessary prerequisite.

Of major interest is the validation of the cause-consequence diagrams. At the moment this is done by cross-checking the cause-consequence diagrams by several independent specialists and by testing the cause-consequence diagrams on-line during the commissioning phase of the nuclear power

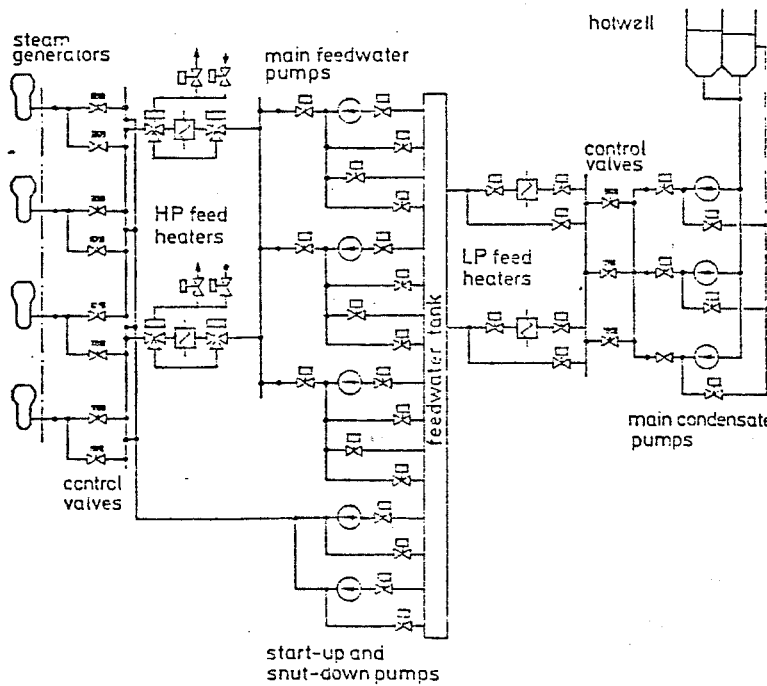


Fig. 1: 530 M SCHEMATIC DIAGRAM OF THE FEEDWATER AND CONDENSATE CIRCUIT

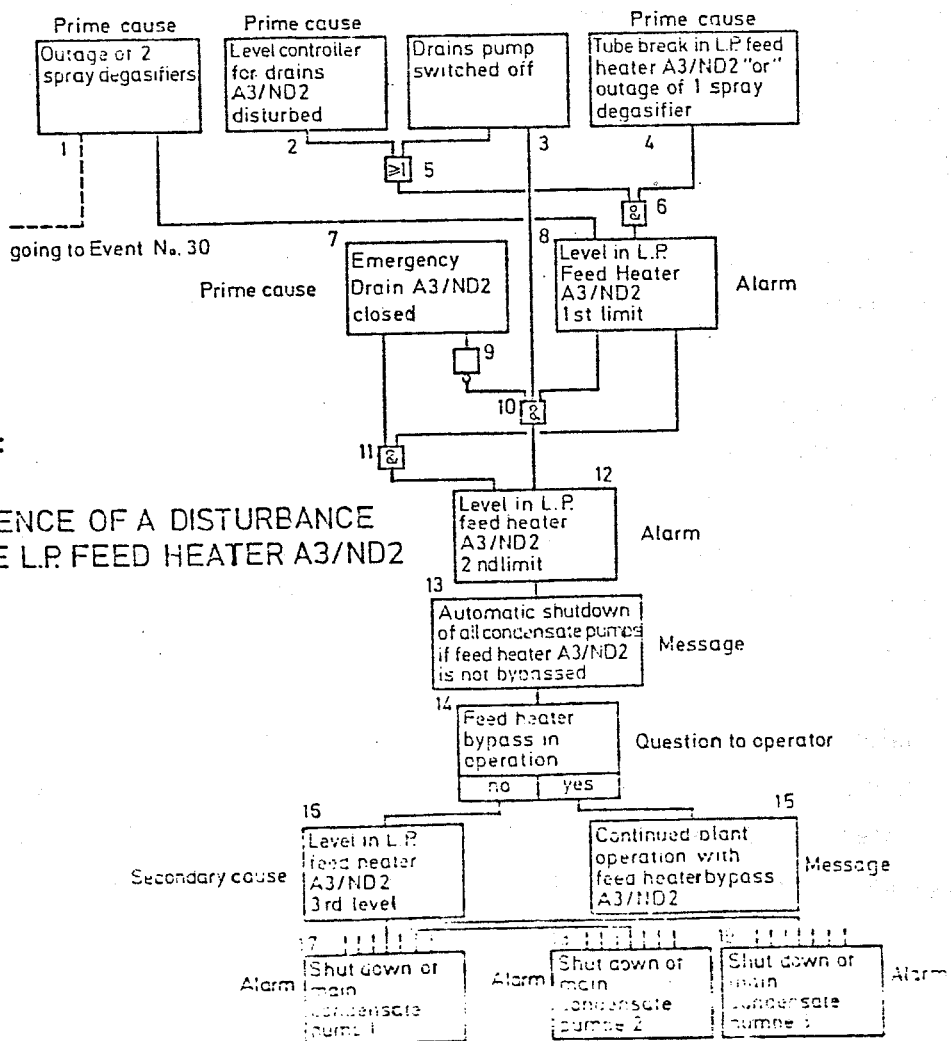


Fig. 2:

SEQUENCE OF A DISTURBANCE IN THE L.P. FEED HEATER A3/ND2

plant. There are however, ways and means being investigated of how a validation of the cause-consequence diagrams can be systematized and partly automated/8/. Detailed information about the structure and the construction of cause-consequence diagrams has been given in earlier reports to which the inclined reader is referred/2, 3/. At the time being there are for the Grafenrheinfeld STAR application five systems contained in the non-nuclear part of the plant for which cause-consequence diagrams have been constructed. These systems are

- the main condensate pumps
- the main feed pumps
- start-up and shut-down pumps
- secondary cooling water loop
- conventional component cooling water system.

The five systems modeled here comprise approximately 700 events which have a logical or chronological relationship.

Sample cause-consequence diagram

A simple example is used in the following to describe a cause-consequence diagram and the result of the disturbance analysis, should there be a disturbance in the system concerned.

Fig. 2 shows a small part of a cause-consequence diagram for the main condensate pumps (fig. 1).

A basic assumption is that the drains pump for the low pressure feed heater is either switched off or in repair (event 3). If there is a tube break in the low pressure feed heater or a spray degasifier in the feed water tank is lost, this event cannot be verified by process instrumentation (this is specific to the Grafenrheinfeld application, other plants may have instrumentation for determining the occurrence of such an event; however, cause-consequence analysis may as a by-product detect gaps in the process instrumentation). However, there will be an increase in the water level of the feed heater. This increase will continue until a first limit is reached (event 8). This is the first observable event from which the disturbance analysis system will conclude that the primary cause can only be the tube break in the low pressure feed heater (event 4). At this

point already, appropriate corrective actions could be taken. In case the corrective action is not taken the water level will continue to rise and will exceed a second limit (event 12). The control system automatically isolates the defective low pressure feed heater after the second limit has been exceeded and the appropriate pre-heater will be by-passed. This may not be successful, in which case an emergency shut-down of all main condensate pumps is imminent. The operator will be notified about this situation by an appropriate message. In the Grafenrheinfeld Nuclear Power Plant the status of the valves for the pre-heater by-pass is not available on the process computer and there is only the operator to know whether or not the pre-heater by-pass was successful. The disturbance analysis system therefore asks the operator an appropriate question (event 14). The operator can answer the question because there are signals in the control room about the status of the pre-heater by-pass. The question is answered by means of a special keyboard in the disturbance analysis system. If the preheater by-pass was unsuccessful there will be still continued increase of the water level in the low pressure feed heater which, after the excess of a third limit causes the automatic shutdown of the two operational main condensate pumps and prevents that the standby condensate pump will be started. As a consequence the feed water tank will be emptied by and by, which eventually leads after some time to the shutdown of the main feed pumps.

Formal description of the cause-consequence diagram to be input to the model generator MOGEN

Cause-consequence diagrams cannot readily be input to the process computer. They have, therefore, to be translated into a form suitable for electronic processing. For this purpose the model generator program MOGEN has been devised/4, 5/. The method used here also guarantees, that the cause-consequence diagrams stored in the process computer can be adapted to the latest status of plant instrumentation, or to revisions in systems analysis. Table 1 gives as an example the verbal description of the cause-consequence diagram shown in fig. 3 (for the main condensate pumps). The formal description is based upon some easily apprehensible rules and does on one hand not impose any burden on systems analysts and on the other can be processed by the model generator program. Our experience proved the average learning time being approximately one day for even a data typist.

Table 1: MOGEN description of the example in fig. 3

System: 'Main Condensate System':

Event: 1

Documentation: 'Outage of two spray degasifiers';
Properties: Deduced by E-8 & E-30,
Prime-Cause;
Successors: E-8, E-30;

Event: 2

Documentation: 'Level Controller for drain A3/ND2 disturbed';
Properties: Deduced by E-8 & E-30 & E-3,
Prime-Cause;
Successors: L-5;

Event: 3

Documentation: 'Drain pump switched off';
Properties: Bit-No = xxxx;
Successor: L-5, L-10;

Event: 4

Documentation: 'Tube Break in L.P. feed heater A3/ND2
OR Outage of one spray degasifier';
Properties: Deduced by E-8 & E-30,
Prime-Cause;
Successor: L-6;

Logicunit: 5

* OR *
In: E-2, E-3
Out: L-6;

Logicunit: 6

* AND *
In: E-4, L-5
Out: E-8;

Event: 7

Documentation: 'Emergency drain A3/ND2 closed';
Properties: Deduced by E-12 & E-3,
Prime Cause;
Successor: L-9, L-11;

Event: 8

Documentation: 'Level in L.P. feed heater A3/ND2 HIGH';
Properties: Bit-No = xxxx,
Alarm;
Successor: L-10, L-11;

Logicunit: 9

* NOR *
In: E-7
Out: L-10;

Logicunit: 10

* AND *

In: E-3, E-8, L-9

Out: E-12;

Logicunit: 11

* AND *

In: E-7, E-8

Out: E-12;

Event: 12

Documentation: 'Level in L.P. Feed heater A3/ND2 VERY HIGH';

Properties: Bit-No = xxxx,

Alarm;

Successor: E-13;

Event: 13

Properties: Message: 'Automatic shutdown of all main condensate pumps if feed heater A3/ND2 is not bypassed';

Successors: E-14;

Event: 14

Documentation: 'Feed heater bypass A3/ND2 in operation?';

Properties: Question to operator;

Successor: YES: E-15 NO: E-16;

Event: 15

Properties: Message: 'Continued plant operation with bypassed feed heater A3/ND2';

Event: 16

Documentation: 'Level in L.P. feed heater A3/ND2';

Properties: Bit-No = xxxx,

Secondary-Cause;

Successor: E-17, E-18, E-19;

Event: 17

Documentation: 'Shutdown of Main Condensate Pump 1';

Properties: Bit-No = xxxx,

Alarm;

Event: 18

Documentation: 'Shutdown of Main Condensate Pump 2';

Properties: Bit-No = xxxx,

Alarm;

Event: 19

Documentation: 'Shutdown of Main Condensate Pump 3';

Properties: Bit-No = xxxx,

Alarm.

The principal objectives selecting the plant systems to be modeled to comprise all disturbances which eventually influence the level in the steam generators. In this respect modeling for the Grafenrheinfeld STAR application is not complete. It would be desirable to model also the live steam system, the turbine system, and the deionised water system. After completion of this task all essential parts in the secondary (non-nuclear) system have been treated.

The present realisation of the models for the Grafenrheinfeld plant was restricted because only those analog and binary signals could be used which were available on the plant supervisory computer. Since the disturbance analysis system provides the possibility of intercommunication with the operator, it was possible also to include process data in the analysis which are not available on the plant supervisory computer, but which are known to the operators, either in the control room or by instrumentation located somewhere in the plant. But, as a matter of fact, the cause-consequence diagrams must not comprise too many questions to the operator, since they may on one hand annoy him or on the other stress him too much. The capabilities of the disturbance analysis system may be enhanced considerably in case systems analysis could include the entire process instrumentation. It may even be desirable to include additional sensors to meet special requirements of disturbance analysis. As far as analog values are concerned this would help to define limit values below plant standard alarms thus to improve the sensitivity of the disturbance analysis as opposed to conventional alarm annunciation. Prime causes could be determined easier and in more detail and the surveillance of plant transients could help the operator to maintain a better general view on the plant behaviour, in particular in case of disturbances, and to estimate the best corrective actions.

Plausibility checks could be performed and sensor failures could be detected. It can also be thought of introducing small and simple dynamic models which are then constantly being updated and could be used for transient prediction.

4. User aspects and ergonomic considerations

During the last decade industrial processes have grown more and more complex due to the higher level of automation and the new environmental and safety demands. In such processes disturbances or alarm situations can arise which the control room personnel may find difficult to get a general view of.

The plant operators can at one moment handle one or a relatively small amount of alarms emerging from the conventional alarm monitoring systems; however, in these complex processes it is indeed possible that a large number of alarms can arise at the same time and then it will be difficult to combine and interpret these alarms in order to define the process status.

The more difficult or complex the situation is, the more information is flowing to the operator /7 /.

Today, there is a "human-filter" built into this system, the operator considers the alarm pattern, connects the different events, then he reduces the amount of data presented to him by an "alarm-pattern-recognition" technique, and then he performs the proper actions.

When introducing a STAR system to a control room, one must be very careful. Normally it should be regarded as a part of the process instrumentation and as such it will be an integrated part of the control room. So when the complex situation occurs, one must be sure that the STAR system does not add one more problem to the operator when he is considering the situation.

For the time being it seems to be a lack of a consistent and comprehensive alarming philosophy. It seems therefore now to be the correct time to introduce and utilize the advantage which the modern computer technology offers in order to reduce the unnecessary information to the operators. The alarm situation or disturbance could be digested by a computer program instead of the control room personnel. The methods and the tools are available. The STAR system is a starting point in this respect, it contains many of the aspects for a consistent alarm handling and digestion procedure before alerting the operator.

When a STAR system is implemented in a plant, one must look at the usage purely from the operational staff's point of view. This includes the specific on-line use of the system and the administrative rules to secure a proper running of the system.

It is difficult to see any reason for educating the operating staff in computer technology as the STAR system should in regular operation be thought of as a process instrument. This means that the personnel which is well educated on the process side should not be bothered with, or even know at all, that there is a computer in between the process and them.

The logical process description (the cause-consequence diagrams) is based upon a thorough analysis of the actual process. This is regarded to be the most complicated and critical task in the entire system. Normally real process systems or subsystems are delivered from the suppliers together with manuals and operational procedures. The logical process description should therefore also be compressed into a short verbal description in plain language for each separate process system. It should contain a basic explanation of the logical interaction between the events and act as an information source for the operator. The logical description behind each chain is in fact the dynamic behaviour of the process itself, so knowledge of the logical description is therefore knowledge of the process.

From a theoretical point of view it is no doubt that the chains are correctly constructed, but the question is whether the chains match the practical life in the specific process. Therefore it seems reasonable that the users should gain sufficient knowledge about the logical process description so that they can participate in discussions for refinements or modifications of the chains.

One other aspect of education is the one directly connected to the on-line use of the STAR system, or the use of the communication system. It is extremely important that the users have the opportunity to get familiar with the system before it is put into regular use. When the system is operational, it would be regarded as an advantage if the system could be operated in two modes:

- on-line mode
- simulation mode.

Simulation mode could be performed - for instance - during shutdown periods. STAR should therefore be able to operate - not only on real process data, but also on data sets given by a simulator or instructor. This gives an opportunity to train the operator both in the STAR system and in the process behaviour of the specific process system.

It is important to point out that the STAR system does not solve all problems in the man-process interaction, it must be regarded as an aid - not a law - because the computer can never be responsible for the safe operation of a process.

5. The principle of operator diagnosis by the STAR system

The operator communicates with the on-line STAR system through the two colour display screens, the function keyboard, the alphanumeric keyboard, and finally the tracker ball/1, 9/. On one of the screens is normally the alarm and summary picture presented and on the other screen is a detailed presentation of the disturbance analysis from any subsystem. He can also request different "question pictures" containing questions from the analysis system to the operator.

Alarm and summary display

This mode of operation displays the alarms detected by the disturbance analysis system. These events are earlier given the property alarm by the systems analyst when he analysed the process. This means that only those alarms which the systems analyst prefers to be displayed in a given situation is shown. (In other words, not every limit violation is shown).

These alarms are presented on the screen as text strings comprising information about:

- name of subsystem reporting this alarm-
- alarm text message.

Since the number of alarms can be greater than what can be contained in one picture, the information can be chained into more pages. In the upper

right corner of the picture, the current number and the total number of pages are listed. When the operator finds that there exist alarms from one of the subsystems, he can request the DAS picture for that subsystem.

The disturbance analysis subsystem status picture

In this picture the operator finds the detailed information about the disturbance status of a plant subsystem:

- the prime cause of the disturbance
- the possible consequence of the disturbance
- the present status
- the possible final event
- a suggestion for counteraction
- the questions given by the analysis system for the operator to answer.

This information is presented on the screen as text strings, messages, which the process analysts have connected to the different events at the time when he analyses the process.

The question picture

There are three different pictures belonging to the question table handling. The first one presents all the possible questions in the system with their current status. The second one presents all the questions currently asked by the analysis system, and the third one presents all the questions answered by the operator.

The dialog used in this picture has two entries:

- QUESTION NO.:
- ANSWER:

If the operator wants to answer a question coming from the analysis, he can use the QUESTION NO and ANSWER fields to type the question number and YES, NO or I DO NOT KNOW.

The operator message field

The left part of the dialogue area shown in fig.3 is called the operator message field. This area is used by the system to alert the operator with messages or to answer some of the inquiries from the operator. As an example will the message:

There exist new analysis
results for the system
currently displayed on the
screen

be shown when the ALKOM system has received new data from the ALSAN system concerning the subsystem which the operator reads at the moment. The reason for introducing this sort of message is that one does not want the annoying redisplay of a picture when new data arrives just while reading the latest messages. Other messages which can appear, come from the question table handler and the alphanumeric keyboard handler.

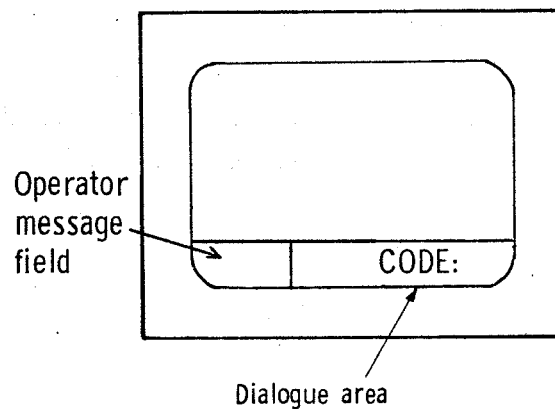


Fig. 3

The function keyboard is used to start a task. The buttons are collected in groups, each group representing a set of plant subsystems which belong naturally together. Every push button is named according to what plant

subsystem or user function it represents. An important detail is that when a button is pushed, a built-in lamp lights to indicate the execution of the request. From each function it is possible to branch out to details by tracker ball addressing. The details may either be a new picture or new information in the one currently displayed.

The standard alphanumeric keyboard is used for writing directly in the displayed picture, as a part of the communication conveyed through a dialogue area with predefined dialogue text.

The dialogue text has a "dialogue"-colour while the operator's input appears in an "operator"-colour. When accepted by the input check software, the "operator"-colour is replaced by an "accepted"-colour. A feature of the dialogue is that the keyboard has a tabulator function that automatically moves the input cursor to the first position of the following input field when the tabulator-button is pushed. The dialogue also includes error messages, presented, when the input check software detects an operator input error, for example a non-existing subsystem name, alarm number, etc.

6. Conclusions

Disturbance analysis systems have been an area of research and development with major efforts in the last five years. The results obtained so far indicate, that the benefit from such a system may significantly increase plant availability and plant safety. The STAR Grafenrheinfeld application is the first one in a plant of the 1300 MWe class.

Parallel efforts on DASs in the U.S. /10/ and in Hungary /11/ as well as other places show, that there is a need for improving the quality of information being given to operators in nuclear power plants.

Even though the developments have an advanced status there are many problems yet to be solved. Validation of the cause-consequence models or reducing the costs for construction of cause-consequence models will be a major field of interest in the next few years. The development in hardware as well as software technology will make improved tools for disturbance analysis available.

The application of colour CRT's in control rooms of nuclear power stations changes the outlook of control rooms as well as the rôle of the operator. The old annunciation systems are found to be inadequate for optimal operator performance. Automatic tools are becoming flexible enough to be adapted to human needs rather than the other way round. Man-machine-communication must start with teaching the machine the human language.

References

- /1/ Felkel, L., Grumbach, R., Zapp, A., Trengereid, J.K., Øwre, F.
Analytical Methods and Performance Evaluation of the STAR application in the Grafenrheinfeld nuclear power plant
paper to be presented at the IAEA Specialists' meeting on NPPCI, Dec. 5-7, Munich, Germany
- /2/ Büttner, W.E.
Ein Konzept zur Störfallanalyse
MRR 141, Techn. Universität, LRA, 1974
- /3/ Büttner, W.E., Felkel, L., Grumbach, R., Herdtle, H.G., Øwre, F.
Data base preparation and operational features of the disturbance analysis system for the Grafenrheinfeld nuclear power plant
EHPG, Loen, Norway, June 5-9, 1978
- /4/ Felkel, L., Grumbach, R.
Rechnergestützter Aufbau von Störungsablaufmodellen
In: Fachberichte MSR, Vol. 1, Springer, Heidelberg, 1977
- /5/ Felkel, L., Grumbach, R., Hoermann, H.
Automatic generation and application of disturbance analysis models
HPR 214, Halden, 1977
- /6/ Basic PEARL Language description
KFK-PDV 120, Karlsruhe, 1977
- /7/ Pack, R.W.
Human Factors in nuclear power plants
EPRI-Report NP-309, Palo Alto, 1978

- /8/ Williams, R.L., Gately, W.V.
GO-Methodology-Overview
EPRI-Report NP-765, Palo Alto, 1978
- /9/ Øwre, F., Felkel, L.
Functional description of the disturbance analysis system for the
Grafenrheinfeld nuclear power plant
EHPG, Lone, June 5-9, 1978
- /10/ Frogner, B., Long., A., Meijer, C.H.
On-line Power plant alarm and analysis system
EPRI-Report NP-613, Palo Alto, 1978
- /11/ Bürger, L., Zobor. E.
On-line alarm analysis of WWR-SM research reactor
Procs. IAEA Symp. on NPPCI, Cannes, 1978

L. Felkel, R. Grumbach, A. Zapp, F. Øwre, J.K. Trengereid
ANALYTICAL METHODS AND PERFORMANCE EVALUATION OF THE STAR
APPLICATION IN THE GRAFENRHEINFELD NUCLEAR POWER PLANT

ANALYTICAL METHODS AND PERFORMANCE EVALUATION
OF THE STAR APPLICATION IN THE
GRAFENRHEINFELD NUCLEAR POWER PLANT

L. Felkel, R. Grumbach†, A. Zapp
Gesellschaft für Reaktorsicherheit (GRS) mbH
Garching, Germany F.R.
F. Owre, J.-K. Trengereid
Institutt for Atomenergi,
Halden, Norway

Abstract

The STAR disturbance analysis system is now installed in the Grafenrheinfeld nuclear power plant and is connected, on-line, to the plant supervisory computer. This paper describes the actual system set-up. The system is now being subjected to a long term performance evaluation. Automatic tools have been designed to partly support performance evaluation; these will be shown in this paper. Another topic is the on-line analysis method used in the STAR DAS. It is also shown how the user may program the system to meet his specific ergonomic requirements.

†The authors are deeply moved by the sudden and unexpected death of their friend and colleague Dr. Rainer Grumbach.

1. Introduction

The development of the STAR disturbance analysis system started as early as 1974. As a basic functional module the ALSAN program has been designed. The concept of this program was to use plant models which were produced by the extended fault-tree methodology, the models being cause-consequence diagrams /1/. In principle, the idea behind the system resembled very much the one underlying the pioneering work of an alarm analysis system at Wylfa and Oldbury power stations in the United Kingdom /2, 3/. The UK approach, however, had certain drawbacks and has therefore fallen below expectations. Computers had been applied, which were costly at that time and as a consequence storage capacity was small. The models used were inflexible and their reliability was overrated.

The design of the ALSAN prototype system tried to avoid these shortcomings /4/. The idea of a model generator system to ease construction, modification and extension of the models existed by then but it could not be pursued due to lack of financial support. There was no idea of how to present the analysis results to plant operators, let alone human factors considerations. There was no possibility for application; an attempt has been made to couple an analog computer to the analysis program but the project has been abandoned due to an excessively low cost-benefit ratio.

In 1975 then, cooperation was started with Instituttt for Atomenergi (IFA) which resulted in an application of a disturbance analysis system in the Halden Boiling Water Reactor /5/. In this application the analysis system was coupled to the operator communication system (OPCOM), developed by IFA /11/. It was thus possible to display the analysis results using colour cathode ray tubes (CRT). Tests and demonstrations during this application indicated that there was a significant gain in the quality of information given to the operator which may have a strong impact on plant safety and plant availability.

By the end of 1976 it was decided that the cooperation between GRS and IFA should continue, aiming at a pilot installation in a German nuclear power plant of the 1300 MWe type. Fortunately, Kraftwerk Union and the Bayernwerk Utility could be interested in disturbance analysis due to the successful experiments performed at the Halden Reactor. The pilot disturbance analysis system (the STAR system) is now installed in the Grafen-

rheinfeld Nuclear Power Plant /10/. This is a 1300 MWe KWU-PWR. It is the first time that an advanced disturbance analysis system is applied to a large nuclear power plant and it need not be emphasized that the application is of high significance with respect to the assessment of reliable figures about the usefulness and necessity of a disturbance analysis system.

2. The Grafenrheinfeld STAR hardware and software set-up

For plant data acquisition, disturbance analysis and operator communication three computers are allocated for the respective tasks. (See fig. 1.1)

In a sampling time interval of about five seconds, the entire plant data base, in the following called the complete process image of the plant, is transferred via a fast data channel from the plant supervisory computer to the analysis computer. The transmission speed is approximately 100 k Bytes/s.

In the analysis computer the data selection and the disturbance analysis are performed. The selected plant data, in the following called reduced process image, will be saved on a magnetic tape.

On the analysis computer, all analysis results are transferred via a standard serial TTY link to the communication and display module where the results are presented to the operator on two colour CRT's in the form of alphanumerical text strings.

The disturbance analysis computer hardware is shown in fig. 1.2. The disturbance analysis computer is a medium sized process computer with 16 bit wordlength and 64 K words of magnetic core memory. It is equipped with a 10 MByte disk for storage of the off-line generated plant models, with a magnetic tape station, a line printer for producing hard-copies of a variety of interesting data, a card reader, and a teletype.

The communication and display module consists of two colour display monitors with appropriate semigraphic display controllers, a function keyboard,

Fig. 1.1:

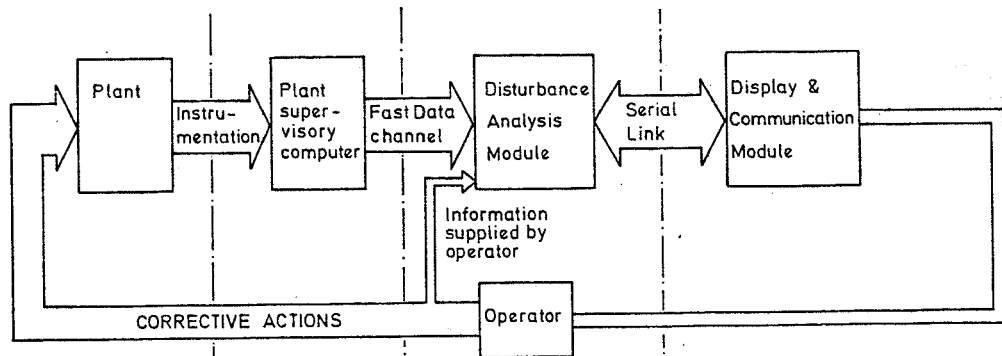


Fig. 1.2:

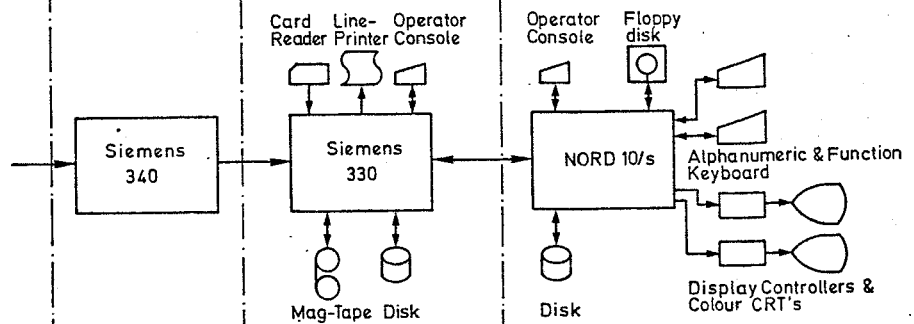
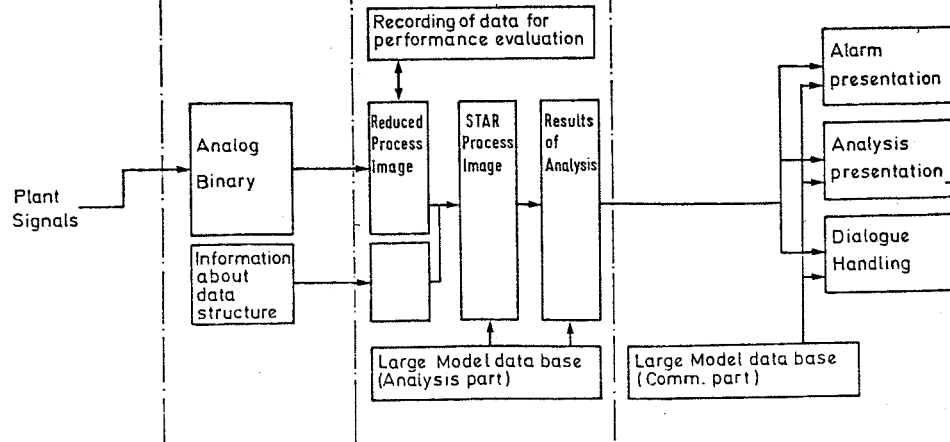


Fig. 1.3:



Functions, Hardware & Required data of the STAR-System

an alphanumeric keyboard, and a tracker ball. The module is controlled by another medium sized process computer with 16 bit wordlength and 64 K words of MOS-memory, provided with error checking and correction. A floppy disk unit for data exchange and a 10 MByte disk for program loading and for storage of the off-line generated alarm and analysis text strings are interfaced to this computer.

The plant supervisory computer is a large size process computer with 265 K words of core storage. The supervisory computer is part of a dual computer configuration to meet high reliability requirements. The plant supervisory computer system is a standard equipment of KWU-PWR plants.

3. The Model Generator

The models used for disturbance analysis are cause-consequence diagrams. These cause-consequence diagrams are a representation of the plant behaviour during disturbances. Cause-consequence diagrams can be considered to be a real-time on-line simulator, where the on-line data are to update the simulator (corrector-step) and running the simulator (performing the disturbance analysis) is the predictor-step. To achieve faster than-real-time simulation the models have to be simple, but they must also be detailed to such an extent, that the process is sufficiently represented and the results of the analysis are useful. Cause-consequence diagrams meet these requirements and have hence been adopted for disturbance analysis.

The cause-consequence diagrams are, however, also the most difficult and costly part in the disturbance analysis system. This is mainly for two reasons

- CCD's cannot readily be used as computer data base,
- the construction of a CCD requires the thorough knowledge of the process.

The problem is that systems analysts, who have detailed knowledge of the process are, in most cases, no computer specialists. They are therefore unable to structure the data (knowledge about process behaviour) in such a way that it can be efficiently used by a computer.

Some approaches /13/, however, have prepared special formatted sheets, where systems analysts can fill in the information about events and their behaviour. For larger applications and in view of applications in different plants, there may be additional information available or required. These "fill-in-the-blank" tables are very inflexible, above all in view of extensions, and in general every translation from one "language" (also these tables can be considered a language, however simple the syntax and the

semantics may be) to another is a tedious, time-consuming and error-prone task.

The approach to this problem in the STAR system aims at isolating plant systems analysis from computers. Systems analysts should be given the possibility of expressing their ideas in terms of mechanical and electrical engineering. A language has therefore been designed to meet the requirements of systems analysts as well as the computers.

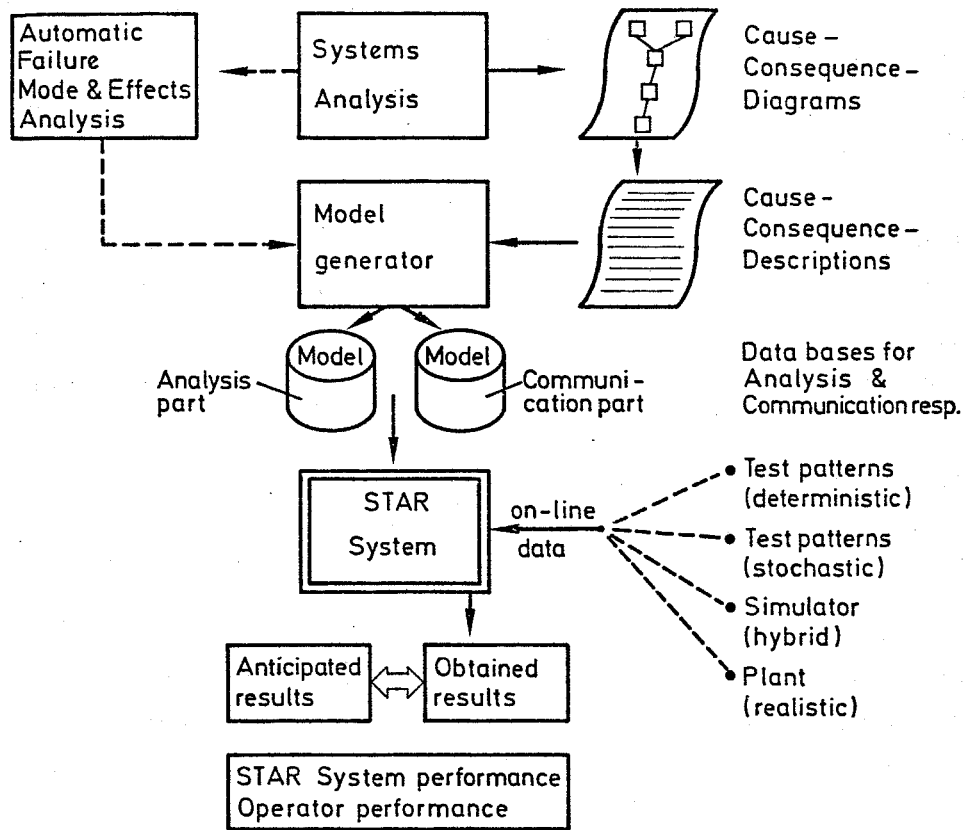


Fig. 2: STAR-Data Base Generation & Performance Evaluation



Fig. 2 shows all the tasks, which have to be performed before disturbance analysis can be done. Cause-consequence diagrams will be constructed first. These have to be translated (by hand, this can, however, be done by a data typist) into the cause-consequence description, the syntax of which is given by a formal grammar. The description is input to the model generator MOGEN and translated into the data bases required by the STAR system. Besides several cross and plausibility

checks, after translation the description could automatically be plotted again into a cause-consequence diagram, thus allowing the systems analysts to see whether the description and his diagram are identical. This is not implemented yet but would be an additional contribution to validation of the plant models.

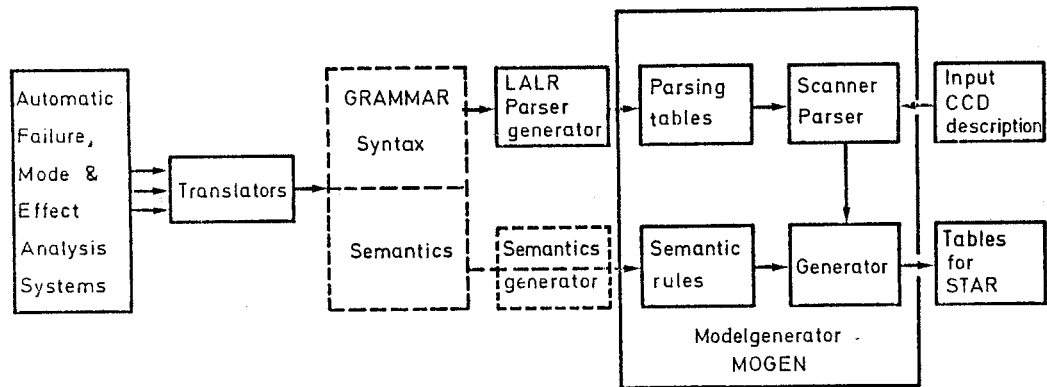


Fig. 3: ^{587M} ADAPTING THE MOGEN PRINCIPLE TO AUTOMATIC TOOLS FOR CCD-CONSTRUCTION

Fig. 3 outlines the functional modules of the MOGEN. The grammar (syntax as well as semantics) have to be prepared by hand according to the special requirements of systems analysis and with the objective, that the syntax is oriented so as to meet the analysts terminology.

Due to experience it may be necessary to enhance or modify the descriptive capability of the language required. This results in modifying the grammar. However, all modules in the model generator, affected by the modification, will have to be adapted accordingly. Therefore the grammar used in the STAR is restricted to a certain type (LALR /14/), so that the appropriate modules can be generated automatically (parser generator). Unfortunately semantics have not yet been formalized sufficiently so as to allow generation of semantic tables. The cause-consequence description is input to the scanner-parser module and syntax of the description is checked.

According to the semantic rules the tables for the STAR disturbance analysis system are generated. The cause-consequence diagram (description) is passed over several times to produce tables which are optimal with respect to savings in execution time of analysis and storage requirements.

As a rough functional description, the model generator is computing everything which is not dynamically dependent on process data. This means that the disturbance analysis algorithm is reduced to fast and efficient table look-up, at least as far as the non-dynamic part is concerned. The speed of one disturbance analysis cycle is there will within the frame which is technically possible today and which has been achieved elsewhere /15/.

The second problem pointed out at the beginning of this chapter is the amount of human work required for systems analysis, which is to blame for high costs constructing the cause-consequence diagrams. However, methodologies /16/ are being developed which yield a reduction in the quantity of manual work needed for cause and effects analysis.

The systems which could be also of use for data base preparation of disturbance analysis systems, have been mainly developed to automatize system reliability evaluation and have now been upgraded so as to perform fault sequence identification. The idea behind these systems is to provide general information about a process to be examined and to define a variety of undesired events. The system will then evaluate the probability of occurrence or the undesired event and give a sequence of precursors which is very similar to a cause-consequence diagram.

Since the output from these systems have a very strict syntax, it can be easily processed or translated into other syntactical forms. Fig. 3, for instance, shows how systems for failure mode and effects analysis (FMEA) could be connected to the STAR data base preparation system.

A major field of research in the next few years will be the definition of formal semantics for process descriptions. One step in this direction has implicitly been done in the development of FMEA systems, because in a way these contain the "meaning" of a process description in a somewhat formalized form.

4. Analysis method

The disturbance analysis is based upon cause-consequence diagrams /1/. These cause-consequence diagrams have been translated by the model generator into very specific tables which provide information about cause-

consequence diagrams and control the functions of the analysis system /6, 8/. The STAR system consists of 4 main program modules (fig. 4):

- the data acquisition module
- the data preprocessor
- the disturbance analyzer
- the operator communication system.

The data acquisition module gets the data from the plant supervisory computer which also comprise the plant's standard time. Each plant signal also carries an indication to denote its validity. If one of the signals which are used by the STAR system is not valid, a warning message is issued and in case the invalid signal is vital to disturbance analysis, analysis is discarded for the subsystem concerned. The data acquisition module also copies those plant data which the STAR system needs, into an area dedicated to disturbance analysis. This is necessary to disentangle the data transmission from the plant supervisory computer from disturbance analysis; for licensing reasons the STAR system is not permitted to send anything to the plant supervisory computer. It must not even be synchronized with the plant supervisory computer and has to receive everything passively.

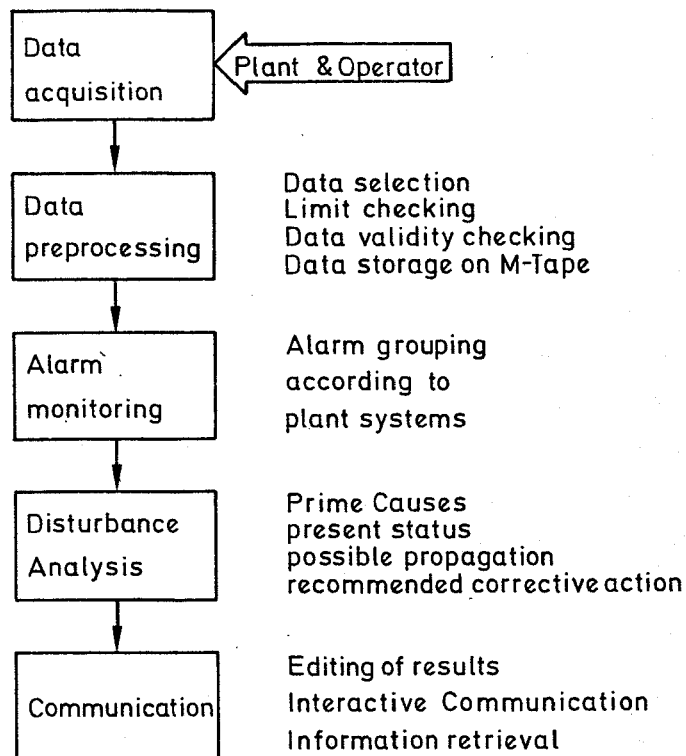


Fig. 4:

Functions of STAR during one update cycle

After the plant data have been acquired, these snap-shot data are available for the STAR system. Data preprocessing is now performed. The binary process data are copied to the appropriate locations in the "STAR process image". According to the limit lists which are provided in the cause-consequence description, the analog values are checked whether or not they exceed the bounds given. The result of this check will again be a binary value to be put to the STAR process image. In the cause-consequence description there are certain events whose occurrence can neither be verified by a binary or analog process signal, owing to the unavailability of such a signal. Often, however, there are possibilities to verify the occurrence of such events by a logical combination of "observable" events. These derived events are also produced during the preprocessing phase, whose binary result again contributes to the STAR process image.

After having established the STAR process image alarms are checked for occurrence. Some events in the cause-consequence description are designated by the systems analyst as alarms. The activated alarms will be collected together systemwise, so that it can be seen at a glance in which systems something has happened.

The next module to be executed is the disturbance analysis program. This program will be called exactly as many times as there are plant systems modeled for disturbance analysis. Each of the plant system models is stored on a fast direct access device and each has exactly the same data structure. Upon calling the disturbance analysis program, the according plant system model is transferred into core. This model contains the exact sequence in which the cause-consequence diagram is to be traversed. For every step in the analysis sequence there is additional information about the type of the node being examined. A node can for example represent an event or a logical unit. They may have certain attributes, which must also be contained in the description, e.g. a prime cause or an AND-gate respectively. Each event being examined is checked for activation by looking into the STAR process image. The analysis sequence is constructed in such a way that, whenever a logical unit is accessed, all necessary inputs have been processed beforehand. The amount of processing done at model generation time now results in a very simple, straightforward and fast analysis algorithm.

The analysis sequence is also constructed in such a way that it facilitates the structuring of information on the display screen. Activated disturbance chains are detected and, unless a one-node look-ahead yields another activated event, look-ahead is extended by means of which the possible propagations are evaluated.

Due to the complex structure of the cause-consequence diagrams, parts of the diagrams may be traversed more than once, viewing the events from a different angle. This may in some cases lead to multiple messages which add in some situations unnecessary redundancy to the information about the disturbance. A special routine filters out redundant information, depending on whether the operator wants compressed or detailed analysis. The complete analysis results are, however, available in an intermediate data base.

The communication system receives the analysis results in the form of telegrams. A special telegram handling routine organizes the receiving and transmitting of telegrams between the ALSAN and the ALKOM modules.

After alarm monitoring and disturbance analysis is performed, the communication system updates the analysis status pictures. If analysis has reached points from where it is impossible to proceed unless the operator supplies additional information, questions are issued to the communication system so that the operator can answer them using the alphanumeric keyboard. After a question has been answered by the operator the answer is transmitted back to the analysis system and will be used in the subsequent analysis.

A picture editing program transfers the telegrams into picture tables which are used as the basis for the picture displayed on the colour screen. If the amount of information in a telegram exceeds one picture table, the program brings the information into more pages, and the operator can retrieve the information by "turning pages".

Eventually, a picture presentation program operates on the picture table and establishes references to the actual strings to be displayed on the screen. The strings are located on a disk file, having been produced by the model generator.

The operator's dialog program services the operator's use of the function keyboard, the alphanumeric keyboard and the tracker ball.

5. Performance evaluation

To be able to evaluate the performance of the disturbance analysis system it is necessary to record all on-line plant data which concern the STAR system. A magnetic tape system has been provided for and will be utilized to record an appropriate selection of the process data which are transferred from the supervisory computer to the STAR system every five seconds. This selection comprises all those data, both analog and binary which are vital for disturbance analysis. Additionally, there will be some process data which are not used by the STAR system but which may be necessary for assessing the actual process status of some important subsystems, for which no cause-consequence diagrams have been created yet.

This kind of data recording renders the possibility to reproduce disturbance propagations in those systems which the STAR analyses, unambiguously and arbitrarily often.

The data recorded at each analysis cycle will also comprise the time at which the snap-shot was taken. Small searching programs are provided for to find interesting data on the magnetic tape. It must be anticipated that a large portion of data on the magnetic tape is of no interest at all, and it would be very tedious to extract interesting data by hand. If an operator, for example, gives an approximate time of a disturbance, the important data may be found automatically.

The magnetic tape yields advantages in several respects. It is possible to replay the disturbances in real-time, faster than real-time, and slower than real-time. In this way, it is possible to gain a "feeling" for the response time of the STAR system.

The performance evaluation will be done under different aspects:

- STAR computational performance
- assessment of the quality of the models
- operator training and performance.

To test the computational capacity the following questions will be investigated:

- has the disturbance been recognised properly
- have the prime causes been detected correctly, has the possible propagation of the disturbance been sensibly estimated, and has the system produced appropriate proposals for corrective actions.
- how does the STAR system react when a disturbance fades away again
- what output is produced by the STAR system when there are different disturbances in the same system
- to what extent can the STAR system operate on insufficient input data.

To assess the quality of the models used in the STAR system, the following questions will be treated:

- which of the models represent the process with sufficient precision
- what degree of sophistication is necessary in the models, should there be more details or less details, is this dependent on parts of the sub-systems
- would it be helpful to have rough and detailed models available at the same time, or should it rather be dependent on superficial or detailed analysis algorithms respectively
- are there sufficient process data the STAR system is supplied with or should an extension of instrumentation be taken into account
- evaluation of the frequency of disturbances with respect to the plant mode of operation, the chronological behaviour, and which systems are very sensitive to disturbances
- how can models be extended such that they are applicable also in extraordinary plant modes of operation, like the commissioning phase, re-tests, startup, and shutdown.

Eventually, the STAR system is to be utilized by operators who need special training and whose performance with the STAR system needs be evaluated. Points of interest are here:

- Did the disturbance analysis system inform the operators about a disturbance in time and was the information in a comprehensible form
- did the operators have sufficient time for corrective action
- was the amount of information adequate or has the operator been annoyed

with nuisance information, how did the operators use the disturbance analysis system

- do they have to acknowledge certain information blocks
- in which way should operators be trained using a disturbance analysis system
- does the disturbance analysis system provide a real advantage over conventional annunciation system
- after shutdown, the disturbance analysis system may also be used for post mortem analysis and it can be anticipated that the operators will be relieved from tedious tasks.

6. Conclusions

As was pointed out at the beginning, the STAR disturbance analysis system set-up in the Grafenrheinfeld Nuclear Power Plant is of high significance evaluating the benefits which are expected by such a system. Using colour CRT's in German nuclear power plants is a novelty, and the STAR system can be considered only the "top of the iceberg" in the development of computer based control and supervision techniques and in advanced control room design.

The present STAR system gives only alphanumeric information to the operator, but experiments are being carried out as to whether there are other forms of information media like mimic diagrams or cause-consequence diagrams displayed on the colour screens. It is also envisaged to use fully graphic systems instead of semigraphic so that trend curves and additional graphic information can be displayed which require high resolution.

By comparison with the activities at other places it appears that the STAR system includes all essential features presently suggested for disturbance analysis systems. However, some aspects deserve increased attention/7, 9/. In particular, this relates to questions of the reliability and verification of the functional software, a validation of the information contained in the data base (cause-consequence diagrams) and the allocation of priorities in case of the simultaneous occurrence of several and uncorrelated disturbances.

As far as future research and development efforts on computer based disturbance analysis and surveillance systems are concerned, the STAR system will be integrated as one functional module into an advanced control room concept.

References

- /1/ Nordic Working Group
Cause-Consequence-Diagrams - A graphical method for description and analysis of failure sequences in complex process systems
Draft, December 1972
- /2/ Jervis, M.W.
On-line Computers in Power Stations
Procs. IEE, IEE Reviews, Vol. 119, No 8R, 1972
- /3/ Patterson, D.
Application of a Computerized Alarm-analysis System to a Nuclear Power Station
Procs. IEE, Vol. 115, No 12, 1968
- /4/ Felkel, L., Grumbach, R.
ALSAN - Ein Programmsystem zur Alarm- und Störungsanalyse mit dem Prozeßrechner
KFK-PDV 93, Karlsruhe, 1977
- /5/ Grumbach, R., Hoermann, H.
Plant disturbance analysis by process computer - Basic development and experimental tests
MRR 160, Technische Universität München, 1976, pp 103-113
- /6/ Felkel, L., Grumbach, R., Hoermann, H.
Automatic generation and application of disturbance analysis models
HPR 214, Halden, 1978
- /7/ Felkel, L., Grumbach, R., Saedtler, E., Wach, D.
Treatment, analysis and presentation of information on component faults and plant disturbances
Procs. IAEA Symp. on NPPCI, Cannes, 1978, Vol. II, pp 13-21

- /8/ Felkel, L., Grumbach, R.
Rechnergestützter Aufbau von Störungsablaufmodellen
In: Fachberichte MSR, Vol. 1, Springer, Heidelberg, 1977
- /9/ Grumbach, R.
Factors enhancing the potentials of on-line plant surveillance systems
EHPG, Loen, Norway, 5-9 June, 1978
- /10/ Øwre, F., Felkel, L.
description of the disturbance analysis system for the
Grafenrheinfeld nuclear power plant
EHPG, Loen, Norway, 5-9 June, 1978
- /11/ Netland, K., Hol, J.Ø., Øhra, G.
Operator Communication in a Computer Based Control Environment
In: HPR 214, Halden, 1978
- /12/ Büttner, W.E., Felkel, L., Grumbach, R., Thomassen, B., Øwre, F.
Functions and design characteristics of the STAR disturbance analysis system,
Paper to be presented at the IAEA meeting on NPPCI, dec. 5-7, Munich
- /13/ Frogner, B.
Methodology and conceptual design of a disturbance analysis system,
Working paper, EPRI Project RP-891, Oct. 1977
- /14/ Lalonde, W.R.
An efficient LALR parser generator
Tech. Rep. CSRG-2, University of Toronto, 1971
- /15/ Long, A.B.
Technical assessment of disturbance analysis systems
to be published in Nuclear Safety Journal, 1979
- /16/ Williams, R.L., Gately, W.V.
GO-Methodology-Overview
EPRI-Report NP-765, Palo Alto, 1978

F. Baldeweg

ON-LINE ALARM ANALYSIS USING DECISION TABLE TECHNIQUE

On-line alarm analysis using decision table technique

Frank Baldeweg

Zentralinstitut für Kernforschung Rossendorf

DDR - 8051 Dresden, P.O.B. 19

Abstract

A procedure for the analysis of event trees will be described, which has been used to develop a programme system for the on-line alarm analysis in a nuclear power plant. The event tree represented by an event graph, $G_E = [E, K]$, with $E \hat{=} \text{set of events } \{e_i\}, i=1..p$ and $K \hat{=} \text{set of relations}$, can be considered as the model of the so called basic system to be surveyed.

The procedure bases on the assumption of the state of the basic system to be a tuple $\vec{z} = (z_1, z_2, \dots, z_k) \in \Pi Z^k$, where $Z \hat{=} \{z_i\}, i=1, \dots, n$, the set of individual states $z_i = (e_i, t) \in Z \subseteq E \times T$, which are nodes of the event graph, $T \hat{=} \text{set of time values}$. It takes into account, that individual measuring points are defect or deficiency of individual events can happen.

The programme system, which bases on the method under consideration, is being realized on a process computer system - consisting of mini- and microcomputer - and hitherto tested for the simulated break down system of the nuclear power plant.

1. Introduction

In the contribution presented a programme system will be described, which has been developed using the decision table technique [1], and which is being developed for diagnosis of disturbed system states in a nuclear power plant, the so called basic system (BS).

It comprises the following tasks:

- monitoring of alarms
- check of the measuring points
- finding out of the causes (break down tree)
- prediction of consequences

Diagnosis in this connection means:

Def: Diagnosis can understand to be as the set of informational processes, which allows the estimation of the elapse of consecutive disturbances in the BS and by the help of them the set of primary causes and possible consequences of the disturbed system states (for instance alarms or break down states) can be found out.

Diagnosis will be carried out by the so called informational system (IS) which is coupled to the BS by set of sensors and effectors (fig. 1).

The programme system has been implemented on a process computer system, consisting of mini- and microcomputers (see also [2], [3], [4]).

For implementation a decision-table precompiler has been used [6].

Definitions of the BS

The disturbed BS should be described by the state vector

$$\vec{z} = (z_i) \in \prod_{i=1}^k Z^k, i=1\dots k.$$

Z is set of possible individual states of the BS, $z_i = (e_i, t) \in Z \subseteq \text{Ext}$. The set E is referend to as the set of events, $e_i \in E = \{e_j\}, j=1\dots p$,

in general there is $p \neq k$; $E \subseteq B \times N$, B is a set of values, for instance $b \in B = \{0, 1\}$, $b_i = 1$ - means "event occurs", $b_i = 0$ - means "no event"; N is set of names; $t \in T$, the set of time values with $\text{card}(t) = \alpha$.

The normal state \vec{z}_0 of the BS can be characterized by

$$\forall z_i \in Z(b_i = 0, n_i \in N, t) \Rightarrow \vec{z} \equiv \vec{z}_0, b_i \in B, \\ i = 1 \dots k.$$

Definition of the IS

BS and IS are coupled by a set M of automatic couplings (s. fig. 1). For M the relation $M = M_s \cup M_e$ is valid, where M_s referred to as set of automatical sensors and M_e as set of automatical effectors.

The coupling of BS and IS can be described by the functions ε and γ

$$\varepsilon: M_s \rightarrow E \quad - \quad \text{produces the set } E_s \text{ of sensor events } e_i^s \\ \gamma: M_e \rightarrow E \quad - \quad \text{produces the set } E_e \text{ of effector events } e_i^e.$$

Furthermore $E_e \cup E_s \subseteq E$ is valid.

In the given case, the automatical therapy control has not been considered, that means $M_e \hat{=} E_e = \emptyset$.

Modelling

To apply a diagnosis system on to at least one class of BS, it is necessary to use an uniform description of the relations between the events.

As a very useful tool of description the alarm tree (AT) can be considered.

Def: The AT is an undirected connected graph, which describes the relations between the events (faults), the so called cause - consequence - relations in a selected set of events.

It can be presented by $G = [V, X_E]$, with V - set of nodes (events), X_E - set of connections. A connection can be characterized by the function $\phi_x: X_E \rightarrow ExE$. To each $x_E \in X_E$ an ordered pair (x, y) is related, where xRy , $R = \prec$; $x, y \in E$.

The disturbances (events) e_i are selected events of the event set E , where $e_i \in E_{Di} \subseteq E$, is valid with E_{Di} , the set of those events, being used for diagnosis. Each node $v_i \in V$ of the AT is related to an event $e_i \in E_{Di} = E_{FA} \cup E_{PA}$.

The subset E_s (sensors) can be defined by $E_s = E_M \cup E_N$ and $E_M \cap E_N = \emptyset$, with E_N - set of non measurable events and E_M - set of measurable events. The subset E_M can again be divided into $E_M = E_E \cup E_{DE}$ with $E_E \cap E_{DE} = \emptyset$, where E_E - set of really measurable events (measuring points: fixed up) and E_{DE} - set of non measurable events (measuring points: defect). From this comes $E_{Di} = E_{FA} \cup E_{PA} \subseteq E_M$.

FA will be induced, when an event e_m (for instance: break down) $\in E_m \subseteq E_M$ occurs.

For the AT the following conditions are to be followed:

- to every definite event e_m (for instance, break down alarm) belongs a subtree
- the structure of the nodes will be made in such a way, that every relation connects only one node of level (j) with only one of level $(j+1)$
- the levels of the graph should be ascending numbered. The start will be with that level, which contains e_m (level number \emptyset)
- the AT might not contain any circles and should be connected.

In that case, the AT can be divided into subtrees G_u .

For all G_u the following facts should be considered (s. fig. 2):

- $v_w \in$ level (j) of the AT, v_w - root node of G_u
- $v_b \in$ level (j+1) of the AT, v_b - leaf node of G_u
- $b_w = f(\forall b_i)$, $f = \{\wedge, \vee\}$, $b \in B = \{0, 1\}$;
 b_w - valuation of the root node events,
 b_i - valuation of the leaf node events.

In the given case, three types of subtrees can be decided.

- type 1: OR-trees without non identifiable events (all leaf events are known and measurable)
- type 2: OR-trees with non identifiable events (i.e. some measuring points are defect, but defects are unknown)
- type 3: AND-trees (all leaf events are known)

Diagnosis

If in the set $E_{Di} \subset E_s$ a set $UR = \{UR^i\} \subseteq E_{Di}$ (set of causes of the events e_i) and a set of consequences $W = \{W^i\} \subseteq E_s$ are defined, if "n" the number of levels of the graph G and "m" that level, which contains e_i , then diagnosis means:

for that event e_i the set of causes ur ; with $UR^i = \{ur_i^j\}$
 $\subset UR \subset E_s$ and the set of possible consequences $W^i = \{w_i^j\}$, $j=1 \dots n-m$
 have to be found out. For every event $e_i \in E_{Di}$, which is situated in the level "m" of G; the following relation is valid:

$$ur_i^{(\nu_1)} \prec ur_i^{(\nu_1+1)} \prec \dots \prec ur_i^{(m-1)} \prec e_i^{(m)} \prec w_i^{(m+1)} \prec \dots \prec w_i^{(\nu_2)}$$

with $ur_i^{(\nu_1)} \in UR^i$ and $w_i^{(\nu_2)} \in W^i$; $1 \leq \nu_1 < n$, $1 < \nu_2 \leq n$, $\nu_1 < \nu_2$.

Diagnosis means in a formal sense, to find out ordered sets of nodes in the event tree.

2. Tasks of the diagnosis system

The programme system, which has been realized by the use of decision table technique, comprises the following tasks in general:

- measuring of analogue and binary data
- data processing
- monitoring
- checking of the measured values concerning deficiency of measuring points
- estimation of causes (break down tree)
- prediction of consequences
- management of the list of defect measuring points
- management of the list of limit values and/or alarm values

Some of them should be discussed in more detail:

Data processing: In this task an event $e_i = (n_i, b_i)$ will be related to a tuple (measuring point name n_{mi} , measuring value m_i), this means: surveillance of process data with respect to tendency values and limits. This task and the following two one need the following informations about the AT:

- for the nodes:
- name of the event e_i : n_i ;
 - actual state of e_i : b_i
 - $b_i = 1$ - event occurred
 - $b_i = 0$ - event not occurred
 - information about the actual state of the measuring point i : d_i
 - $d_i = 1$ - measuring point defect
 - $d_i = 0$ - measuring point not defect
 - information about the node v_i : w_i
 - $w_i = 1$ - w_i leaf node of G_{ui}
 - $w_i = 0$ w_i not leaf not node of G_{ui}

- information about the state of e_i in the past: a_i ;
- $a_i = 1$ - event occurred in the part once at least
- $a_i = 0$ - event did not occur in the part

These informations are presented in special storage regions:

$$\begin{aligned} \text{PEA}[i] &= b_i \\ \text{DEF}[i] &= d_i \\ \text{VOR}[i] &= w_i \\ \text{ALT}[i] &= a_i \end{aligned}$$

Furthermore the following informations are necessary for the structure of the AT:

- number of the root node V_w , number of leaf nodes V_{b_i} and the boolean function f of G_u .

Monitoring: In this task that set I_1 of the events are estimated and put on record, which occurred for the first time:

$$I_1 = \{ n_i/b_i = 1 \wedge a_i = \emptyset \wedge d_i = \emptyset \} \text{ with } a_i \in \{0,1\} \text{ and } d_i \in \{0,1\}.$$

Checking with respect to deficiency of measuring points: Here the valuation of the root nodes V_w are checked.

The set I_2 of those events estimated, whose valuation deviates from that of the calculated leaf valuations.

$$I_2 = \{ n_i/w_i = 1 \wedge a_i \neq f(\forall a_{b_i}(G_{ui})) \}, w_i \in \{0,1\}.$$

I_2 in this case should be understood as connected set of subsets of three event types, $I_2 = I_2^I \cup I_2^{II} \cup I_2^{III}$.

$$I_2' = \{n_i/w_i = 1 \wedge \text{type}(G_{ui}) = 1 \wedge d_i = 0 \wedge a_i \neq y(G_{ui})\}$$

$$I_2'' = \{n_i/w_i = 1 \wedge \text{type}(G_{ui}) = 2 \wedge d_i = 0 \wedge a_i = 0 \wedge y(G_{ui}) = 1\}$$

$$I_2''' = \{n_i/w_i = 1 \wedge \text{type}(G_{ui}) = 3 \wedge d_i = 0 \wedge a_i \neq z(G_{ui})\}$$

with

$$y(G_{ui}) = ((a_{b1} \vee d_{b1}) \wedge (a_{b2} \vee d_{b2}) \dots (a_{bq} \vee d_{bq}))$$

$$z(G_{ui}) = ((a_{b1} \vee d_{b1}) \wedge (\quad) \dots (\quad))$$

$\{v_{b1}, v_{b2} \dots v_{bq}\}$ - set of the leafs of the subtree G_{ui} .

As an example for the use of decision table technique the algorithm of the two tasks - given just before - is represented in the decision tables ET 1, 2, 3.

ET 1 (G_u type 1)

R - number of rule

S - selector = calculated value of the root

i - number of the measuring point = number of the node

A(i) - bit "i" of ALT

D(i) - bit "i" of DEF

O - output

K - number of the root

n - lower number of the leafs

m - upper number of the leafs

l - index

ENDE - jump to the next subtree

R	S	i	A(i)	D(i)	S	A(i)	D(i)	O	i	Goto
1	-	-	-	-	0	-	-	-	n	R2
2	-	-	0	1	1	1	0	-	-	R4
3	-	-	1	0	1	-	-	-	-	R4
4	-	m	-	-	-	-	-	-	i+1	R2
5	-	-	-	-	-	-	-	-	K	R6
6	0	-	1	0	-	-	-	i	-	R8
7	1	-	0	0	-	-	-	i	-	R8
8	-	-	-	-	-	S	0	-	-	ENDE

ET 2: G_u type 2

R	S	i	A(i)	D(i)	S	A(i)	D(i)	O	i	Goto
1	-	-	-	-	0	-	-	-	n	R2
2	-	-	0	1	1	1	0	-	-	R4
3	-	-	1	0	1	-	-	-	-	R4
4	-	m	-	-	-	-	-	-	i+1	R2
5	-	-	-	-	-	-	-	-	K	R6
6	1	-	0	0	-	1	0	i	-	R8
7	1	-	-	-	-	1	0	-	-	R8
8	-	-	-	-	-	-	-	-	-	ENDE

ET 3: G_u type 3

R	S	i	A(i)	D(i)	S	A(i)	D(i)	O	i	Goto
1	-	-	-	-	1	-	-	-	n	R2
2	-	-	0	0	0	-	-	-	-	R4
3	-	-	0	1	-	1	0	-	-	R4
4	-	m	-	-	-	-	-	-	i+1	R2
5	-	-	-	-	-	-	-	-	K	R6
6	0	-	1	0	-	-	-	i	-	R8
7	1	-	0	0	-	-	-	i	-	R8
8	-	-	-	-	-	S	0	-	-	ENDE

Estimation of causes: That set I_3 of events is found out, which belongs to the break down tree.

$I_3 = \{n_i/v_i \in G_{BD}\}$; G_{BD} is defined as a special partial graph of AT. It is characterized by the set of those disturbances (events), which could be the causes of the occurrence of a definite disturbance e_m (for instance; break down alarm). For all the nodes v_i of the G_{BD} , there is $b_i = 1$.

Prediction of the set of consequences: The set I_4 of possible consequences w_i of an event e_i is estimated by extrapolation inside of G : $I_4 = \{n_i/v_i \wedge G \neg G_{BD}\}$

The principle of this task should be explained by an example. The event graph $G = [E, U]$ of a real subsystems is given in the fig. 3.

The decision table of one of the three subgraphs are shown in table 1.

The set of event E_s comprises q element $\{e_i\}$, $i=1, \dots, q$. After checking the condition \bar{b} , the actions appropriated \bar{a} are initiated, i.e. the output of alarms, of causes and possible consequences.

Tab. 1: Decision table of $SG(i)$

tab	DPP(i)	OTP(i)	OPP(i)	i	i	e	output ur	w	GOTO
1					1				
2	1					DPP(i)		unknown	
3	1	1					OTP(i) > 70		
4	1		1				OPP(i) < 5		7
5	0	1				OTP(i) > 70	unknown	DPP(i)	
6	0		1			OPP(i) < 5	unknown	DPP(i)	
7				< 3	i+1				2
8	-	-	-	-					n

3. Process computer realization

The programme system is being realized on a process computer system - at present consisting of a mini- and a microcomputer system (s. fig. 4). The diagnosis scheduled to be developed on a complete microcomputer system on cause of the following reasons:

- diagnosis needs much storage. On the other hand, it operates relatively scarcely. In case of a centralized computer realization this would reflect a loss of costly capacity of storage.
- in the case of extended AT the reaction time of the IS and the decision capability of microcomputer networks become more favourably
- in general the use of microcomputers seems to become more economical and reflects a higher reliability of the IS.

In table 2, given close bey, a part of the logging print and the result of diagnosis in case of a test example is presented.

Fig. 5 shows the pertinent AT.

Table 2: Logging print

```
00.15 PROGR. FEFE
      REACTOR PER. LOW
      POSS. CAUSE:
      COMP.-CASS.-AND/OR AUT. REG. CASS. LIFTING
      OR COLD WATER FALL
      POSS. CONSEQUENCE:
      BREAK DOWN 1. ORDER

00.16 PROGR. FEFE
      VAC. IN TURBINE COND.
      POSS. CAUSE:
      UNKNOWN
      POSS. CONSEQUENCE:
      TURBINE DEF.
      BREAK DOWN 2. ORDER
```


4. Final remarks

The present state of the diagnosis system is characterized by tests and by set into operation of the algorithm under consideration.

The check of the system is first of all restricted on the breakdown system of the NPP.

An extension with the following aspects is planned:

- joining of further groups of measuring points, among them: use of noise analysis informations (vibrations, loose parts and so on).
- implementation on a microcomputer network
- extension to a computer aided automatic diagnosis-therapy system (s. ref. [5_7]), i.e. realization of a IS with $M_e = E_e \neq \emptyset$ (comp. part. 2.).

5. References

- [1] Baldeweg, F., Junclaussen, H., Stahn, H.
"Grundlagen der Kybernetik II"
ZfK-308, März 1976
- [2] Baldeweg, F., Gaßmann, F. H., Gurke, G.
"Störablaufanalyse und Schadensfrüherkennung für ein
stetig-kontinuierliches Basissystem"
ZfK-362, Oktober 1978
- [3] Bürger, L., Zebor, E.
"On-line Alarm Analysis of WWR-SM Research Reactor"
loc. cit. [4], IAEA-SM-226/17
- [4] Felkel, L., Grumbach, R., Saedtler, E., Wach, D.
"Treatment, Analysis and Presentation of Information
about Component Faults and Plant Disturbances"
IAEA-SM-226/40, International Symp. on Nuclear Power
Plant Control and Instrumentation, 24. - 28. April, 1978
Cannes
- [5] Baldeweg, F., Gaßmann, F. H.
"Formale Beschreibung von Diagnose und Therapiesteuerung
für ein diskontinuierlich-diskretes Basissystem"
to be published
- [6] Büsch, H.-J.
"Entscheidungstabellentechnik - methodische Beschreibung,
Anwendung und maschinelle Verarbeitung", Dissertation,
TU Dresden, 1978

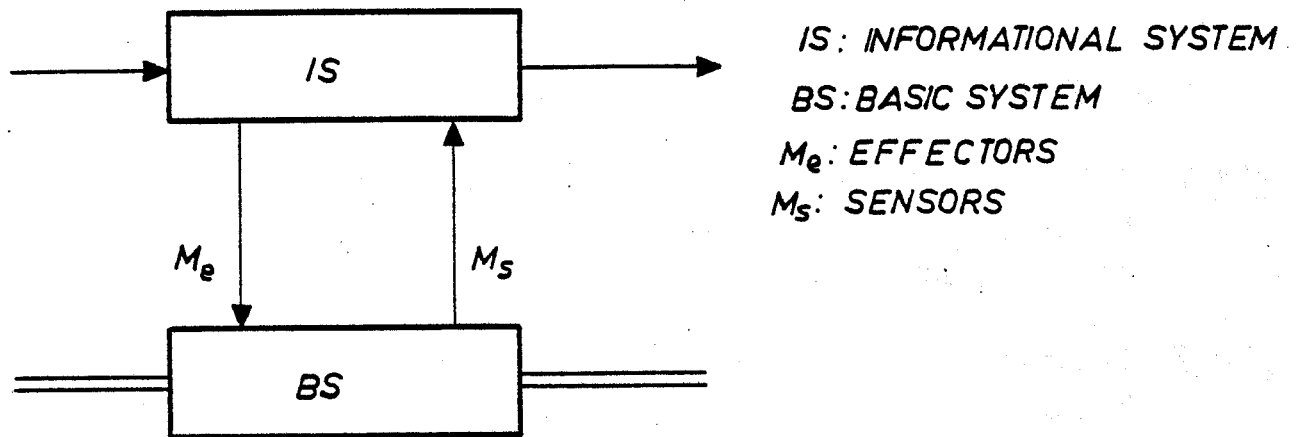


Fig. 1 Automatical System

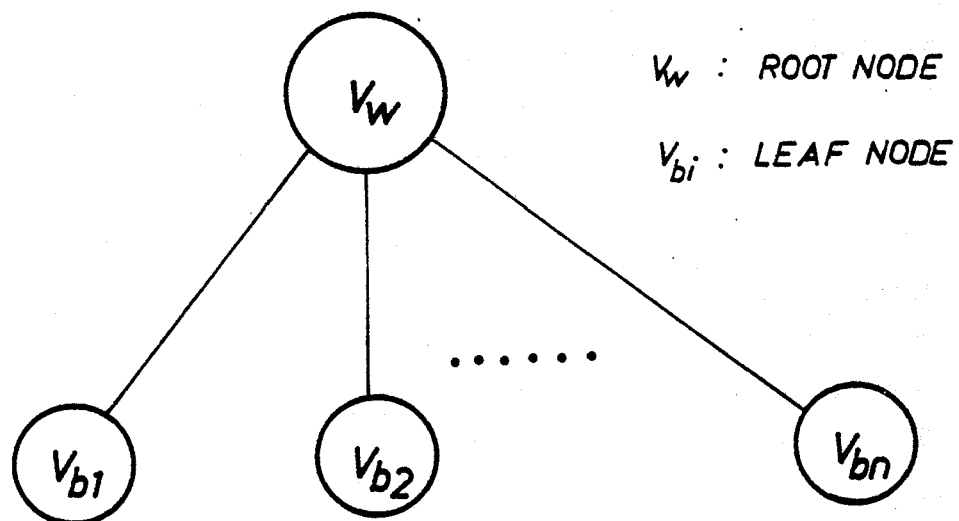


Fig. 2 Representation of a subtree

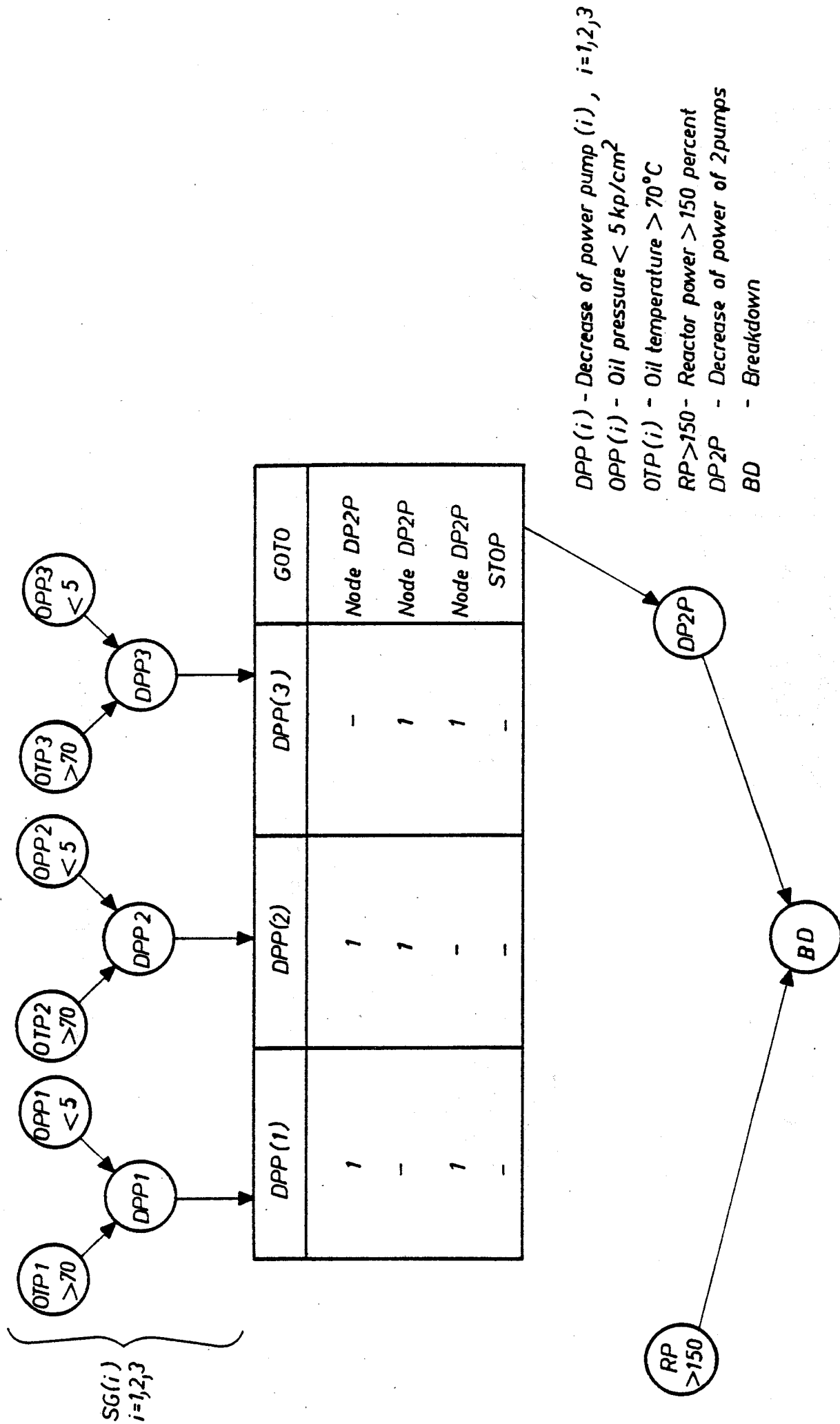


Fig. 3: Eventtree of a subsystem

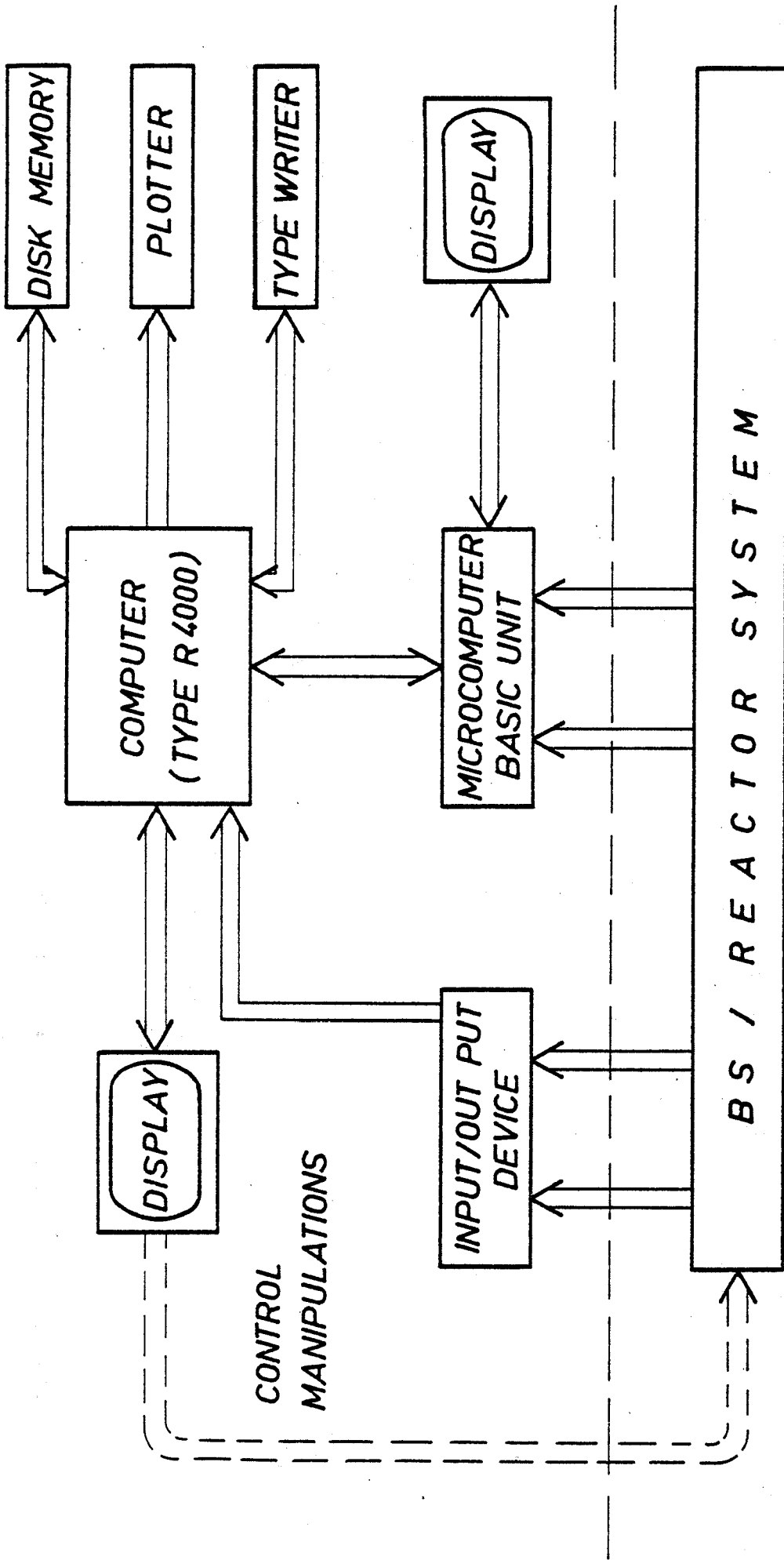
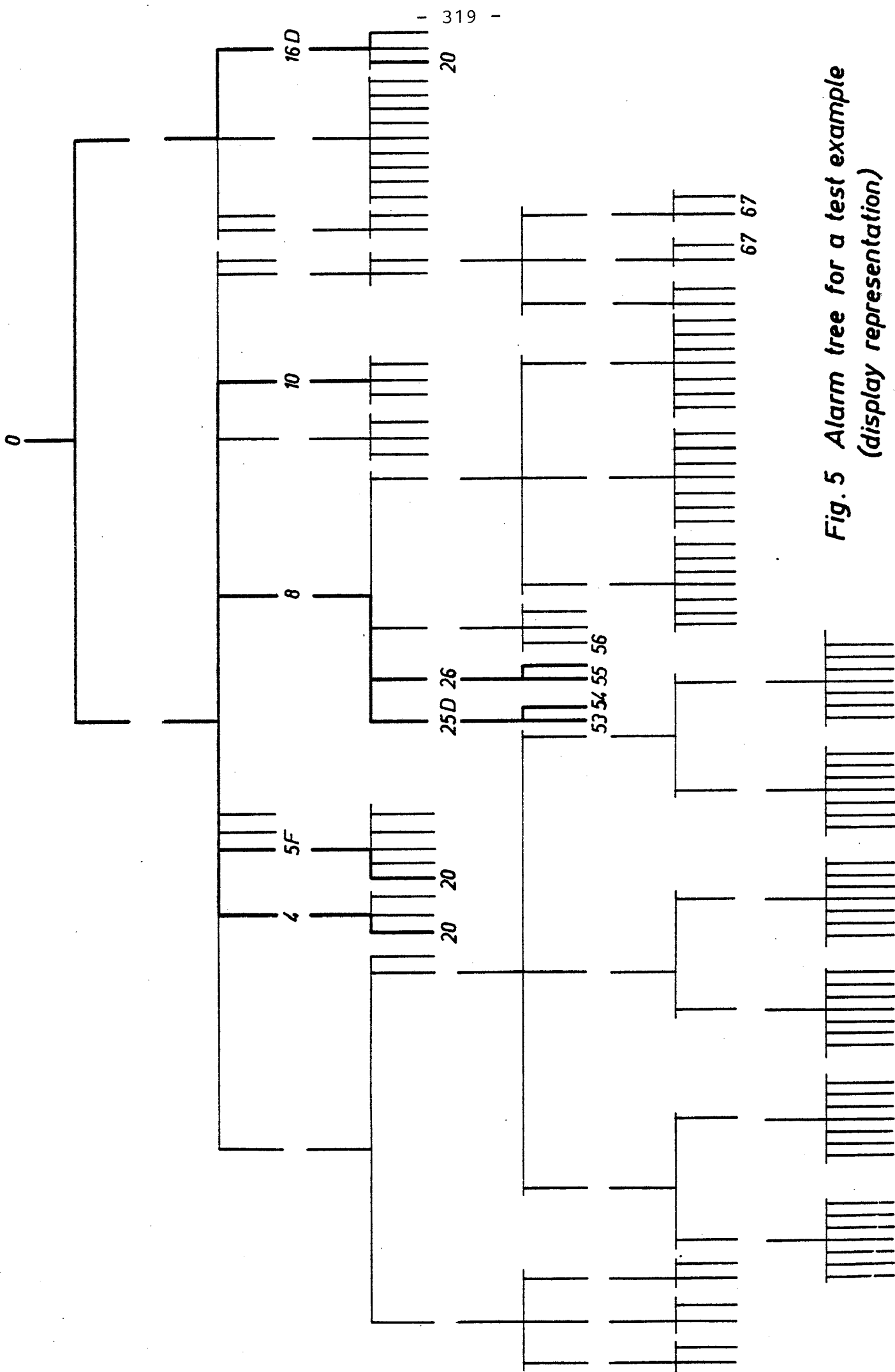


Fig. 4 Schematic representation of the computer system



**Fig. 5 Alarm tree for a test example
(display representation)**

L. Felkel, A. Zapp

THEORETICAL ASPECTS OF DISTURBANCE ANALYSIS

THEORETICAL ASPECTS OF DISTURBANCE ANALYSIS

L. Felkel, A. Zapp
Gesellschaft für Reaktorsicherheit (GRS) mbH
Garching, Germany F.R.

1. Introduction

How far can you usefully be from the truth?

Nasrudin saw some tasty-looking ducks playing in a pool. When he tried to catch them they flew away. He put some bread in the water and started to eat it.

Some people asked him what he was doing. "I am eating duck soup", said the Mullah.

When we consider really large processes like that of a nuclear power plant, we are faced with the task of determining the status of the process. The plant instrumentation supplies information about the process to the control room and operator. Being only a partial mapping of the process though, the signals still carry an enormous amount of information. In a nuclear power plant of the 1300 MWe PWR class, for example, there are about 8000 binary status indicators, let alone analog signals which could in another non-surjective mapping be discretized giving a total of about 30 000 bits in a binary status pattern. This would amount to $2^{30\ 000}$ possible process states from point of view of instrumentation under the assumption of equiprobability of the states.

With

$$H(x) = \sum_{i=1}^N p(x_i) \lg \frac{1}{p(x_i)} \text{ [bits]}$$

the excessive quantity of information at each time interval Δt would result to

$$H = \sum_{i=1}^{30000} \frac{1}{30000} \lg 30000 = \lg 30000 \cong \lg 2^{15} = 15 \text{ [bits]}$$

This figure is beyond of being processable. From this can be seen, that a complete description or representation of a process of this size is utterly impossible.

Our human experience, however, shows that we are able to control such processes and that we implicitly (the operator) or explicitly (the simulator) use models of the process or parts of it in an incomplete but effective way: This is mainly for two reasons:

- 1) The states outlined above are (fortunately) not equiprobable and not equally significant.
- 2) We abstract the real process to a model process and thereby we can master complexity.

In three ways, as a consequence, we deviate from the "truth" of the process:

- 1) We get incomplete information about the process,
- 2) We zero probabilities of occurrence of states, whose probability or significance is next to zero.
- 3) When modelling the process we consider only "significant" parts of the overall behaviour.

What we need now is a formal methodology and criteria for determining "how far we can usefully be from the truth" quantitatively and depending on the purpose of the application.

The application considered in this paper is disturbance analysis and man-machine-communication /12/.

As is pointed out in numerous papers /1,2/, the models used for disturbance analysis are cause-consequence diagrams. These are directed graphs which carry additional information, so as to construct the information flow to the operator at any stage during analysis. Graph theory, therefore, plays a major rôle in this paper (chapter 3).

Graphs, however well they provide an intuitive understanding of the disturbance propagation, are in their original form not directly processable by a computer. A verbal representation (description) has to be provided. This is done by formal languages. Problems of syntactical expressibility are also discussed (chapter 4).

Construction of process models is a difficult and error-prone task. However, methods are being developed to (partly) automatize it. Some approaches will be discussed, as well as the basic requirements of process knowledge and level of abstraction, in chapter 5.

Chapter 2 is a collection of basic definitions referred to in each of the chapters.

2) Basic Concepts

Graphs /13/

A graph is a pair (N, E) where N is the set of nodes and $E \subset N \times N$ is the set of edges. The graph is finite iff ^{*)} N is finite. A graph is directed if E is a set of ordered pairs. A path p from n_1 to n_k is a sequence of edges $p_{n_1 n_k} = (n_1 n_2) \dots (n_{i-1} n_i) (n_i n_{i+1}) \dots (n_{k-1} n_k)$.

A graph is acyclic iff \forall paths $p_{nk}: n \neq k$. Any mapping $m: E \rightarrow L$ is called labelling. The triple (N, E, m) is called a labelled graph.

*) iff stands for "if and only if".

Grammars /13/

A context-free grammar is a quadruple (V, T, Π, S) . V is a set of symbols, T is the set of terminal symbols, $V-T$ is the set of syntactic variables. V^* is the free semigroup on the set of symbols under concatenation. The string $\epsilon \in V^*$ is called the empty string, i.e. the string which consists of no symbols at all. $V^+ = V^* - \{\epsilon\}$. $\Pi \subset (V-T) \times V^*$ is the set of production rules. $\pi \in \Pi$ is usually written as $(a ::= b)$, where $a \in (V-T)$ and $b \in V^*$. $S \in (V-T)$ is the start symbol. The relation $\rightarrow \subset (V-T)^+ \times V^*$ is called direct derivation, written $\alpha \rightarrow \beta$ where $\alpha = \alpha_1 a \alpha_2$ and $\beta = \beta_1 b \beta_2$ and $(a ::= b) \in \Pi$. The relation $\rightarrow^* \subset (V-T)^+ \times V^*$ is the transitive closure of \rightarrow , written $\alpha \rightarrow^* \beta$, where $\alpha = \alpha_1 \rightarrow \alpha_2 \rightarrow \dots \rightarrow \alpha_n = \beta$. The language L generated by grammar G is the set of all terminal strings which can be derived from the start symbol, i.e. $L(G) = \{w \in T^* \mid S \rightarrow^* w\}$.

Automata /13/

A finite (deterministic) automaton M over an alphabet Σ is the quintuple $(K, \Sigma, \delta, q_0, F)$. K is a finite nonempty set called states, Σ is a finite input alphabet. δ is a mapping of $K \times \Sigma$ into K called the state transition function. $q_0 \in K$ is the initial state, $F \subset K$ is the set of final states. $\hat{\delta}$ is the transitive closure of δ , i.e. $\hat{\delta} : K \times \Sigma^* \rightarrow K$ with $\hat{\delta}(q, \epsilon) = q$ and $\hat{\delta}(q, xa) = \delta(\hat{\delta}(q, x), a)$, $x \in \Sigma^*$, $a \in \Sigma$. Thus $\hat{\delta} \equiv \delta$ on Σ . The set of strings accepted by M is $T(M) = \{x \in \Sigma^* \mid \hat{\delta}(q_0, x) \in F\}$, i.e. all strings which eventually cause state transition to a final state.

Fuzzy sets /14/

Let X be a set of objects. A fuzzy set A is characterized by a membership function $f_A(x \in X) \in [0, 1]$, i.e. for each $x \in X$ there is a real value $\in [0, 1]$ to denote the grade of membership of x in A . $f_A(x \in X) = 1$ is equal to the "classical" $x \in A$ and $f_A(x \in X) = 0$ to $x \notin A$. The fuzzy sets A and B are equal iff $f_A(x \in X) = f_B(x \in X)$ for all x . The complement A^c of A in X is denoted by $f_{A^c}(x \in X) = 1 - f_A(x \in X)$. Containment is defined by $A \subset B$ iff $f_A(x \in X) \leq f_B(x \in X) \forall x \in X$.

Union $C = A \cup B$ is $f_C(x \in X) = \text{Max}_{x \in X} [f_A(x \in X), f_B(x \in X)]$

and intersection $C = A \cap B$ is $f_C(x \in X) = \text{Min}_{x \in X} [f_A(x \in X), f_B(x \in X)]$.

3) Process Models /15/

Systems analysis is to provide information about the behaviour of the process in general and the propagation of disturbances in particular. The first question to ask therefore is: What is an event, especially an undesired one?

A process consists of a (hopefully finite) set of physical variables V and constants C . The variables $v \in V$ have at any time point a specific value $v(t)$. The state S_p of the process p at time t then is the values of all variables at time t , i.e. $S_p(t) = (v_1(t), \dots, v_n(t))$. Each of the variables have technical specification limits $ub(V_i(t))$ and $lb(V_i(t))$ (upper and lower bounds resp.), which may be dynamically dependent on the values of other variables.

The state of the process usually is not constant and the subsequent state depends on the previous set of variables with their values and a state transition function $ST: T \times V \rightarrow V$. T isomorphic to \mathbb{R} or \mathbb{N} and the systems are called continuous or discrete in time resp.

Every transition from one state to another is called an event. Formally an event is one pair $(t, v) \in T \times V$, where $T \times V$ is the event space. The event space can be subdivided in a finite number of disjoint subsets called "modes of operation". Note that in practice this subdivision is a collection of fuzzy subsets, since often it is left to engineering judgement as to where one mode of operation ends and the other starts. The subdivision on the event space also includes subdivisions on the sets $\{ub^{(v_i)} \mid i \in I\}$ and $\{lb^{(v_i)} \mid i \in I\}$. Also the subdivision of the event space requires to split the state transition function into different domains of the time frame as far as there is a fixed sequence in which the modes have to be run. If in addition there are several options for mode of operation, different partial state transition functions may be applied to the same portion of the time domain.

Since we have assumed that there is only a finite number of modes, we can express the mode transition by a finite automaton. An example is given for the Biblis Block B plant (see also chapter 2, automata).

Set of states $K = \{a_0, a, b, c, e, f, i_1, i_2, i_3, i_4, m, p\}$

Set of inputs $\Sigma = \{m_0, m_1 \dots m_{12}, \text{auto}_1, \text{auto}_2 \dots \text{auto}_4, \text{TT}, \text{RT}, \text{corr}_1, \text{corr}_2 \dots \text{corr}_4, \text{undef}_1, \text{undef}_2, \text{undef}_3, \text{dis}_1, \text{dis}_2 \dots \text{dis}_4\}$

The state transition function : $K \times \Sigma \rightarrow K$ is given in the following table:

$\{(a_0, m_0)=a, (a, m_1)=b, (b, m_2)=c, (c, m_3)=d,$
 $(d, m_4)=e, (e, m_5)=f, (f, \text{dis}_1)=i_1, (i_1, \text{auto}_1)=m,$
 $(i_1, \text{TT})=d, (i_1, \text{RT})=c, (i_1, \text{corr}_1)=f, (f, m_6)=e,$
 $(e, m_7)=d, (d, m_8)=c, (c, m_9)=b, (b, m_{10})=a,$
 $(a, m_{11})=a_0, (e, \text{dis}_2)=i_2, (i_2, \text{corr}_2)=e, (i_2, \text{TT})=d,$
 $(i_2, \text{RT})=c, (i_2, \text{auto}_2)=m, (d, \text{dis}_3)=i_3, (i_3, \text{corr}_3)=d,$
 $(i_3, \text{RT})=c, (i_3, \text{auto}_3)=m, (c, \text{dis}_4)=i_4, (i_4, \text{corr}_4)=c,$
 $(i_4, m_{12})=b, (i_4, \text{auto}_4)=m, (m, \text{undef}_1)=p, (p, \text{undef}_2)=a,$
 $(p, \text{undef}_3)=b\}$

final states $F = \{a_0\}$

initial state = a_0

In practical application the states can be assigned a meaning:

- a_0 : Reactor during refuelling, reactor lid off
- a : Reactor prepared for refuelling, reactor lid on
- b : Cold subcritical reactor
- c : Hot subcritical reactor
- d : Hot critical reactor, 40% power (turbine not running after Turbine Trip)
- e : Normal operation, turbine power 40%
- f : Normal operation 40-100% power
- i_n : Disturbance, eventually leading to Turbine Trip, Reactor Trip or an emergency situation
- m : Emergency situation
- p : State after emergency, not predictable

The state transitions caused by some (admissible) input are the changes from one mode of operation to another. $m_0 \dots m_{12}$ denote manual operator actions (in a more detailed automaton each of these would be replaced by a sequence of manual actions according to the operations manual). "Auto" denotes automatic control and "corr" are the corrective actions taken to return to a normal state. In practice certain state transitions cannot be predicted in such a deterministic manner, therefore the inputs "undef" have been provided to account for this situation, TT denotes Turbine Trip and RT Reactor Trip. A graphical representation is given by the following graph (see also chapter 2).

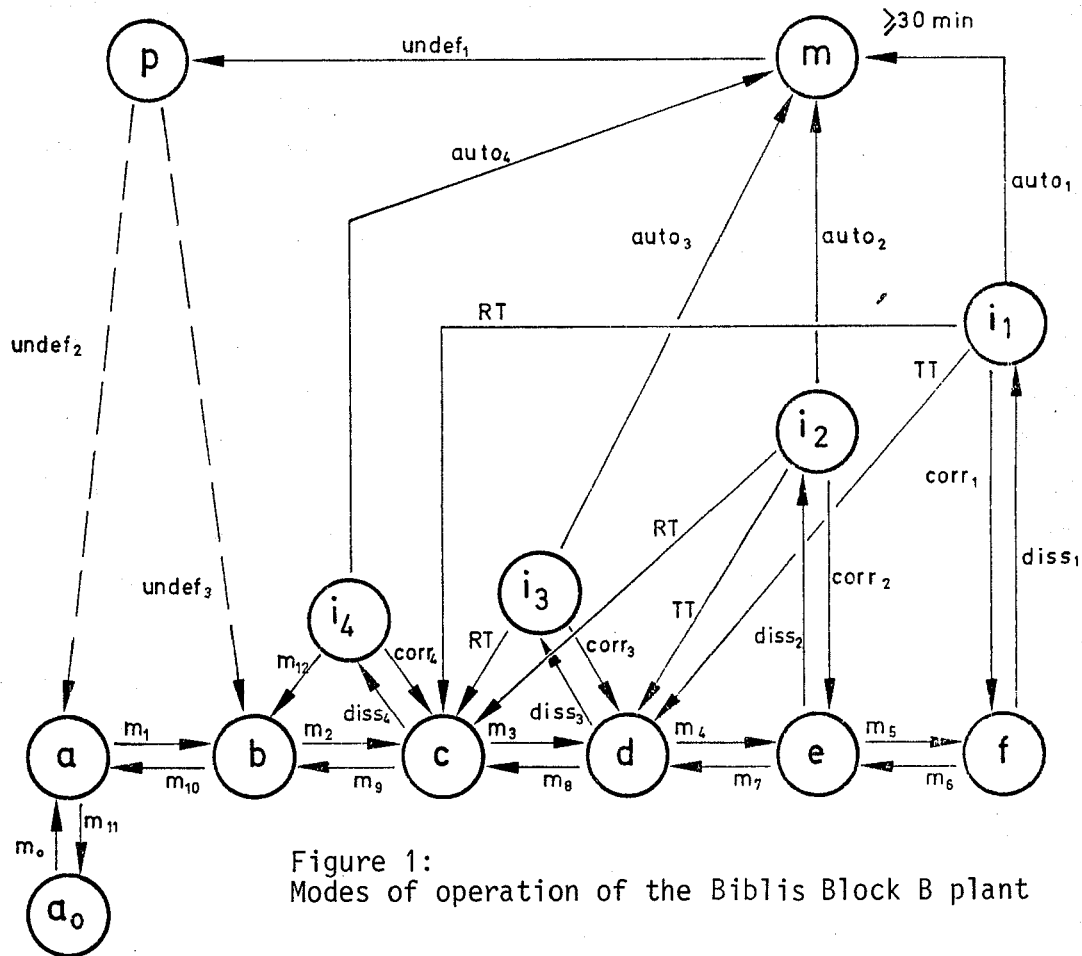


Figure 1: Modes of operation of the Biblis Block B plant

For disturbance analysis we are mainly interested in the transition between nodes e , f , i_n . To be useful in reality the deterministic behaviour of the finite automaton is not adequate since there is no natural clear-cut separation between the different modes of operation.

The other extreme, however, would be to build up a complete mathematical model. Experience shows that with a reasonable effort around 10 - 20 variables can be considered /3/. Then there exists a continuous transition from one mode of operation to another. In a practical application we have to consider not only the main process variables but also many state indicators and secondary variables (some of them measurable by process instrumentation) in the range between 5000 and 10000. This is practically impossible to include in a mathematical model.

Therefore we have to find theoretical concepts to master the plant complexity. Of course some information will be lost, but the model needs to serve only specific purposes and the simplifications may be permissible.

As was pointed out in the example, the states i_n denote disturbance situations, eventually leading to reactor trip or an emergency situation or return to an admissible status. There are several ways of modeling the disturbances. To be consistent with the representation of the "mode of operation" the disturbance might as well be a finite automaton. However, it would be very tedious and error-prone if systems analysts would attempt to create those automata. An equivalent description is therefore required which maps the disturbance in a transparent and straightforward manner. The description chosen here are cause-consequence diagrams. It will be shown in the sequel, how this CCD can be uniquely mapped onto a finite automaton. A simple example is to illustrate the transformation.

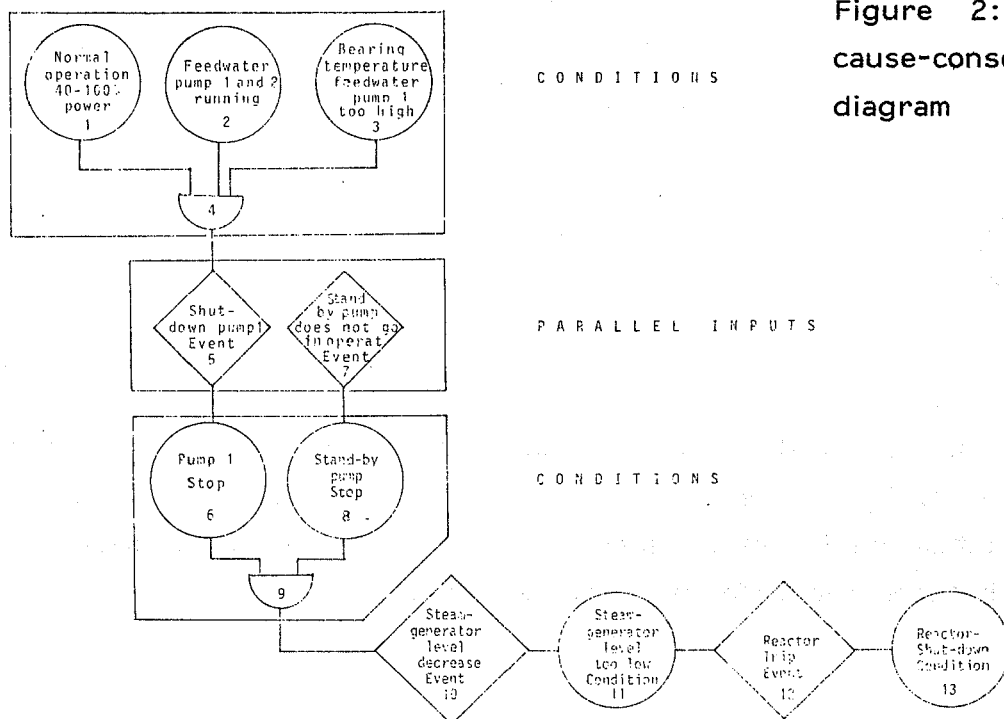


Figure 2: Simple cause-consequence diagram

Assume that we are in state f of example 1. We now have to distinguish between inputs that cause events (state transitions) and conditions (steady state). In example 2 the states 1,2,3,6,8,11 und 13 are conditions, whereas 5,7,10 and 12 are events. The conditions (steady states will be the states of the automaton, i.e. $K = \{ "1&2&3", "6&8", "11", "13" \}$ and the inputs $\Sigma = \{ "5&7", "10", "12" \}$). The "AND"-gates (No. 4 and No. 9) need special treatment. They will be represented by one state comprising those inputs to the AND which have been classified as conditions. The "AND"-gate No. 4 would for example then be represented as:

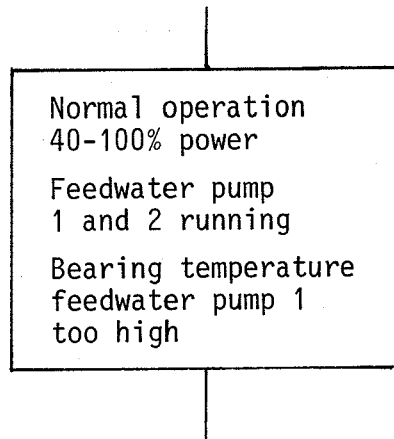
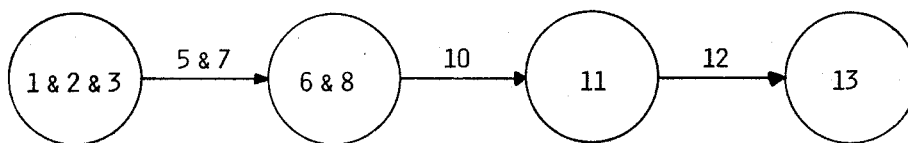


Figure 3:
Transformed
AND-gate

In case of an "OR"-gate instead merging conditions into one state we would have parallel edges from the conditions. Similarly a "NOT"-gate is treated. Since all boolean functions can be expressed by the basic AND, OR and NOT functions, we can by repeated application model all boolean functions.

Figure 4:
The resulting finite automaton



It should be noted that when the conditions and inputs are properly classified there is an algorithm to perform the transformation.

In reality the state transitions are not as deterministic as assumed in the automaton. Thus it would be necessary to add probabilities for transition. These automata are called stochastic automata. The authors believe that

these are to fuzzy set theory what the deterministic ones are to classical set theory. A formal proof, however, is beyond the scope of this paper.

There is one drawback in modeling the process by automata and that is that it is very hard to naturally fit time into these models.

4) Processable Model Representation

In order to easily perform safety analysis and obtain a greater reliability of large-scale dynamical systems, methods for the modelling and computer simulation have been developed in the last ten years. There are several ways to get a model of a dynamical system.

One possibility is to write down the general unsteady state differential equations for mass, energy and momentum transport in the system which has the advantage that if the model is sufficiently detailed one can exactly predict when the process moves from a safe operational state to an unstable, undesired state of operation. The disadvantages of this method are, that with some degree of accuracy these models become very complex and very difficult to solve. Moreover they are usually limited to a specific operating region and mode of failure. Furthermore it is a difficult and tedious task for the systems analyst to construct them and for the transfer of the model to the computer usually a computer scientist is required.

To by-pass at least some of these problems drawing diagrams or graphs of the physical system as an intermediate step in the modeling process can be very helpful. It is not only a very effective and clear way of representation of process models, but also can special graphs very often be used as a basis for programming analog or digital computers.

Two very efficient techniques of generating a mathematical model of a physical system are the linear graph technique /4/ and the bond graph technique /5/. These two techniques provide the systems analyst in a similar way as the cause consequence diagram technique does, with tools which reduce the amount of work for modelling large scale systems.

The first step in the modelling chain, however, consists always in the abstraction from the physical system and the decomposition into subsystems. This step cannot be automatised and therefore none of these techniques give rigid rules or hints to the systems analyst. Its up to him to decide how detailed the models have to be, how strongly the different physical variables affect the dynamic behaviour and what effects can be neglected. Yet, once having decided on the structure of his models, any of these techniques can be used. With only a small set of primitive elements the systems analyst can construct the graph or the diagram from the physical system to be modelled using a special language for either the linear graphs, the bond graphs or the CCD's.

If the graph or the diagram is defined analysis programs can be used for generating a set of equations and computing their solutions from the description of the system to be analysed.

For analysing linear graphs programs called ECAP II and SCEPTRE /6/ have been developed, for the bond graphs a program named ENPORT /7/ can be used. The final dynamical model is a set of differential equations or even an algorithm for its solution on a digital computer.

The same applies to the CCD's. We have shown, that they can be mapped on a finite automaton. It is necessary though, that there exists a formal representation, processable by a digital computer.

Since the CCD's have also been chosen because they do not require system analysts to be computer scientists the processable representation should have the same property.

The basic representation is therefore verbal. To be processable the verbal descriptions have to follow formal requirements. Formal languages and formal grammars (chapter 2) provide the flexibility to serve as link between man and computer.

As an example the grammar used by the model generator MOGEN /1/ is shown in the appendix. It consists of 154 rules and is a context-free grammar. The grammars of this class have the general property that there exists an algorithm to determine whether or not a given string of symbols is in accordance with the grammatical rules given by the grammar.

Context-free here means that a string of symbols that appears on the right-hand-side of a production rule can be replaced by the left-hand-side of the production rule, regardless what the surrounding symbols are. The class of context-free grammars and the appropriate context-free languages can further be subdivided into deterministic and non-deterministic grammars. The deterministic grammars can be parsed in a deterministic fashion, i.e. the application of a production rule to reduce the given input strings is unambiguous. Therefore, when parsing a string generated by a deterministic grammar, no deadlocks are encountered (unlike finding a way through a maze, where you have to trace back and try the other (also admissible) way.)

The obvious advantage is that the parsing time is optimal. There is a significant loss in semantic expressibility though, which has to be traded off against efficiency. The grammar used in the STAR disturbance analysis system still retains sufficient expressibility.

Example 3: Grammar (see Appendix)

It should be noted that context-free languages describe a larger variety of states than finite automata do. They are equivalent to so called push-down automata which comprise an infinite set of (intermediate) states. Thus they may be more adequate describing time dependent processes. However, little research has been done in this field yet.

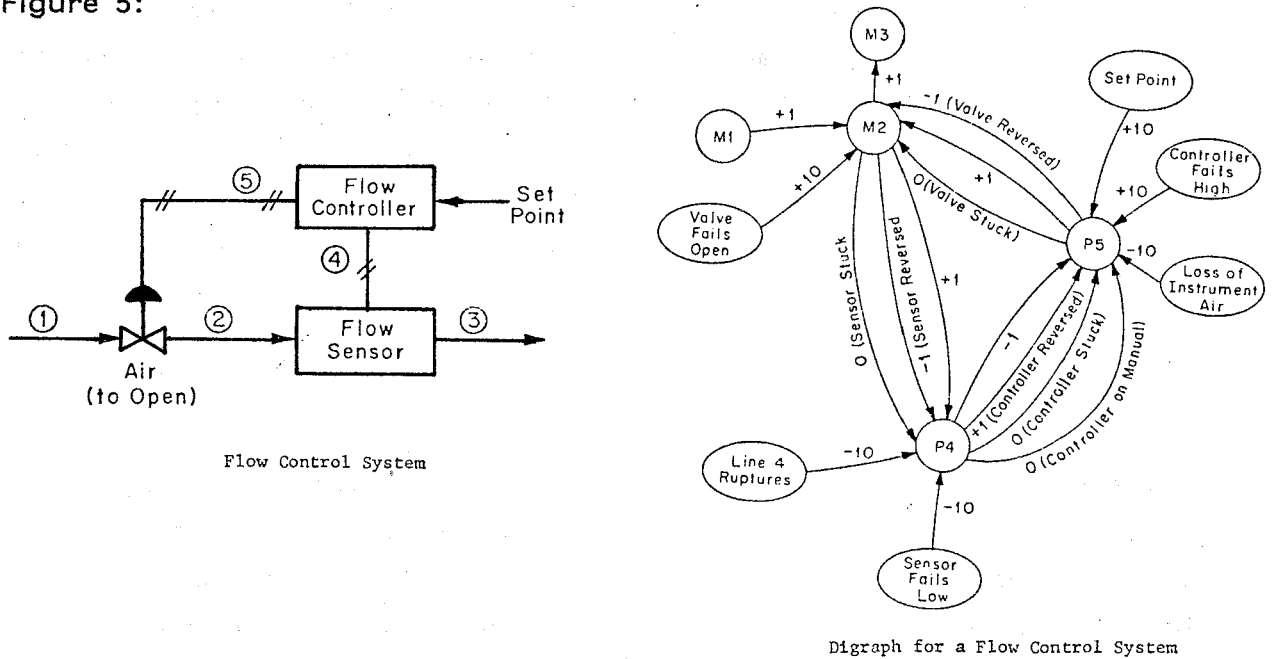
5) Automatic Construction of Process Models

Only recently methods have been developed to (at least partly) automatize the construction of process models suited to particular application.

It is beyond the scope of this paper to describe all of them in detail. Rather a brief overview of work being carried out in this field as well as references are given.

Powers and Lapp /8/ developed a method where, starting from a graph in which essential interactions between components, energy, mass, and momentum are described in a way that the topology of the underlying process is still transparent, by giving the (undesired) top-event. The appropriate fault tree can be generated automatically.

Figure 5:



Taylor and Hollo /9/ developed algorithms where cause-consequence diagrams are automatically (and interactively) generated by the use of component models stored in a component library. A similar method is that of Andow and Lees /10/, who automatically construct fault-trees from "mini-fault-trees", equivalent to the component models of Taylor.

Lind /11/ at present develops so-called flow models where especially the physical properties of the process to be modelled is taken into account. The modelling concepts used are shown in the next example.

Figure 6:

PROCESS etc.		SYMBOL USED IN FLOW STRUCTURE		
		MATERIAL	PURE ENERGY	PROPERTIES VARIABLES
STORAGE	CONTENT			INTENSIVE
				EXTENSIVE
TRANSPORT	FLOW			ACROSS
				THROUGH
BOUNDARY	INTERFACE			POTENTIAL
				PLUX
		(condition)		

Since all these attempts to model the process so as to be processable in a reasonable amount of time and since all of them are algorithmically generated, there is no reason why they should not be describable by a grammar of the type discussed in chapter 4. All the methods may therefore contribute to improving reference models and when associating on-line process data to improve also the information on which disturbance analysis is based.

6) Conclusion

The authors are aware of the fact that the treatment of the theoretical problems connected with disturbance analysis is not at all complete. This is due to the limited space allotted to this paper but is also an indicator, that this research area is relatively new and work is still in progress. The authors feel that many of the problems which evolve with process modelling in general and disturbance analysis and man-machine-communication in particular are being treated in a branch of cybernetics and computer science called artificial intelligence (AI). It would be worth while to investigate the results obtained in AI and to check whether or not they are applicable to process modelling. One aspect of special interest is the question whether or not it is possible to create cause-consequence diagrams automatically, which can deal with non-anticipated hazardous process situations without their being explicitly modelled, thus reducing the probability of human errors and oversights.

References

- /1/ L. Felkel, R. Grumbach, H. Hoermann
Automatic Generation and Application of Disturbance Analysis Models
Halden Project Report, HPR 214, 1978
- /2/ D.S. Nielsen
Use of Cause-consequence Charts in Practical Systems Analysis
Danish Atom. Energy Comm., Res. Est., Risö, Denmark,
Rep. Risö-M-1743 (1974)
- /3/ A. Hoeld, D. Beraha
A Non-linear Digital Simulator for BWR Nuclear Power Plants and
its Application within the Scope of Optimal Digital Load-following
Control
Mathematics and Computers in Simulation XXI(1979) 150-162,
North-Holland P.C.
- /4/ S. Seshu and M.B. Reed
Linear Graphs and Electrical Networks
Addison Wesley, Reading, Mass., 1961.
- /5/ Jean U. Thoma
Grundlagen und Anwendungen der Bonddiagramme
Verlag W. Girardet, Essen, 1974.
- /6/ S.R. Sedore, et al.
Mathematical Formulation of SCEPTRE
Air Force Weapons Laboratory, AFWL-TR-72-77,
Kirtland Air Force Base, N.M.
- /7/ R.C. Rosenberg
ENPORT User's Guide
Michigan State University, Div. of Engineering Research,
E. Lansing, Michigan, June 1972.
- /8/ G. Powers, S.A. Lapp
The Synthesis of Fault Trees
Internat. Conf. on Nucl. Syst. Rel. Eng. and Risk Ass.,
Gatlinburg, June 1977

- / 9/ J.R. Taylor, E. Hollo
Experience with Algorithmus for Automatic Failure Analysis
Internat. Conf. on Nucl. Syst. Rel. Eng. and Risk Ass.
Gatlinburg, June, 1977.
- /10/ P.K. Andow, F.P. Lees and C.P. Murphy
The propagation of Faults in Process Plant: a State of the Art
Review, in "Chemical Process Hazards with Special Reference to
Plant Design",
Vol.7, Instn Chem.Engrs, London (1980).
- /11/ M. Lind
The Use of Flow Models for Automated Plant Diagnosis
Paper presented at NATO Symposium "Human Detection and
Diagnosis of System Failures",
Roskilde, August 1980.
- /12/ T. Sheridan, W.R. Ferrell
Man-Machine Systems: Information, Control and Design.
Models of Human Performance. MIT Press, 1974.
- /13/ J.E. Hopcroft, J.D. Ullman
Formal Languages and their Relation to Automata,
Addison Wesley, 1969.
- /14/ L.A. Zadeh
Fuzzy Sets
Inf.& Contr., Vol.8, pp 338-353, 1965
- /15/ R.E. Kalman, P.L. Falb, M.A. Arbib
Topics in Mathematical System Theory
McGraw Hill, New York, 1969.

APPENDIX

EDITED GRAMMAR

```

1 <DESCRIPTION> ::= <MODULES> _ _
2 <MODULES> ::= <MODULES> <MODULE>
3 <MODULE>
4 <MODULE> ::= <MODULEDESCRIPTION> <NODES>
5 <MODULEDESCRIPTION> ::= <MODTEXT> <PRIO> <MODCOMP> <LIMITS>
6 <MODTEXT> ::= SYSTEM : TEXT ;
7 <PRIO> ::=
8     PRIORITY : INTEGER ;
9 <MODCOMP> ::= COMPONENTS : <LIST-OF-EVENTNUMBERS> ;
10
11 <LIMITS> ::= <LIMITS> <LIMIT>
12 <LIMIT>
13
14 <LIMIT> ::= <PROCESS-VARIABLE> <LIMIT-ID> <HIGH> <LOW>
15 <PROCESS-VARIABLE> ::= SIGNAL-NO : INTEGER
16 <LIMIT-ID> ::= LIMIT-NO : INTEGER
17 <HIGH> ::= HIGH : <FIX-FLOAT>
18
19 <LOW> ::= LOW : <FIX-FLOAT>
20 <LIST-OF-EVENTNUMBERS> ::= <LIST-OF-EVENTNUMBERS> , INTEGER
21 INTEGER
22 <NODES> ::= <NODES> <NODE>
23 <NODE>
24 <NODE> ::= <EVENTDESCRIPTION>
25 <LOGICUNITDESCRIPTION>
26 <EVENTDESCRIPTION> ::= EVENT : <E-NUMBER> <DESCRIPTOR>
27 <LOGICUNITDESCRIPTION> ::= LOGICUNIT : <L-NUMBER> <LOGICUNIT>
28 <DESCRIPTOR> ::= <DOC> <PROP> <SUCC> <EXP-EVENTS> <PAGE> <PSPEC>
29 <EXP-EVENTS> ::= EXPECTED : <LIST-OF-EVENTNUMBERS> ;
30
31 <PROP> ::= PROPERTIES : <L-O-P-SPECS> ;
32
33 <SUCC> ::= SUCCESSORS : <SUCC-LIST> ;
34 SUCCESSORS : <Y-N-E-SUCC> ;
35
36 <L-O-P-SPECS> ::= <PROP-SPEC>
37 <L-O-P-SPECS> , <PROP-SPEC>
38 <SUCC-LIST> ::= <S-EDGE>
39 <SUCC-LIST> , <S-EDGE>
40 <S-EDGE> ::= <S-NUMBER> <T-P-DENOTATION>
41 <S-NUMBER> ::= E- INTEGER
42 L- INTEGER
43 <PROP-SPEC> ::= BIT-NO= INTEGER
44 MESSAGE : TEXT
45 MESSAGE LIKE <E-NUMBER>
46 DEDUCED BY <BOOL-EXPRESSION>
47 ISOLATED
48 RMESSAGE
49 QUESTION TO <TARGET>
50 ALARM
51 PRIME-CAUSE
52 SECONDARY-CAUSE
53 WARNING
54 ENTRY : TEXT
55 EXIT : TEXT
56 <BOOL-EXPRESSION> ::= <BOOL-TERM>
57 <BOOL-TERM>
58 <BOOL-EXPRESSION> ! <BOOL-TERM>
59 <BOOL-TERM> ::= <BOOL-FACTOR>
60 <BOOL-TERM> & <BOOL-FACTOR>
61 <BOOL-FACTOR> ::= <E-NUMBER>
62 ( <BOOL-EXPRESSION> )
63 <TARGET> ::= OPERATOR
64 SYSTEM
65 PROCESS
66 <LIMIT-ID>
67 <Y-N-E-SUCC> ::= <YES> <NO> <ELSE>
68 <YES> ::= YES : <SUCC-LIST>
69 <NO> ::= NO : <SUCC-LIST>
70 <ELSE> ::= ELSE <SUCC-LIST>
71
72 <LOGICUNIT> ::= * <BOOLEANSTANDARD> * <I/O> ;
73 <DECISIONTABLE> ;
74 <PAGE> ::= REFERENDES : TEXT ;
75
76 <PSPEC> ::= SPECIFICATIONS : TEXT ;
77
78 <BOOLEANSTANDARD> ::= AND
79 NOT
80 OR
81 INTEGER OUT OF INTEGER
82 <I/O> ::= <ITIN> <ITOUT>
83 <ITIN> ::= IN : <ITEMS>

```

```

84 <ITOUT> ::= OUT : <T-P-ITEMS>
85 <T-P-ITEMS> ::= <T-P-ITEMS> , <T-P-ITEM>
86 <T-P-ITEM>
87 <T-P-ITEM> ::= <ITEM> <T-P-DENOTATION>
88 <ITEMS> ::= <ITEMS> , <ITEM>
89 <ITEM>
90 <ITEM> ::= E- INTEGER
91 L- INTEGER
92 <DECISIONTABLE> ::= <LIN> <LOUT>
93 <LIN> ::= IN : <LINES>
94 <LOUT> ::= OUT : <T-P-LINES>
95 <T-P-LINES> ::= <T-P-LINES> , <T-P-LINE>
96 <T-P-LINE>
97 <T-P-LINE> ::= <LINE> <T-P-DENOTATION>
98 <LINES> ::= <LINES> , <LINE>
99 <LINE>
100 <LINE> ::= <ITEM> <BOOLEANNUMBER>
101 <BOOLEANNUMBER> ::= <BOOLEANDIGIT>
102 <BOOLEANNUMBER> <BOOLEANDIGIT>
103 <BOOLEANDIGIT> ::= 0
104 L
105 <T-P-DENOTATION> ::= / <DELAY> , <PROBABILITY> /
106 / <DELAY> /
107 / <PROBABILITY> /
108
109 <DELAY> ::= D : INTEGER
110 D : INTEGER - INTEGER
111 <PROBABILITY> ::= P : <FIX-FLOAT>
112 <FIX-FLOAT> ::= <FRACTION> <EXPONENT>
113 <FRACTION> ::= INTEGER . INTEGER
114 - INTEGER . INTEGER
115 <EXPONENT> ::= * * - INTEGER
116 * * INTEGER
117
118 <DOC> ::= DOCUMENTATION : TEXT <DISPLAY> ;
119 DOCUMENTATION LIKE <E-NUMBER>
120
121 <DISPLAY> ::= / <FG> <BG> <DIR> <BLINK> /
122
123 <FG> ::= FG : <COLOUR>
124
125 <BG> ::= BG : <COLOUR>
126
127 <DIR> ::= DIR : <DIRECTION>
128
129 <BLINK> ::= BLINK
130 NOBLINK
131
132 <COLOUR> ::= RED
133 LIGHT-GREEN
134 DARK-GREEN
135 YELLOW
136 BROWN
137 BLACK
138 WHITE
139 VIOLET
140 LIGHT-BLUE
141 DARK-BLUE
142 PURPLE
143 ORANGE
144 AMBER
145 GREY
146 CRIMSON
147 PINK
148 <DIRECTION> ::= LEFT
149 RIGHT
150 UP
151 DOWN
152 <E-NUMBER> ::= INTEGER
153 L-NUMBER ::= INTEGER

```

*** NOTE *** CALLED FOR A NEW ALLOCATION - CASE 4

CONTENTS

Session IV

APPROACHES TO SPECIAL SURVEILLANCE PROBLEMS

Chairperson: J. Furet

Secretary: A. Zapp

J. Furet	
SUMMARY OF SESSION IV	343
A. Nedelik, H. Roggenbauer	
A COMPUTERIZED SYSTEM FOR EVALUATION OF THE STATUS OF A PROTECTION SYSTEM	349
R. Haubert, R. Stokke	
MONITORING READINESS OF SAFETY RELEVANT DEVICES IN NUCLEAR POWER PLANTS BY MEANS OF CRT-COLOUR DISPLAYS	363
P. Cormault	
SURVEILLANCE SYSTEMS UNDER DEVELOPMENT AT ELECTRICITE DE FRANCE	381
Y. Hashimoto, K. Kawai, M. Suzuki, S. Izumi, Y. Michiguchi, K. Yamada, T. Joge	
ACOUSTICAL SIGNAL PROCESSING FOR LIGHT WATER REACTOR DIAGNOSIS	393
R. Assedo, P. Bernard, J.C. Carre, J. Cloue, A. Epstein	
PWR NEUTRON NOISE SURVEILLANCE: NOISE SOURCES AND THEIR EFFECTS	407

G. Zwingelstein, M. Déat, Le Guillou APPLICATION OF PATTERN RECOGNITION TECHNIQUES TO THE DETECTION OF THE PHENIX REACTOR CONTROL RODS VIBRATIONS	439
M. Edelmann SIMULATION OF FUEL ELEMENT THERMAL HYDRAULICS FOR SENSITIVE MONITORING OF COOLANT FLOW	455
G. Weinkötz, H. Martin, L. Krebs DETECTION OF COOLANT DISTURBANCES IN THE FUEL ELEMENTS OF AN LMFBR BY TEMPERATURE FLUCTUATION ANALYSIS	483
P. Liewers, P. Schumann, F.P. Weiß USE OF NOISE DIAGNOSIS FOR SURVEILLANCE OF PARTI- CULAR DISTURBING PROCESSES IN A PRESSURIZED WATER REACTOR	497
<u>Written Contributions</u>	
M. Sato, T. Sato, A. Kameda, Y. Yoneda OPERATIONAL GUIDANCE EQUIPMENT FOR FUEL HANDLING SYSTEM	509
G.P. Beraud, A. Bonnemay, A. Le Dieu de Ville, J.C. Nimal ESTIMATION OF LOCAL POWER IN A PWR CORE FROM GAMMA RAYS MEASUREMENTS	525

J. Furet

SUMMARY OF SESSION IV

J. Furet

SUMMARY OF SESSION IV

In this session we had four presentations dealing with noise analysis technics, one presentation referring to a computerized system for evaluation the state of protection system, and one presentation referring to surveillance systems under development concerning turbines and electric generators.

The first presentation has shown us the large possibility and the effectiveness of the computerized system when it is associated with CRT colour displays. It seems to me that this tool can be very usefully developed and used for other systems of the nuclear power plant control equipments.

The attention given to the surveillance of turbine and generator has been outlined. In fact as you know the availability of these two main components of the balance of the plant have a great incidence on the availability and the safety of the nuclear reactor. This explains the necessity in the near future of the development of specific equipment for this.

We have noticed in the presentation the importance of the memory needed by this specific equipment.

Concerning the surveillance problems dealing with the noise analysis technics, you have certainly noticed the great improvement of their use. In this domain we are now far away from theoretical work and theses, as it was several years ago during a too long period.

The authors of the papers concerned by these technics have given a lot of results obtained on power plant and this has convinced us that it is possible with these methods to detect disturbances or failures in the structures or near the structures of the nuclear core. But it seems that for localising these disturbances and failures and to evaluate their impact on the safety and availability, the evaluation of the results of noise analysis has to be made by what we call "noise people" and this may explain why all these presentations have been made by people of the research domain.

We have now to convince utility people: operators or plant manager to use these technics and equipments associated as a communication system between them and the nuclear power plant. As you know, this is not easy to obtain and I hope that the noise international team specialists will be happy in this way.

My personal opinion is that to be successful in this way, it is necessary to improve the knowledge and the background of operators. This improvement has to be made not only by training and education but by including in the operators team people which are familiar and which have experience in the noise analysis technics, nuclear engineering and digital computers.

And now if you permit Mr. Chairman, I want to comment briefly on the program which is going in every country on procedures and systems for assisting operators during abnormal nuclear power plant situations.

For this, during this meeting we have seen that technics, methods, specific equipment, some of them very sophisticated, are now available. We have also heard that a lot of experience is available.

To improve this experience and the use of the tools, it is necessary for the people of the domain to go back more often and more deeply to the nuclear process and also to the steam process, and it is necessary for them to go more deeply in the analysis of the results

of the operation of the nuclear power plants. It is necessary to analyse and examine in more details the incidents and accidents which occurred. But for this, the need of precise information on these incidents and accidents is very important. It is in fact necessary to know and to take care of all details of main incidents or accidents of nuclear world community. In this domain, we have to follow, may be with the aid and support of the international atomic agency, the recent example of our colleagues of U.S.A.

We have to thank them for giving all over the world, rapid and precise information, about Three Mile Island incident.

Thank you Mr. Chairman and all of you for your patience and attention.

A. Nedelik, H. Roggenbauer

A COMPUTERIZED SYSTEM FOR EVALUATION OF THE STATUS OF A
PROTECTION SYSTEM

A COMPUTERIZED SYSTEM FOR EVALUATION
OF THE STATUS OF A PROTECTION SYSTEM

A. Nedelik, H. Roggenbauer
Österreichische Studiengesellschaft für
Atomenergie Ges.m.b.H.

Specialists' Meeting on "Procedures and Systems for Assisting
an Operator during Normal and Anomalous Nuclear Power Plant
Operation Situations",
Munich, December 5 - 7, 1979

1. The protection system

The protection system of a reactor may be viewed as a powerful controller, superimposed on the reactor and its operational control systems. Normal operation of the plant occurs within the dead band of this "controller" and no interference from the safety actuation systems (the "actuator" of the protection system) is to be expected.

If, however, the controller output is actuated (either by monitored safety variables exceeding pre-set limits or by internal failures in the protection system) the absolute priority of these protective actions usually interrupts normal reactor operation immediately.

It should be noted that spurious initiation of safety actions is not only an economic burden but also undesirable in view of plant safety, especially if "not distinctly safety-oriented" actions are started (e.g. cold water injection into the core).

For this reason our "controller" must be designed with a high degree of reliability, it must be tolerant to both active and passive failures (i.e. spurious actions as well as failure to respond properly on demand).

To achieve this goals, a variety of special design principles are employed: self-checking instruments, redundancy and diversity of equipment and many other measures.

A peculiarity of the complex controller "protection system" is, that it is designed to cope with complete event sequences (design basis accidents or postulated initiating

events) and not just controlling single variables. Nevertheless, the input information consists of physical values (safety variables) such as pressure, neutron flux, etc. The system logic has to interpret this information and must initiate appropriate counter measures. (Fig. 1).

Normally each postulated initiating event is to be recognized by at least two diverse criteria and has to be controlled or mitigated by the proper set of protective actions. (Fig. 2). This of course adds enormously to the complexity of the system.

A minimum design requirement is the system's tolerance of a single failure (and its consequences) without losing the ability to perform the required protective tasks. This means, that as long as the system is running "as designed", the operator may rely on the designer for this "single failure criterion" being met.

However, according to current safety philosophies (e.g. KTA 3501) this requirement also applies to a system which is temporarily degraded by repair, test or other influences.

By making use of the redundancy and diversity of the protection system this can usually be assured, even if an additional random defect may occur before the first failure has been repaired.

To justify continuation of operation under these circumstances, the operator has to check whether his remaining system still fulfills its basic design goals and whether all general and plant specific regulatory requirements are met.

This evaluation has to be made within short time, one of the possible consequences being the need for immediate controlled shut-down of the reactor.

For this reason a fast and un-ambiguous evaluation of the given situation (including specific instructions which may be spread over different chapters of the operation manual) is very important not only for the safety but also for the availability of the plant.

2. Evaluating the status of the protection system

Since the protection system is essentially functioning as a stand-by system, the question arises, how failures of its components or parts of the system can be

- detected and localized
- evaluated with respect to the (degraded) system's ability to perform its protective tasks.

Well established methods for failure detection and identification exist (e.g. use of comparators, automatic and manual testing, various annunciation equipment, alarm indication etc.). In many cases the faulty component can be directly displayed by the process computer, especially in the electronic sections of the system.

In comparison to these possibilities the evaluation of the newly created system status is to a large extent dependent on the operator's experience and familiarity with his plant. As mentioned above, the problem is not so much the "first" failure in an otherwise fully undisturbed system but the occurrence of a "second" failure (in general independent of the first) before the originally defective component has been repaired or replaced.

The evaluation whether the resulting combination of these particular failures leaves the system within the limits set by safety regulations may not always be done easily and quickly.

It seems unfair to force this decision fully on the operator in a stress situation.

Example: Fig. 3 shows very schematically the high pressure and low pressure cooling systems together with the reactor vessel water level transmitters of a hypothetical BWR. Three protective actions using reactor level as initiating criteria are also shown.

Assuming an initial status of pump A undergoing inspection and transmitter 1' being in the "fail-high" state, it is certainly not obvious that the reactor is actually in a potentially dangerous situation. Suppose, however, that - as a human error or a random occurrence - an instrument line in redundancy 2 or 3 were interrupted to make the associated level signals to fail "high". This would cause stop of feedwater flow and high pressure cooling (active failure) as well as disabling start of low pressure cooling (passive failure). This totally unacceptable situation would be avoided by a proper information system, requiring for instance an immediate controlled shut-down for the assumed initial failure combination.

It should be noted, that using a 2v 4 system would improve the tolerance towards passive failures as compared with a 2v3 system, but the possibility of loss of a protective task remains unchanged.

3. Table of "second failures" and "RGB"

During the safety assessment for licensing the first Austrian nuclear power plant the problem of failure combinations in the protection system and safety systems as

well as their evaluation was taken up. The ensuing discussions finally led to the development of decision matrices, the so-called "tables of second failures". These tables have been included in the operation manual, to assist the operator in his evaluation of a given situation. (Because of this historical development many features of this presentation that may seem very plant specific can be explained by this fact.)

Assuming that a component failure has been detected and identified, the component is declared having "failed", regardless of its mode of defect - it may be in the "tripped" or "untripped" state (the only exception being the safety function "reactor scram", which can be regarded as distinctly safety oriented. In this case failed components are switched deliberately to "tripped state").

There are several reasons for this treatment:

- Faulty actuation of "not distinctly safety oriented" functions may (under certain circumstances) be as undesirable as temporarily paralysing protective actions.
- It cannot be excluded that during repair the state of a component being repaired is switched.
- It is a conservative assumption (worst - case treatment)
- The resulting tables become less complex.

Input to the tables of second failures are simply the code-numbers of failed units or system parts, the output consists of an instruction whether operation may be continued or not. In addition permissible repair times are given, based on probabilistic assumptions about the maximum tolerable unavailability of each protective function.

In the first version of tables this probability analysis has been made by designer, safety assessors and plant operator in a mainly qualitative manner, based on experience and good engineering judgement. Nevertheless the result should be a marked advantage compared to the situation, where the same kind of analysis is demanded from the operator alone within minutes! It should be mentioned that this non-mathematical first approach did try to take into account the increased probability of additional failures in a redundancy caused by repair work being done in this part of the protection system.

Experience showed, however, that the practical utilisation of the somewhat voluminous lists is rather inconvenient, so the idea of programming the tables for a computer evolved rather naturally.

For this purpose, and in order to study ways of optimum display on a small scale model, a hypothetical, simplified BWR-protection system has been designed as a basis for programming a pilot version of a "table of second failures".

Once a computerized system of this kind - not replacing but completing the written operation manual - has been accepted, it is logical to extend its use to other parts of this manual.

For this reason - some what ambitiously - the working title "RGB" for the project has been chosen. This is the abbreviation of "Rechnergestütztes Betriebshandbuch" or computerized operation manual.

At the moment further work on this subject is being done together with OECD Halden project.

The development work in the near future will concentrate on more general aspects and on the assessment of reliability characteristics of degraded redundant systems with the help of statistical methods. This shall serve primarily to refine the determination of repair and maintenance strategies for redundant systems in general and for reactor protection systems in particular.

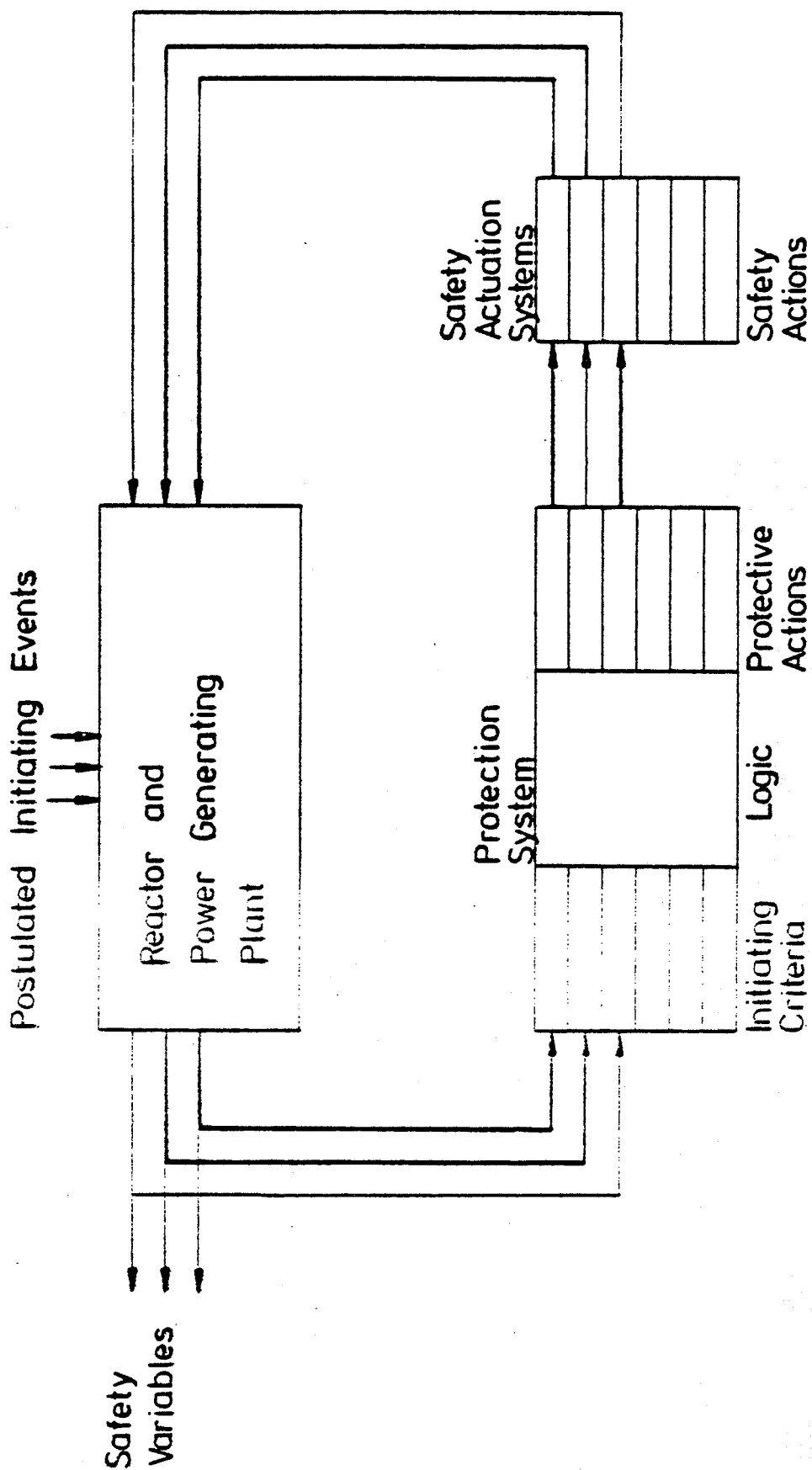


Fig.: 1

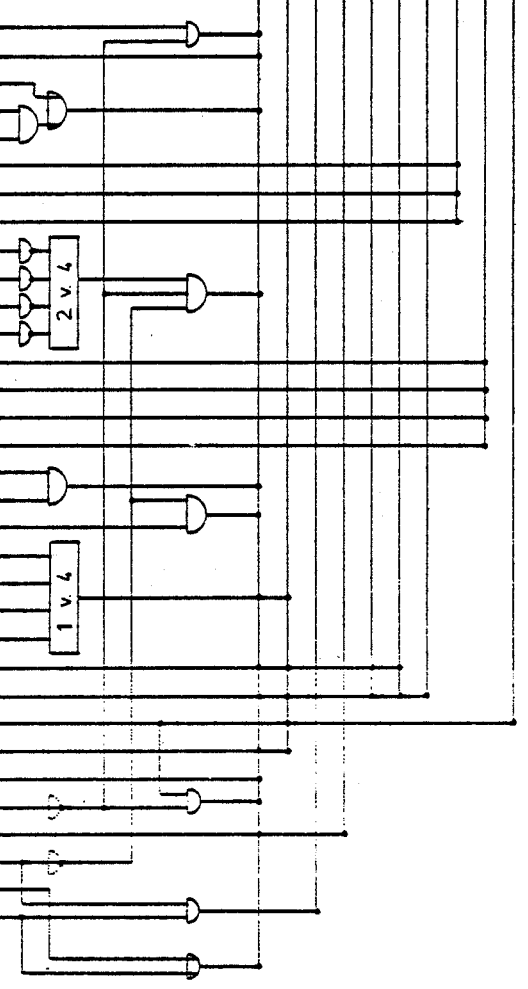
INITIATING EVENTS

- 01 LOSS OF PRIMARY HEAT SINK
- 02 LOSS OF OFF-SITE POWER
- 03 LOCA OUTSIDE CONTAINM
- 04 LOCA WITHIN CONTAINM
- 05 CONTROL ROD EJECTION
- 06 NEUTRON SENSOR OVERLAP FAILURE
- 07 H₂O SHORTAGE IN SCRAM-TANKS
- 08 HIGH REACTOR WATER LEVEL
- 09 CONDENSER DISTURBANCE
- 10 ABNORMAL SCRAM-TANK STATUS
- 11 INJECTION OF COLD WATER

SAFETY VARIABLES

NA	HIGH	NEUTRON FLUX -	NA
NL	LOW	POWER RANGE	NL
PR	HIGH	REACTOR PRESSURE	PR
PR	LOW	REACTOR PRESSURE	PR
PR	HIGH-RATE	REACTOR PRESSURE	PR
PR	HIGH-RATE	REACTOR PRESSURE	PR
FR	HIGH	REACTOR - LEVEL	FR
FR	LOW	REACTOR - LEVEL	FR
PS	HIGH	CONTAINM. PRESSURE	PS
PA	HIGH	STEAM - FLOW	PA
PB	HIGH	STEAM - FLOW	PB
PC	HIGH	STEAM - FLOW	PC
PD	HIGH	STEAM - FLOW	PD
FE	HIGH	FLOW HPCI	FE
VA	LOW	BUSBARS VOLTAGE	VA
VB	LOW	BUSBARS VOLTAGE	VB
UA	LOW	BUSBARS - VOLTAGE	UA
UB	LOW	BUSBARS - VOLTAGE	UB
UC	LOW	BUSBARS - VOLTAGE	UC
UD	LOW	BUSBARS - VOLTAGE	UD
SA	OPEN	POSITION OF	SA
SB	OPEN	STEAM - VALVES	SB
SC	OPEN	STEAM - VALVES	SC
SD	OPEN	STEAM - VALVES	SD
LA	LOW	SCRAM-TANK LEVEL	LA
LB	LOW	SCRAM-TANK LEVEL	LB
LC	LOW	SCRAM-TANK LEVEL	LC
YA	TRIGGERED	SCRAM-TANK SURVEILLANCE	YA
YB	TRIGGERED	SCRAM-TANK SURVEILLANCE	YB
YC	TRIGGERED	SCRAM-TANK SURVEILLANCE	YC
TK	HIGH	SUPPR.-POOL / TEMP	TK
LK	LOW	SUPPR.-POOL / LEVEL	LK

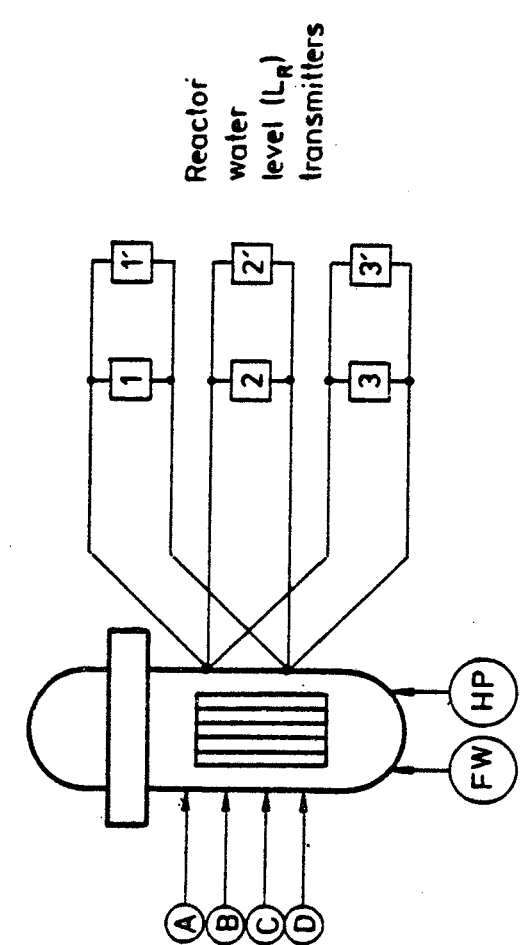
ACTIVATION CRITERIA



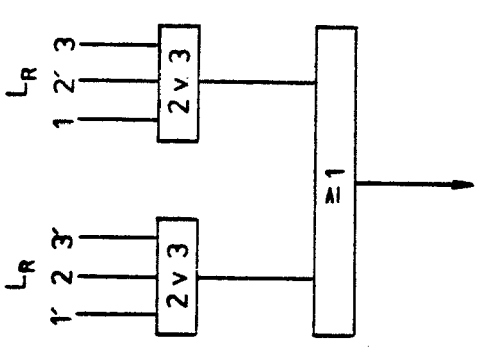
PROTECTIVE ACTIONS

- 01 REACTOR SCRAM
- 02 CONTAINMENT ISOLATION
- 03 CONTROL ROD INSERTION
- 04 OPENING OF SAFETY VALVES
- 05 SWITCH ON HPCI
- 06 RHRS (PHASE 1)
- 07 RHRS (PHASE 2)
- 08 CLOSURE OF SCRAM-VALVES
- 09 POWER SUPPLY-START EMERG. DIESEL
- 10 SWITCH OFF HPCI

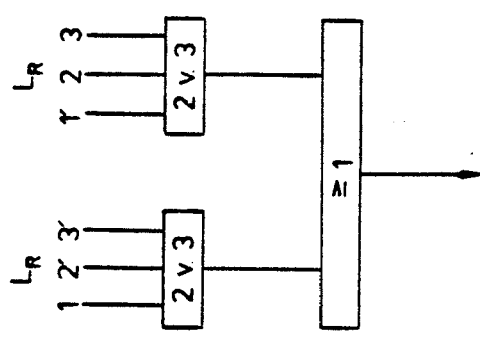
Fig. 2



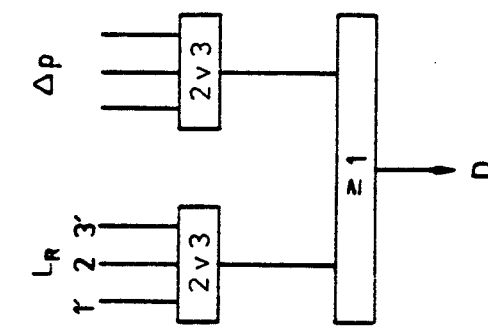
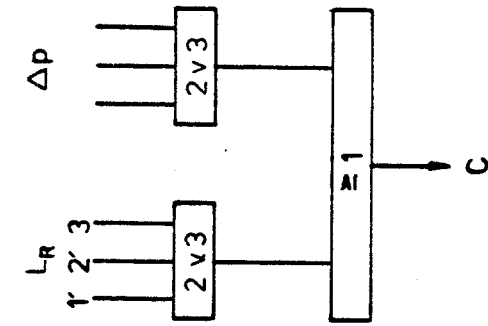
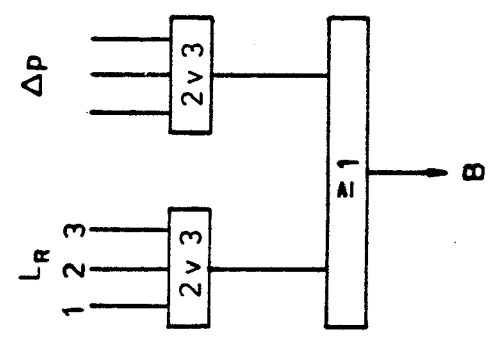
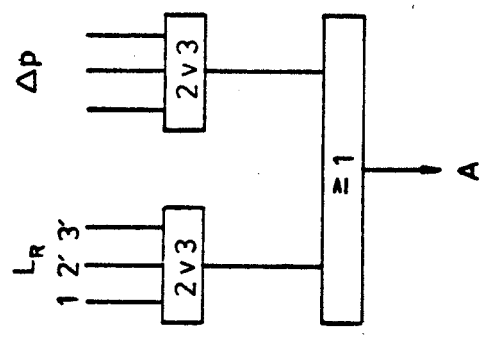
A,B,C,D... low pressure ECCS
 HP..... high pressure ECCS
 FW..... feedwater



Stop FW and HP (high L_R)



Start HP (low L_R)



Start low pressure emergency cooling (low L_R or high containment pressure)

Start low pressure emergency cooling (low L_R or high containment pressure)

Fig. 3

R. Haubert, R. Stokke

MONITORING READINESS OF SAFETY RELEVANT DEVICES IN NUCLEAR
POWER PLANTS BY MEANS OF CRT-COLOUR DISPLAYS

MONITORING READINESS OF SAFETY RELEVANT DEVICES IN NUCLEAR
POWER PLANTS BY MEANS OF CRT-COLOUR DISPLAYS

by

R. Haubert, SGAE, Austria

R. Stokke, OECD Halden Reactor Project, Norway

ABSTRACT

The development of an information system for monitoring readiness of safety relevant devices is encouraged by the requirements of KTA-rule 3501 (DIN 25434), which states in section 4.9.1.1. "A display shall be provided for giving a survey of the condition of the components of the reactor protection system and the active engineered safeguards including their energy and auxiliary media supplies".

In the first stage of the development which was reported at the Enlarged Halden Programme Group Meeting in Loen, Norway, 5th - 9th June, 1978, only the components of parts of a BWR-protection system were considered and no display was provided. This paper outlines the next step in the development which comprises implementation of the active engineered safeguards into the system and development of a display system based on a colour CRT-screen.

A prototype of this computer-based system for monitoring of protection systems has been established, and it is planned to demonstrate this prototype system using the computer equipment at GRS, Garching in connection with the IAEA/NPPCI specialist meeting.

Paper to be presented at the Specialists' Meeting on "Procedures and Systems for Assisting an Operator during Normal and Anomalous Nuclear Power Plant Operation Situations"

München, December 5th-7th, 1979

1. INTRODUCTION

In a previous paper with the title "Reactor Safety System Surveillance by Computer" (1) the emphasis was placed on the technical solution of the problem of transforming rules concerning repair strategy of a Reactor Safety System into computer language.

In the present paper the integration of the computerized part of the operational manual into the overall functional requirements of modern control room design is treated. Therefore, emphasis has been placed on the development of an adequate operator/process interface.

The relevance of the development work described below is confirmed by some requirements of KTA rule 3501 (2). One section states: "A display shall be provided for giving a survey of the condition of the components of the reactor protection system and the active engineered safeguards including their energy and auxiliary media supplies". The keywords in this connection are "condition of components" and "display".

In the design of reactor safety systems, i.e. the reactor protection system and the active and passive engineered safeguards - the designer is faced with a conflict between different goals:

- minimization of average cost for the operation of the plant, i.e. maximization of plant availability by avoiding unnecessary shutdowns or
- minimization of immediate risk.

Concerning the structural design of reactor safety systems the conflict between these two goals has led to the principles of majority voting, redundancy and diversity according to the relevant statements in KTA 3501.

Indeed, concerning operation of the reactor safety system in the event of faults the safety aspects is reflected exclusively in the following statement:

"Operation of the reactor protection system in the event of faults:
During repairs in the reactor protection system the reactor shall be immediately brought into a safe condition if, as a result of a random failure including secondary failures, the remaining part of the safety system is no longer able to fulfill its safety functions."

In an additional note this statement is explained by an example:

"This is the case, e.g., in the event of a failure of the controls in the redundancy group 1 and the repair of a mechanical component in the redundancy group 2 and a failure in the redundancy group 3 due to an incident in a 4 x 50% emergency core cooling system.

The transfer into a safe condition can be brought about, e.g. by immediate repair or controlled shut-down of the nuclear power plant. Preference shall be given to an immediate repair, if the repair can be completed faster than the controlled shut-down".

The preceding example is a typical application of the well known "Single Failure Criterion". This criterion states: "A safety system shall function even then, when - in the case of an incident - a single component or a subsystem of the safety system is in the failed state".

This is a qualitative criterion and includes only two extreme possibilities:

- immediate shutdown of the plant and
- arbitrary repair time

Considering the large amount of possible failure/repair combinations within the reactor safety system, the application of the single failure criterion of a plant is rather unsatisfying. It is left to the human operator to decide which repair times are appropriate in order to comply with the two different goals of safety and availability. In contrast to the situation of the designer of the reactor safety system, the situation can be rather stressing for the operator because he often has to decide very quickly and under pressure. Because of possible mental overloading of the operator, he can become a weak, i.e. unreliable component in the total system.

The determination of allowable repair times is only possible with quantitative methods, i.e. reliability assessments. For practical application of the results of these reliability assessments the electronic components of the reactor protection system can be arranged in tables relating them to the appropriate active engineered safeguards to be actuated. Such tables, called "Tables of Second Failure", have been provided for the first Austrian power plant by the reactor vendor, KWU.

Although these "Tables of Second Failure" represent a major progress

compared to the "Single Failure Criterion" in estimation of the allowable repair times, they are laborious to manage during plant operation. This becomes obvious when looking at the structure of the tables as will be illustrated in the next chapter. Moreover, from the "Tables of Second Failure" the state and the readiness of the safety systems do not become transparent enough for the operator.

This situation was the motive for the development of a prototype of a computer aided information system for the operator. This prototype system is based on the "Tables of Second Failure" for the most important protective actions of the reactor safety system (3).

Referring to KTA we conclude that the development of this prototype system is in agreement with the requirements of this standard. The "condition" of the *components* is represented by the binary states

- working (successful) state
- failed state.

The "condition" of a redundant *system* like the reactor safety system is represented by the accepted time of readiness. In the case a system degradation, because of faults, is observed (either by testing or selfmonitoring), the *repair* time expresses the accepted time of readiness. These "conditions" then will be brought to the operator's notice by means of colour CRT-displays.

2. THE "TABLES OF SECOND FAILURE"

2.1 Structure of a Reactor Safety System

Fig. 1 shows the principal structure of a reactor safety system. The protective function is the basic element. One or more protective functions can initiate a protective action (physical diversity).

Originally only the reactor protection system comprising section 1 and 2 (Fig. 1) was represented in the "Tables of Second Failures". Section 3, the active engineered safeguards ("actuated devices") including power supply was missing.

In our recent development work these components have been considered according to the requirements of KTA 3501.

2.2 The Derivation of "Tables of Second Failure" from Fault Tree Analysis

As an illustrative example for derivation of "Tables of Second Failure" from fault tree analysis, protective action No. 6 "Start Low Pressure Cooling Injection System" is chosen, which also serves as our demonstration example. (See chapter 4.2) This protective action consists of 4 x 50% subsystems.

Fig. 2 shows the fault tree of subsystem B (safety area 2) of the "Low Pressure Cooling Injection System". The transformation into the corresponding "Tables of Second Failure" is shown in Fig. 3. The engineered safeguards and power supply - abbreviated in Fig. 2 by "mech. c. power" - are indicated in the "Table of Second Failure" of Fig. 3 in detail.

According to the rules of the operational manual a subsystem is considered to be lost if one row of the corresponding "Table of Second Failure" is lost. Two of the 4 x 50% subsystems must function. If this is not the case, shutdown is required. The rules provided in the operational manual have been translated into decision table for evaluation by a computer.

3. THE MAN-PROCESS INTERFACE

As already mentioned the "Tables of Second Failure" are laborious to handle manually because of the variety of possible failure combinations and counteractions. Hence it can turn out that this job can be a risk of human error influencing the overall performance of the plant:

The reactor operations crew has to:

- (1) locate and identify the faults after detection
- (2) keep record of the time necessary for these actions mentioned above
- (3) locate the failed component in the "Table of Second Failure"
- (4) evaluate the associated failure combinations
- (5) find the right counteraction (repair time) to be taken
- (6) supervise the repair times

It seems to be advantageous to automatize some of these actions, especially the use of the "Tables of Second Failure" and the information processing between the operator and the process to be controlled, i.e. the status of the reactor safety system. This has been done by use of a computer. Action (1) cannot be automatized totally. In many cases even selfmonitoring failures in the reactor protection system have to be identified from a collective message, and

moreover, failures in active engineered safeguards must be detected by testing.

In our present version there is no option for on-line coupling between the computer and the reactor safety system, and action (2) is not performed automatically. Fig. 4 shows schematically the configuration process - computer - man. The operator gets the alphanumeric symbol of the failed or repaired component(s) and puts it into the computer via the keyboard. Action (3) - (6) are performed by the computer.

The result of the computer-evaluation is presented on a colour display which is the output device. Designing the display was done always with the human operator primarily in mind following the principle: "The display system design is the quantum jump in the operator's interface".

Direct operator interaction may easily follow, if deemed desirable, once the display system has been made effective by applying the display design methodology outlined in Fig. 5.

4. THE COLOUR DISPLAY SYSTEM

4.1 Purpose and Function of the Display Set

The purpose of the display set which has been developed is to give the operator the optimum overview of the repair state of these safety systems. To allow the operator to make the necessary observations and decisions quickly and intellegently, a display hierarchy has been chosen as the appropriate tool as shown in Fig. 6. This hierarchy comprises two levels of presentation:

- monitoring level
- diagnostic level

At the "monitoring level" the present version of our system has two pictures:

- a representational overview picture showing the structure of the four safety systems
- a time table showing the (running) time left for repair before shut-down of the reactor has to be performed.

At the "monitoring level" the operator can recognize:

- the permissible repair interval expressed by colours as follows:

red: immediate shutdown
lilac: 10 hours repair interval
yellow: 100 " " "

- the designation of the subsystem which has to be repaired (e.g. safety area 1A)
- a pointer to the appropriate detailed picture on the diagnostic level

Hence, on the basis of this overview picture on the screen, the operator can see which protective action he has to study in more detail. By pressing the button on the keyboard whose number is displayed on the overview picture close to protective action in question, he automatically is led to that part of the safety system where the fault has occurred.

According to the requirements of KTA 3501 the diagnostic level should include three kinds of pictures showing:

- D1: protection system with its subunits including initiation level, logic unit and control level
- D2: energy and auxiliary media supplies
- D3: details of mechanical components (e.g. motor section of emergency coolant pumps) which are of interest for the operator

At the diagnostic level it is difficult to decide how far to go into detail. At the present stage of model development only D1 is represented.

4.2 Illustrative Example

As a representative example for the application of this display technique the Emergency Core Cooling Systems have been chosen as they are represented in our model (Fig. 7). The system include:

- Relief and Safety Valves
- Low Pressure Coolant Injection System (LPCI-System) consisting of 4 x 50% engineered safeguard subsystems
- Core Spray System

Consider the simplified "Low Pressure Cooling Injection System" (LPCIS) with its 4 x 50% subsystems (respectively safety areas). In the emergency case this system acts after operation through 600 seconds as Residual Heat Removal System (RHRS). Major active components of the system are the four emergency

cooling pumps and the four heat exchangers. For this example the following state of the system is supposed:

- subsystem C (safety area 3) is in repair (fault in the control level of the reactor protection system is being eliminated)
- two of the six alarm units of the protection function activated by "water level very low" have failed; this means in this case: Subsystem A (safety area 1) cannot be activated by that physical diversity criterion.

According to the rules connected with the "Table of Second Failure" for this protective action, the permissible repair time is 10 hours. The overview picture will show the following situation: The 4 x 50% subsystems are symbolized by one line and the four emergency coolant pumps by one pump. According to the 10 hours repair state they appear in lilac colour. The unavailable subsystems A, C (safety region 1, 3) are indicated in red besides the pump symbol. The

other systems which are expected to be in non-failed state, are all displayed in green colour.

A number (6.1) in cyan colour is the number of the button the operator has to press to get the proper picture on the diagnostic level.

4.3 The Structure of the Software (7), (8), (9)

4.3.1 *General Discussion*

At the Halden Project development work within the fields of control room design and applications of computers in operator communication systems has been an ongoing activity during the last ten years. It has turned out that computer controlled colour displays are very useful tools for presentation of correct and comprehensive information of the plant status for the operators.

At the Halden Project general programme packages have been developed for generation, display and updating of colour diagrammes. It was therefore natural to adapt this ongoing research work to the development of the prototype system for surveillance of reactor safety system.

This adaptation led to a processing system including general software modules for the display system, and specific modules for the models of reactor safety systems. Even though these two sets of software modules were developed independently of each other, the present version can be looked upon as an

integrated system. This integrated system can on the other side be divided into system generating modules and active analysis modules.

4.3.2 *Generating Modules*

The generating software modules comprise routines to generate the model of the reactor safety system in terms of "Tables of Second Failures", decision tables and status tables. This model is the framework of the whole analysis part including tables to store the results of the analysis (status of the reactor safety system). Other generating modules exist for the generation of the mimic diagrammes which present the status of the reactor safety system to the operator. This picture-editor creates the framework of these diagrammes in the form of tables for colours and conditions for the different strings in a picture.

The model generator and the picture-editor produce both a library containing tables of the reactor safety system and the picture tables, respectively. The pictures are at this stage prepared to fetch information about the status of the reactor safety system.

4.3.3 *Analysis Modules*

The other software modules perform the analysis and status updating task, including some service routines. These modules can briefly be divided into the following groups:

- Keyboard service modules
- Updating and analysis modules for the reactor safety system model
- Picture display and updating modules

The first and the last group are general software packages adapted to the special needs of the programmes in the second group. Even if the analysis modules are special, they are general in the sense that any model of a reactor safety system (within some limitations) can be analysed by them. The different models can be generated by the model generator.

The information flow within the total system is illustrated in Fig. 8. The keyboard handling service routines treat input from the keyboard(s) used in the actual installation. Information from the keyboard(s) are used both for updating the status tables of the reactor safety system model and for the display system. The status tables of the reactor safety system model are updated when the operator types in a failed or repaired component, and the display system

will react upon requests from the operator via the keyboard, to display a new picture on the colour screen.

When the status of the reactor safety system is changed, the analysis modules are automatically started. First one routine will update a component status table, then the failure combination analysis module will analyse the status of the reactor safety system, and the results from this routine are transferred to the message analysis modules which in turn will prepare correct messages (counteraction and "verbal" status report) to the appropriate picture. Only the message valid for the currently displayed picture is shown on the screen. The repair time supervision module initiate simultaneously a count down sequence for the actual protective action, and will give a plant shutdown message if no counteraction is performed when the repair time has elapsed.

The display modules fetch information from the keyboard service modules and display the requested picture on the display screen. The status of the reactor safety system model is fetched from the status tables and are combined with the predefined colour/condition-tables in the picture such that the correct string with the correct colour appear on the screen. In the message area in the lower part of the screen, there will appear a corresponding counteraction message prepared by the message analysis modules.

All modules outlined in this section run in so-called "real-time" mode according to the requirement that the repair time is a critical parameter.

5. CONCLUSION

In this paper a possible solution of the problem "Monitoring readiness of the engineered safety systems" has been presented.

The further development work should include:

- on-line transmission of the detected failed state of a component into the computer as far as it is possible,
- computerized inspection of engineered safety systems during periodic test-start ups as described in (6)

By such improvements it is believed that the presented system for surveillance of the reactor safety system will provide the operator with a powerful tool in his supervision of the plant, thereby increasing both plant safety and plant availability.

LIST OF REFERENCES:

1. R. Haubert et al: Reactor Safety System Surveillance by Computer. Paper presented at the Enlarged Halden Programme Group Meeting, Loen, Norway, 5th - 9th June, 1978.
2. KTA 3501: Reaktorschutzsystem und Überwachung von Sicherheitseinrichtungen. (English translation: Reactor Protection System and Monitoring of Engineered Safeguards).
3. A. Nedelik, H. Roggenbauer: A computerized system for evaluation of the status of a protection system. Paper to be presented at the IAEA/NPPCI Specialist Meeting, 5th - 7th December, 1979, München.
4. M.D.Danchak: The Man-Process Interface using Computer Generated CRT Displays. Instrumentation in the power industry, Vol. 20, 1977.
5. J.Ø.Hol, G. Øhra and K. Netland (OECD Halden Reactor Project): Design of pictures and use of colours and symbols for a CRT based supervision system. Paper presented at the EHPGM, Loen, Norway, 5th-9th June, 1978.
6. A general approach to computerized inspection of engineered safety systems by W. Hawickhorst. (Laboratorium für Reaktorregelung und Anlagensicherung, Garching).
7. G. Isaksson, R. Stokke: RGB Programme Documentation. HIR-94, 1979 (OECD Halden Reactor Project). Private Communication.
8. R. Stokke: RGB Users Manual. PC Note 2040, 1979 (OECD Halden Reactor Project). Private Communication.
9. B. Fagerstrøm, R. Stokke, B. Blomsnes, J. Augustin, T. Olli: Present Status and Planned Use of the Computer Control Experimental Facility at the Halden Project. Paper presented at the EHPGM, Loen, Norway, 5th-9th June, 1978.

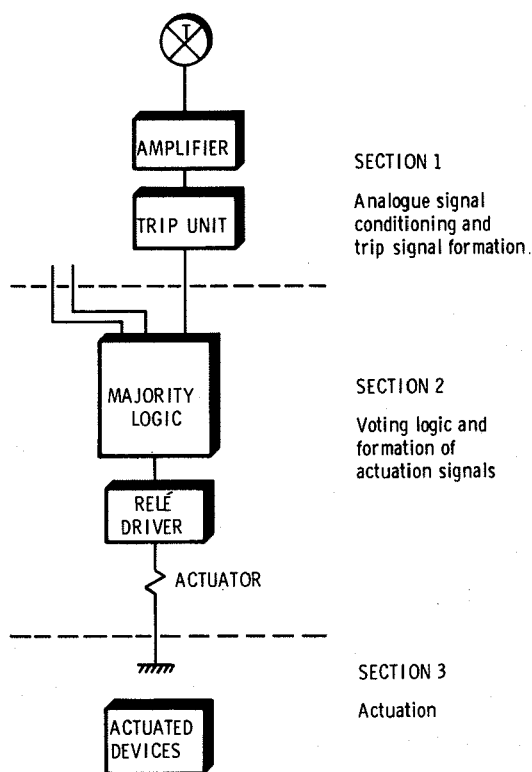


FIG. 1. PROTECTIVE FUNCTION BLOCK DIAGRAM

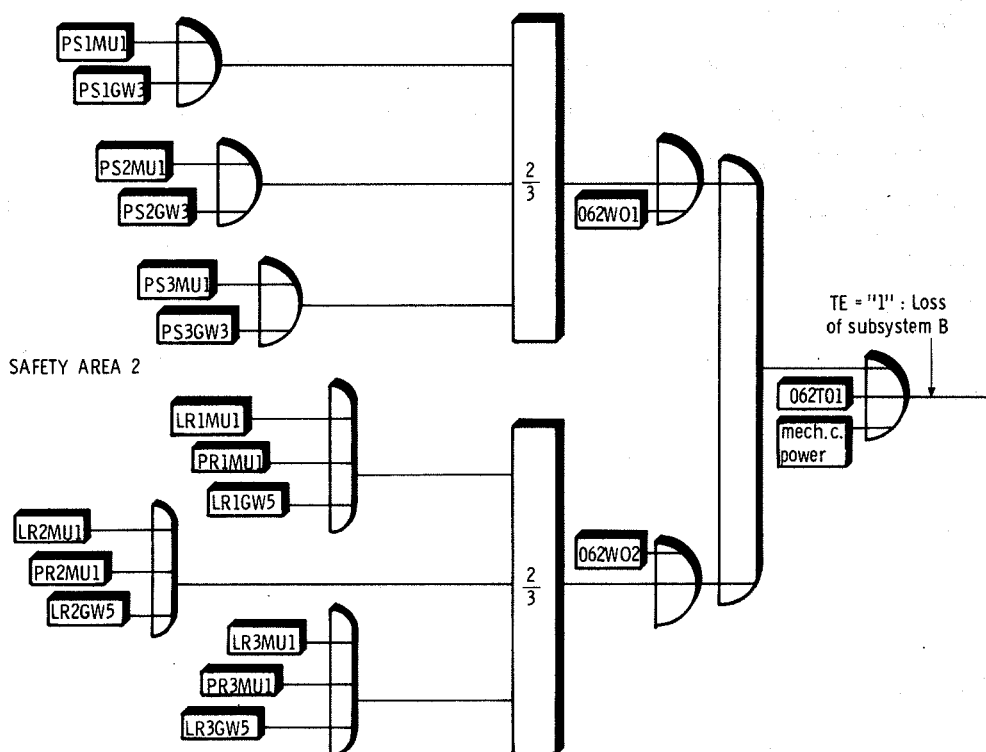


FIG. 2. FAULT TREE OF "LOW PRESSURE COOLING INJECTION SYSTEM", SUBSYSTEM B

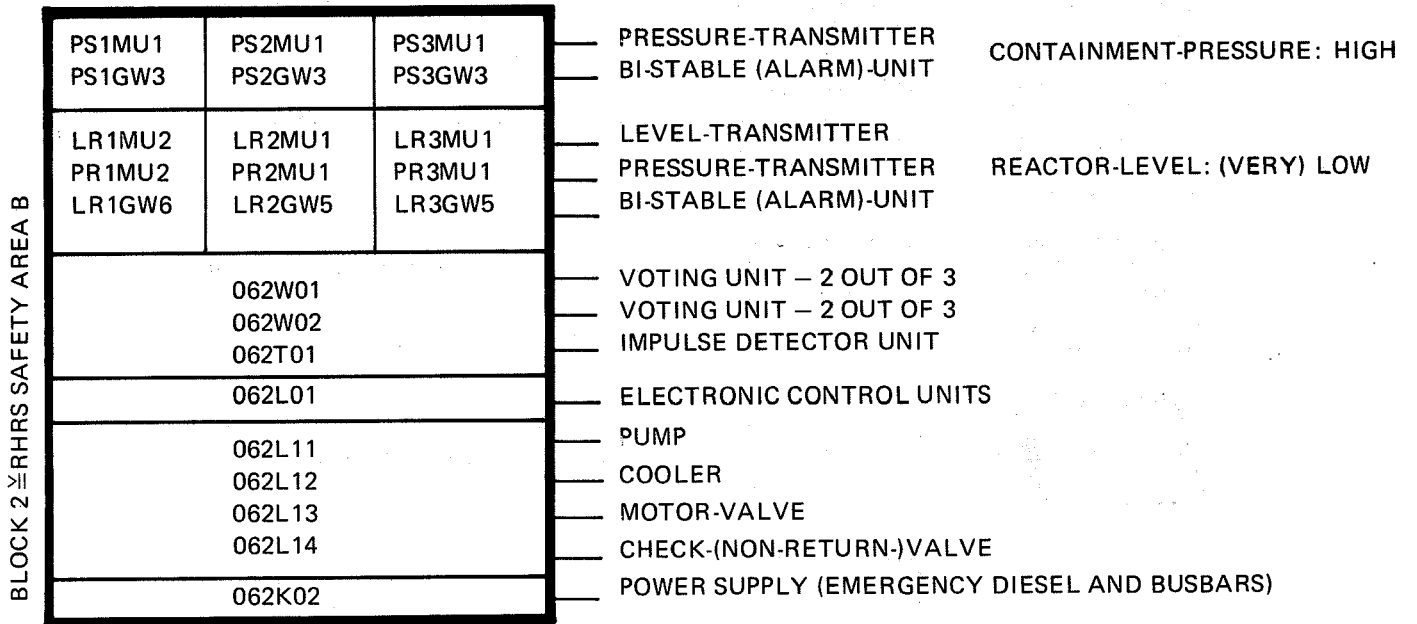


FIGURE 3. TSF OF "LOW PRESSURE COOLING INJECTION SYSTEM", SUB. B

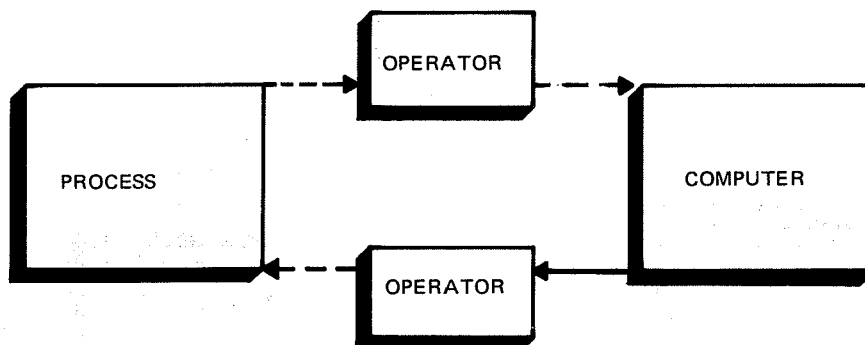


FIGURE 4. OFF-LINE COMPUTATION (DASHED LINES INDICATE HUMAN DELAY OR HANDLING)

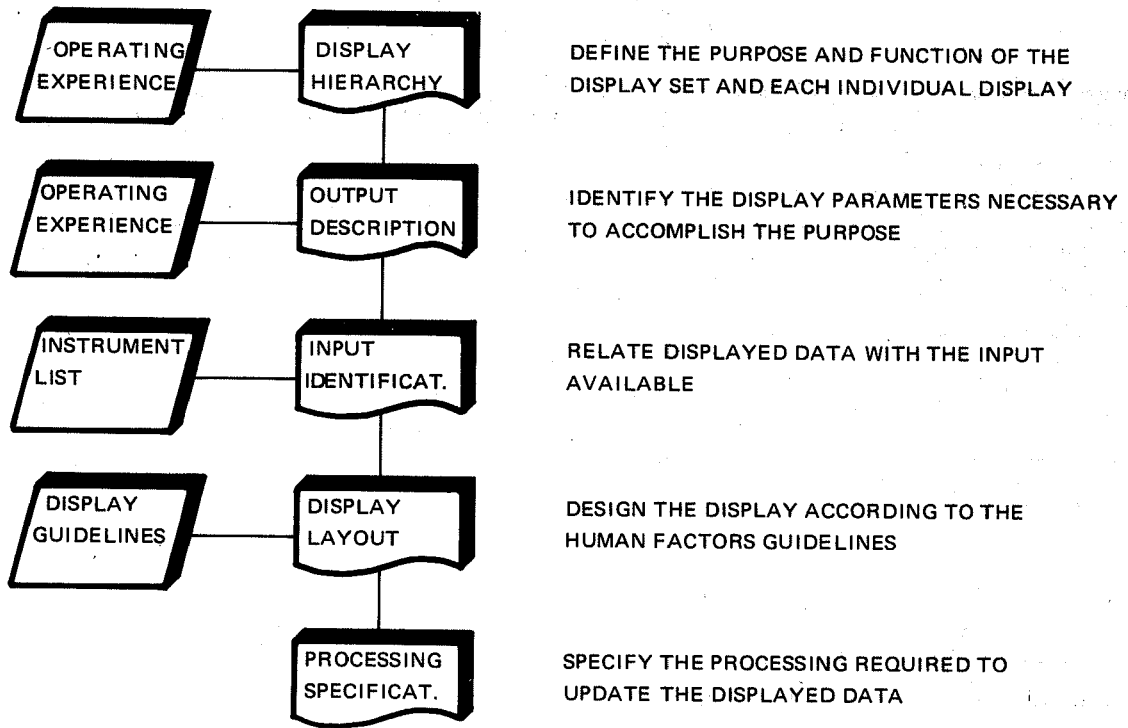


FIGURE 5. DISPLAY DESIGN METHODOLOGY

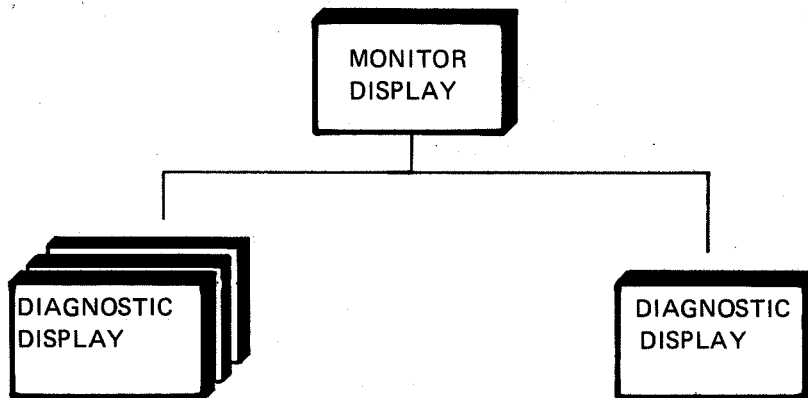


FIGURE 6. OPERATOR FUNCTION/DISPLAY HIERARCHY

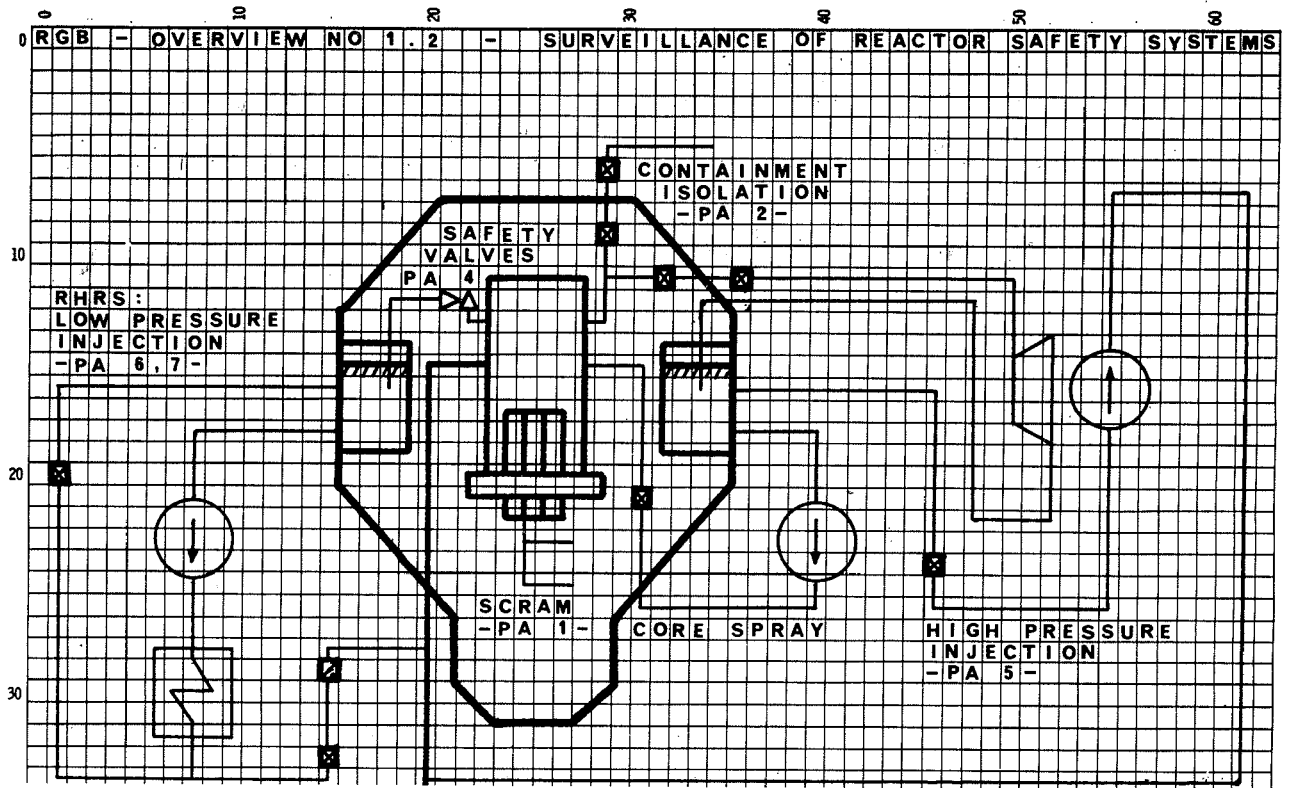


FIG. 7. EMERGENCY COOLING SYSTEMS

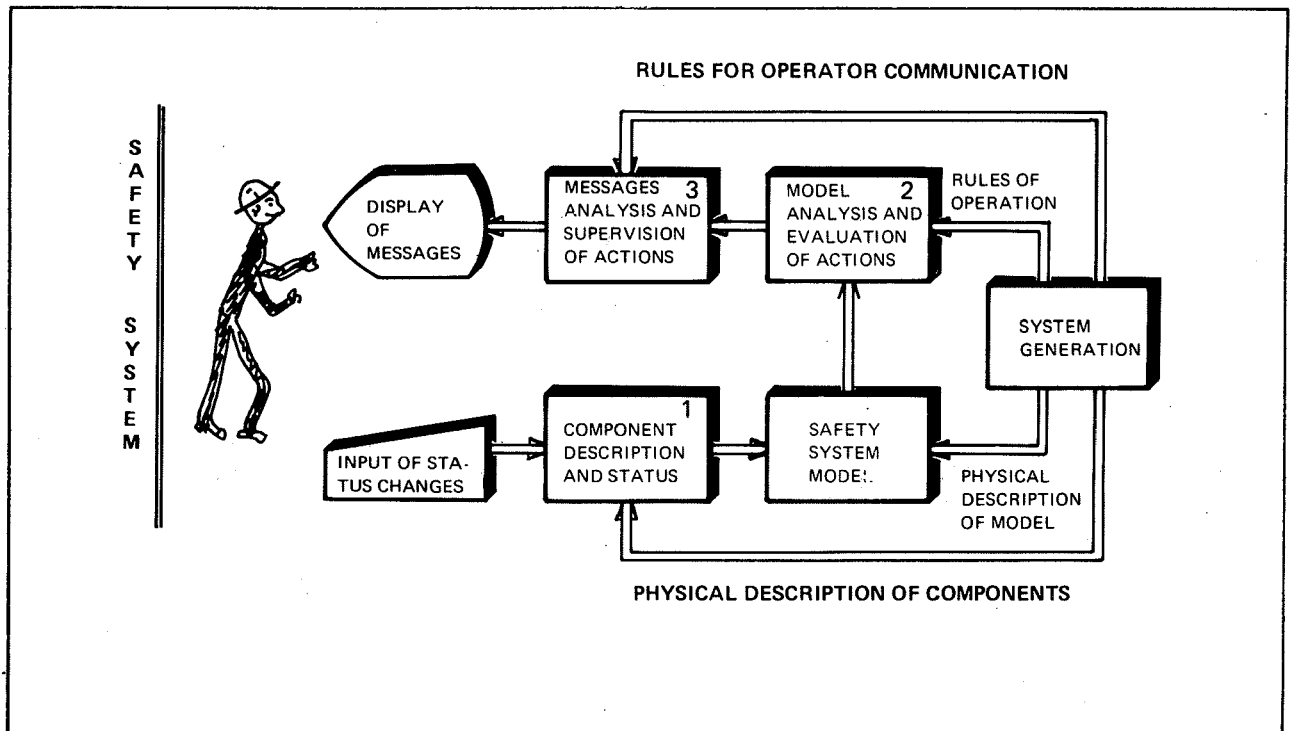


FIG. 8. INFORMATION FLOW IN THE PROTOTYPE SYSTEM FOR SURVEILLANCE OF THE REACTOR SAFETY SYSTEM

P. Cormault

SURVEILLANCE SYSTEMS UNDER DEVELOPMENT AT ELECTRICITE DE
FRANCE

INTERNATIONAL ATOMIC ENERGY AGENCY
(I.A.E.A.)

N P P C I Specialists' Meeting on
PROCEDURES AND SYSTEMS FOR ASSISTING
AN OPERATOR DURING NORMAL AND ANOMALOUS
NUCLEAR POWER PLANT OPERATIONS SITUATIONS.

5-7 december 1979 MÜNICH (R.F.A.)

SURVEILLANCE SYSTEMS UNDER DEVELOPMENT AT
ELECTRICITE DE FRANCE
(Systèmes de surveillance de développements à Electricité de France)

P. CORMAULT
ELECTRICITE DE FRANCE
DIRECTION DES ETUDES ET RECHERCHES
Service Ensembles de Production
6, Quai Watier
Boîte Postale n° 24
78400 CHATOU (France)

ABSTRACT

The paper is providing an overview of some projects recently developed or under development at ELECTRICITE DE FRANCE in the field of surveillance of particular plant processes or subsystems.

The first system described is devoted to the on line surveillance of protection sensors response time. Experience gained both in laboratory experiments and in plant testing led to the implementation of a microprocessor based on line monitor.

The second surveillance system described is a fast transient monitor designed for turbine and generator surveillance and disturbance analysis.

SURVEILLANCE SYSTEMS UNDER
DEVELOPMENT AT ELECTRICITE DE FRANCE

CONTENTS

1. Introduction
2. On-line evaluation of sensors response time
3. Fast transients monitors for generator and turbine surveillance.
 - 3.1. Transient recording system for generator surveillance.
 - 3.2. Fast transient monitor for turbines.
4. CONCLUSION

SURVEILLANCE SYSTEMS UNDER
DEVELOPMENT AT ELECTRICITE DE FRANCE

1. INTRODUCTION

Since the beginning of the important program of erection of nuclear power plant carried out by ELECTRICITE DE FRANCE, much attention has been paid to the development of data processing and data display systems intended to enhance operator's aid and guidance. The computer system for data processing and display in the PWR 1300 MW power stations to be started in 1982 was described previously [1]. This paper will present some complementary systems presently under development at the Research and Development Center of E.D.F., at CHATOU (FRANCE).

The first system described is devoted to the on line surveillance of protection sensors response time.

The two other ones are fast transient monitors designed for generator and turbine surveillance and disturbance analysis..

2. ON-LINE EVALUATION OF SENSORS RESPONSE TIME

Several surveillance methods were developed in order to evaluate, on site and without dismounting, the response time sensors used in the protection system of PWR plants. This is part of a joint program developed by COMMISSARIAT A L'ENERGIE ATOMIQUE, E.D.F., FRAMATOME and WESTINGHOUSE (U.S.A.). Basic principles and experimental investigations have been described elsewhere [2]. Two types of surveillance methods were investigated. The first one is an active method to study thermal response of the sensor to an electrical excitation. The second one is a passive method to perform a noise analysis of the sensor itself, in normal operating conditions.

Active method : Loop Current Step response.

The active test unit, (figure 1), generates a step in the current flowing through the resistance sensor under test. This increase of current causes a self-heating process and a transient response transmitted to the data processing unit.

It can be shown by using a thermal model of the sensor that the transfer function associated with such a process of internal heating by an electric current is of the form :

$$H_{in}(p) = \frac{\prod_i (p - z_j)}{\prod_i (p - \alpha_i)}$$

While the desired transfer function associated with a change of the fluid temperature is :

$$H_{ext}(p) = A_i \prod_i \frac{1}{p - \alpha_i}$$

The measured transient :

$$R_{in}(t) = \sum_i B_{ie} e^{-\alpha_i t}$$

is analysed in order to determine estimates of poles α_i .

The knowledge of their values is sufficient to deduce the transfer function $H_{ext}(p)$, and thus the step response associated with it (figure 2). The response time of the sensor is taken as the time for which step response is 63,2 % of its final value.

Passive method : sensor noise analysis

The fluctuations of the signal delivered by the sensor are the noise of the physical process filtered by sensor. Assuming that the process noise is stationary and white, it turns to be that the spectrum of the sensor noise signal represents the modulus of the sensor transfer function $H(p)$.

Two methods have been compared and are leading to similar results : in the frequency domain, the power spectrum computed by a Fast Fourier Transform is approximated by a simple transfer function, and the response time can then be deduced.

In the time domain, an Auto-Regressive model of the noise is computed, using the Yule-walker equation and the autocorrelation function of the measured signal. The step response of the sensor is deduced by applying a step input to the model obtained.

Implementation

The above described investigations were performed on an HP 9845 computer connected to a NICOLET SCIENTIFIC spectrum analyser. A prototype system based on a microprocessor approach is presently developed and final choice between a dedicated system (figure 1), or a centralized approach making use of the computer system described in [1] is not yet decided.

3. FAST TRANSIENTS MONITORS FOR GENERATOR AND TURBINE SURVEILLANCE.

Instrumentation systems installed in nuclear power stations have to fulfil three functions :

- (i) to provide the operators with the data necessary for routine operation of the plant.
- (ii) to detect any significant change in equipment status, and help to formulate a diagnostic.
- (iii) to make possible the analysis of any fast transient giving rise to abnormal or accidental conditions.

Function (i) is fulfilled by the data processing and display system described in [1].

Functions (ii) and (iii) will be implemented in two dedicated systems designed for surveillance of turbines and generators of the 900 MW units and 1300 MW units to be built and operated by E.D.F.

Future similar developments could lead to the surveillance of the primary circuit or other subsystems.

3.1. Transient recording system for generator surveillance

In 1976, new needs were expressed for generators surveillance, due to the increase of power of the new machines to be operated.

The demand was for a system performing an off-line analysis of the electrical disturbances occurring during turbogenerators operation.

The general requirements were the following :

- analog and logic inputs.
- memory of a period of time preceding the triggering of the system.
- external and internal triggering.
- good response time.
- direct reading of records
- good accuracy
- low price.

A two years development study led to a modular system to be now installed in any PWR power station built by E.D.F.

Each module receives 8 analog inputs (currents and voltages) and 9 logic inputs (circuit-breakers positions, stator or rotor earth indication, maximum voltages or currents occurrences, etc.).

The frequency response is better than 300 Hz, the accuracy better than 3 %, and the time resolution better than 1 ms.

The storage time before triggering is 250 ms and the storage time after triggering variable from 2 to 14 s.

Triggering is manual or automatic, by selection of any combination of logic inputs.

Up to 4 modules can be operated in slave mode under the control of a master unit.

Records are displayed on paper rolls by thermal graphic recorders. Thus, the reading speed in the memory system is 100 samples per second, which is to be compared with the writing speed in the memory, equal to 2000 samples per second. For this reason, the system is operated slightly off-line, the total retrieval time for a 14 s record not exceeding 1 minute.

The system is designed for high reliability, with no mechanical part (except in the strip chart recorder).

The 800 K system memory makes use of 16 K RAM LSI circuits.

Two prototypes have sustained without any failure a six months testing period in a conventional thermal power plant.

Industrial operation will begin in 1980 ; the system, called O.P.G.14, will be built under patent by CERME, Chaville, (France).

3.2. Fast transient monitor for turbines

This system is intended for the description of the evolution with time of a certain number of parameters, just before and just after the occurrence of any abnormal condition in the operation of the turbine.

The capacity of the system is as follows :

- 40 analog inputs scanned each 40 ms
- 20 analog inputs scanned each 0,5 s
- 60 logic inputs scanned each 10 ms.

The triggering is external or internal. If triggered at time t_0 , the system will memorize permanently all the data between $t_0 - 60$ s and $t_0 + 80$ s. If any other triggering action occurs, the system must be able to execute the same process during 3 complete cycles.

The operator is provided with interactive communication system allowing him to select and display any sequence of data selected among the 100 inputs and the ($t_0 - 60$ s, $t_0 + 80$ s) time interval.

Two different prototype systems are presently under construction, giving thus the possibility to evaluate competing technologies.

One project (figure 3) makes use of conventional solutions, with isolation amplifiers for analog inputs, opto-electronic couplers for logic inputs, 32 K RAM memories and Zilog Z 80 microprocessor as a central unit.

The display makes use of a HP2648A graphic terminal and a HP7245A plotter.

The second project (figure 4) is intended to test more advanced technologies. Isolation of analog inputs is done optically, data storage makes use of magnetic bubbles memories, with a capacity of 1152 K bytes.

The display is a digital graphic and static recorder (ES 1000 of Gould-Allco).

The time schedule of the project is as follows :

March 1980 : delivery of the 2 prototypes.

April-May-June 1980 : Lab' tests.

July to december 1980 : Testing period in power plants.

June 1980 : industrial operation in 1300 MW
PWR power plants.

4. CONCLUSION

Three surveillance systems presently under development at ELECTRICITE DE FRANCE have been described. They are planned to be in industrial operation in 1981, and to present comprehensive information to the operator about the status of a limited number of subsystems within the plant.

Similar approach is believe to be meaningful for others subsystems, and should be investigated during next years.

R E F E R E N C E S

- [1] C. HERMANT - S. GUESNIER : "Data processing and data display in ELECTRICITE DE FRANCE PWR 1300 MW nuclear power plants".

Specialists' meeting on procedures and systems for assisting an operator during normal and anomalous nuclear power plant operation situations.

Munich, december 5-7, 1979.

- [2] G. ZWINGELSTEIN, P. CORMAULT, J.P. JACQUOT, J.C. AUTHIER, B. GIRET, R. GOPAL : "Comparative study of on-line response time measurement methods for platinum resistance thermometer".

VIII IMEKO CONGRESS, MOSCOW, may 1979

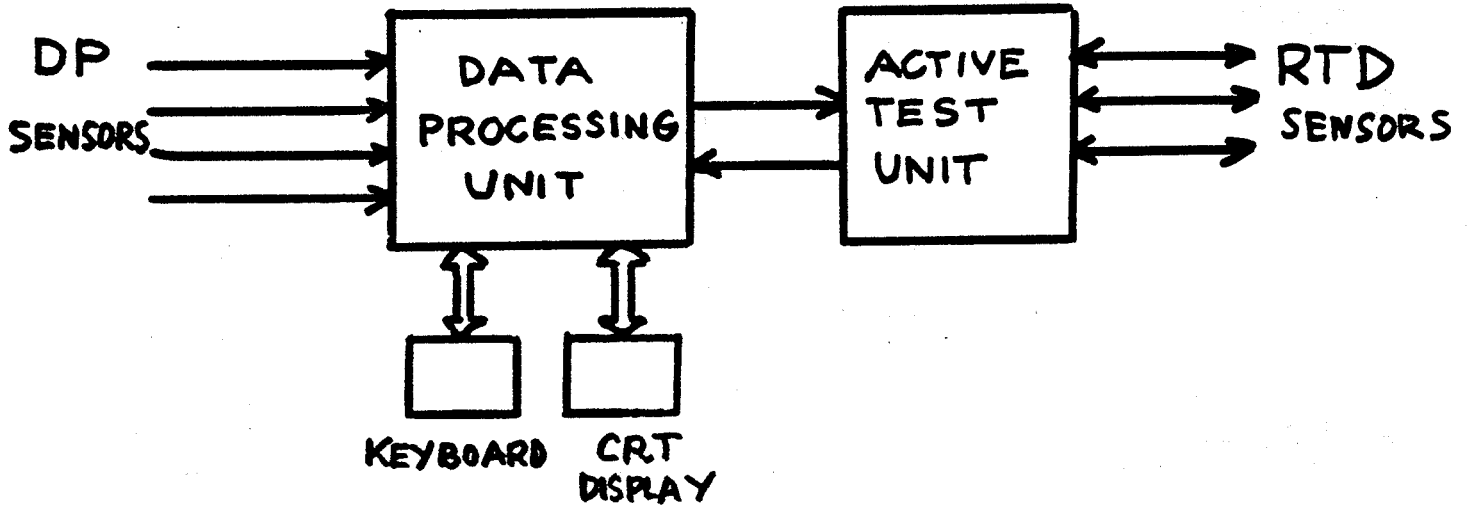


FIGURE 1 : Surveillance of sensors. General lay-out of equipment.

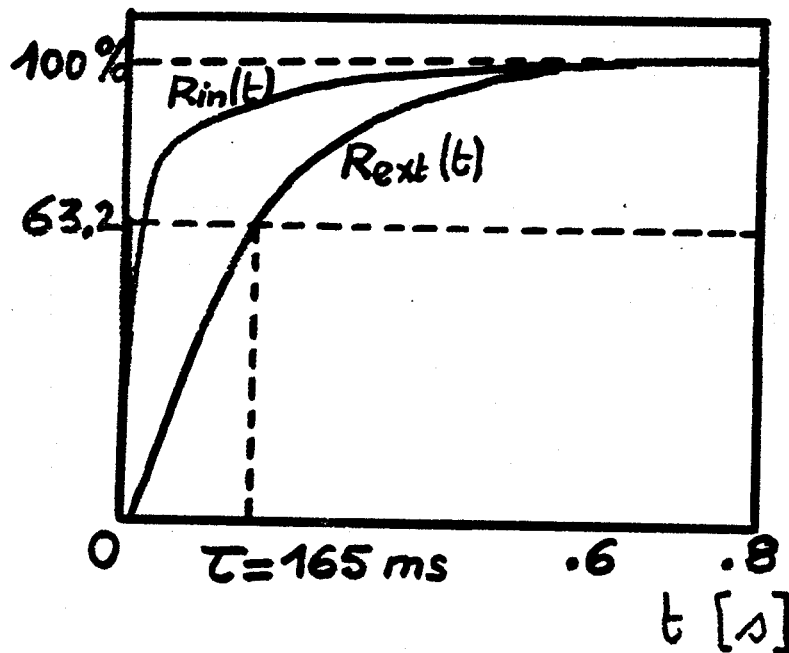


FIGURE 2 : Measured and computed step responses of a RTD sensor

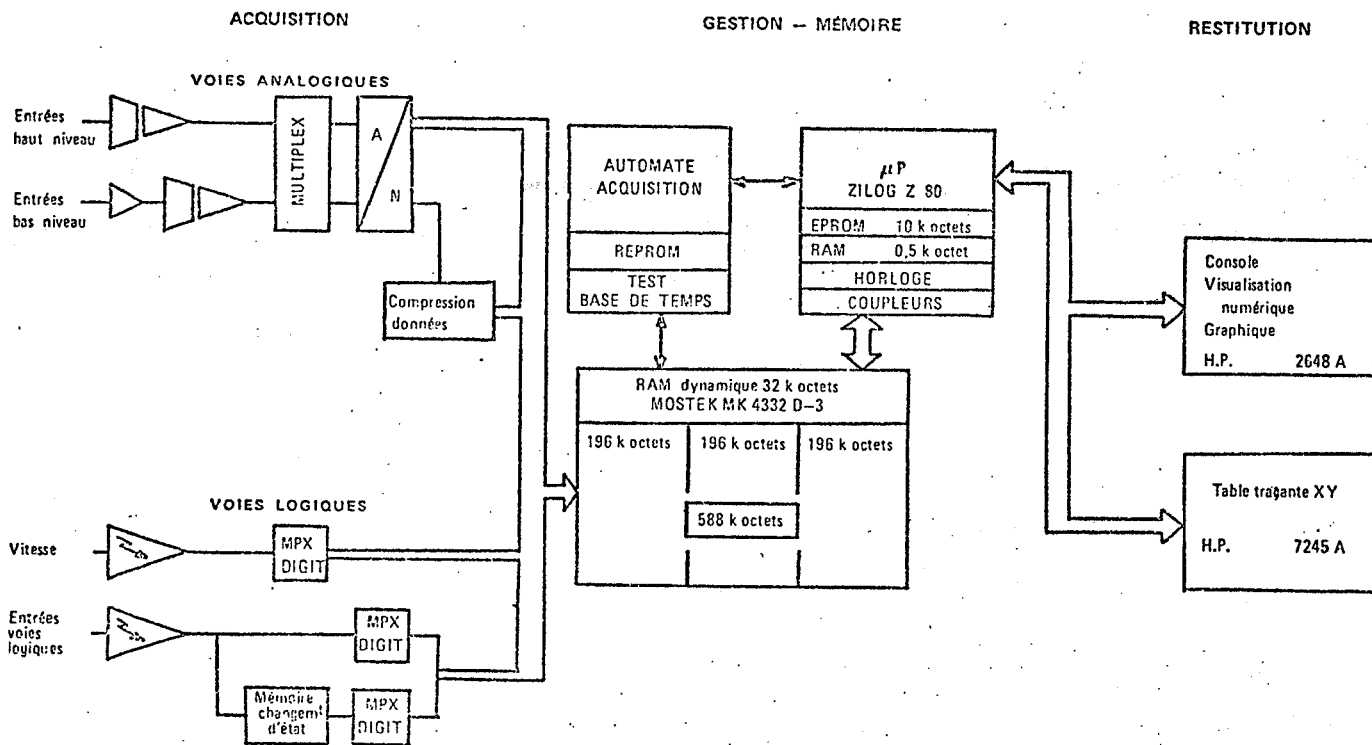


FIGURE 3 : Fast transient monitor for turbines.
Project N° 1

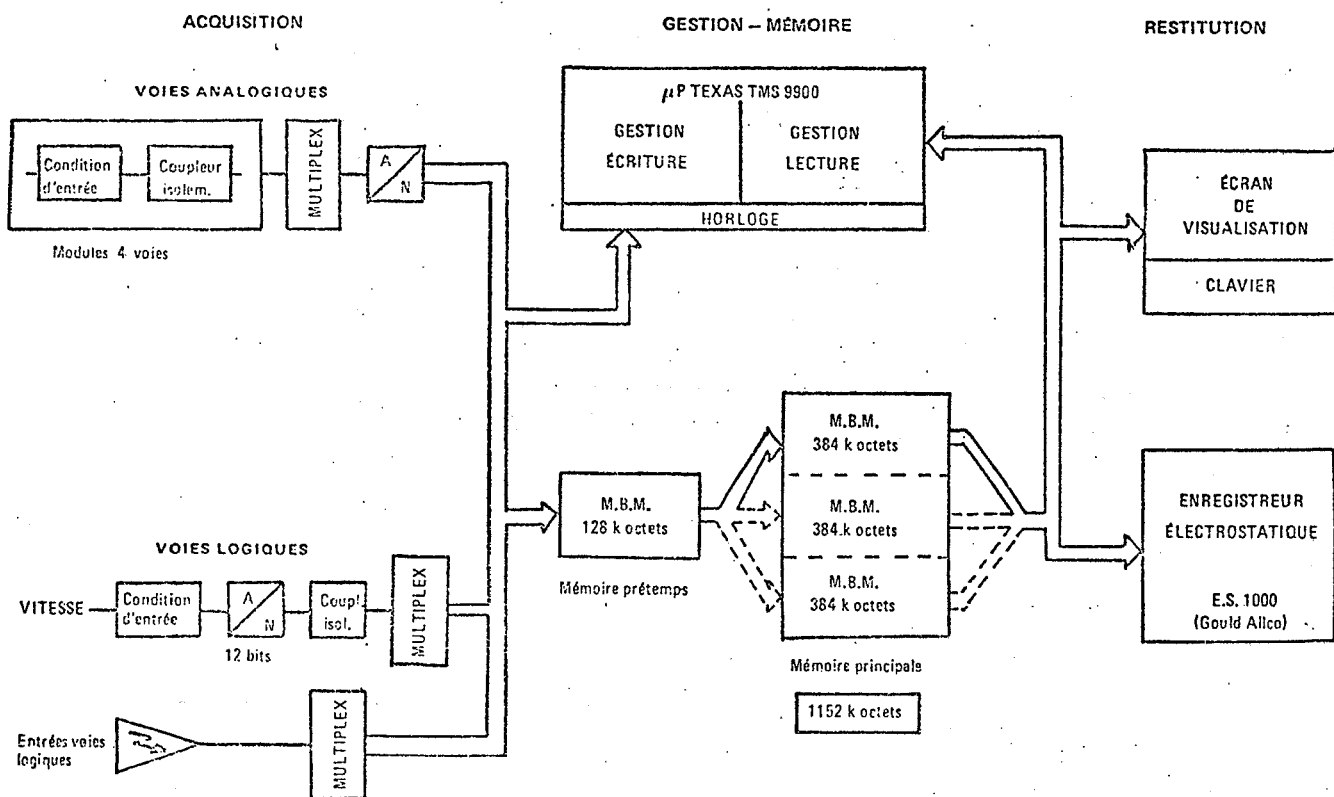


FIGURE 4 : Fast transient monitor for turbines.
Project N° 2

Y. Hashimoto, K. Kawai, M. Suzuki, S. Izumi, Y. Michiguchi,
K. Yamada, T. Joge

ACOUSTICAL SIGNAL PROCESSING FOR LIGHT WATER REACTOR DIAGNOSIS

Acoustical signal processing
for light water reactor diagnosis

by

Y. Hashimoto

Chugoku Electric Power Company
Hiroshima-shi, Japan

K. Kawai

Tokyo Electric Power Company
Chiyoda-ku, Tokyo, Japan

M. Suzuki

Chubu Electric Power Company
Nagoya-shi, Japan

S. Izumi, Y. Michiguchi and K. Yamada

Energy Research Lab. Hitachi Ltd.
Hitachi-shi, Japan

and

T. Joge

Power Generating and Transmission Group, Hitachi Ltd.
Hitachi-shi, Japan

Submitted to
IAEA-NPPCI Specialists' Meeting, 5th-7th December,
1979, Munich

Acoustical signal processing
for light water reactor diagnosis

Abstract

Acoustical signal processing methods for the detection of loose parts and abnormal vibration of reactor internals are investigated. The study involved extracting features of impact and friction sounds caused by anomalous phenomena in a reactor from accelerometer signals which are contaminated by background noise. For this purpose, three methods are investigated. These are: 1) a demodulation method; 2) impact period analysis; and 3) amplitude-time difference method.

The effectiveness of these methods are demonstrated through mockup testing and in-plant experiments for simulated impacts in a boiling water reactor.

1. Introduction

Recently, acoustical signal processing techniques for condition monitoring of mechanical equipment have been developed in order to achieve reliable plant operation. A piezoelectric accelerometer attached on the outside of a nuclear reactor can be used to detect anomalous phenomena related to metal to metal impacts or friction in the reactor. Application of an acoustic method to the on-line surveillance, however, has a problem which arises from the large and undesirable background noise generated by coolant flow and boiling.

The purpose of the present study is to extract features of impacts and friction sound caused by motion of loose parts

and anomalous vibration of reactor internals and to estimate the source position of the sound using accelerometer signals contaminated by background noise.

2. Signal processing

2.1. Demodulation method

The amplitude of metal to metal friction sounds depends on relative speed of the two metals. Therefore, the friction sound caused by vibration is modulated by twice the vibration frequency. (See Fig. 1.)

This fact suggests that vibrational information is contained in the envelope of the friction sound. The frequency of the reactor internals vibration accompanying the friction can be estimated from the demodulated (envelope) signal of the friction sound. It is difficult to detect vibration of reactor internals by a sensor attached to the outside of the reactor vessel, although the sound is propagated to the outside of the vessel.

Experiments were carried out using the flow induced vibration test facility shown in Fig. 2. As a partial model of a BWR core, four full scale models of fuel channel boxes and a in-core instrumentation tube were installed in a water tank. The tank had four water jet flow holes on the bottom. The jet flow induced vibration of the components. Accelerometers were attached to the lower end of the instrumentation tube, the top of a fuel channel box and the outside of the tank.

Friction occurs between fuel channel boxes and the channel box support.

The frequency spectrum for a output signal obtained by the accelerometer attached to a fuel channel box is shown in

Fig. 3-(a). The fundamental vibration frequency of the channel box is 1.25Hz. The frequency spectrum obtained by the demodulation method is shown in Fig. 3-(b). The friction sound is detected by the accelerometer on the tank and the signal in the region of 1kHz - 10kHz is demodulated. The frequency component of 2.5Hz (twice the fundamental frequency of the channel box) appears in the spectrum.

2.2. Impacts period analysis

The metal to metal impacts caused by reactor component vibration are periodic and the period corresponds to the vibration frequency. The identification of impacting components is possible from the relationship between the natural frequency of the component and the impact period.

The impact period can be determined statistically by histogram analysis. As shown in Fig. 4, a period histogram is made from impacts signals. The horizontal and vertical axes of the histogram correspond to the time interval of impact and the detection frequency of each time interval for a given measuring time, respectively. The histogram can be made easily using a microprocessor. The random noise has an exponentially decayed distribution. The periodic signal appears as a peak on the histogram and the peak position corresponds to the impact period.

Fig. 5 shows results obtained for a histogram analysis. The data were collected using the flow induced vibration test facility (Fig. 2). Vibration was induced in the in-core instrumentation tube by the jet flow. The tube then hit the fuel channel boxes and the impact sound was detected by the accelerometer at the end in the tube. The peak seen in the histogram corresponds to these tube impacts.

2.3. Amplitude-time difference analysis

For the detection of impacts accompanying anomalous phenomena in a reactor, similar signals such as electrical spike noise and sound of machine components under normal operation should be rejected.

The information relating to impact position is valuable for spurious alarm rejection and location of loose parts.

Impacts which accompany normal machine operations, such as control rod motion, occur at known positions. Therefore, these impact signals can be discriminated from impacts generated by anomalous phenomena by analysis of position information.

The information on impact position is contained in mutual relationships between amplitudes and detection times of impact signals of three or more acoustic sensors. As shown in Fig. 6, impact signals detected by 3 sensors (A, B and C) have time differences relative to each other and the amplitudes are also different. The detection time and amplitude depend on the length of the sound path and shape of the sound media. The ratio of amplitudes and time differences between the sensor signals, however, is invariable for an impact at the same position. This information is represented as an amplitude-time difference pattern (Fig. 6). In the figure, the horizontal and vertical axes represent time from the first detection signal and amplitude normalized by maximum amplitude (V_c), respectively. The information from each sensor signal is represented as a position on the two dimensional plane. This pattern is invariable for the impact occurring at the same position.

Experiments with the amplitude-time difference analysis were carried out by using a BWR. As shown in Fig. 7, accelerometers were attached to several positions of the BWR. Impacts were given to the reactor vessel by hitting with a

hammer. The acoustic signals were recorded on a 16 channel transient memory (1024 words/channel) and the analysis was carried out by microprocessor.

An example for an amplitude-time difference pattern of the reactor vessel impact is shown in Fig. 8. These data are average values of 10 impacts and deviations of time differences are denoted by the bars. The deviations of amplitude are less than 5% of full scale. The data scattering for the impacts at the same positions is sufficiently small.

The position of impact can be estimated by searching for a similar pattern from a list of known patterns, filed previously, and obtained by hitting positions of a reactor vessel with a hammer.

3. Conclusions

For the detection of loose parts and abnormal vibration of reactor internals, several acoustical signal processing methods were investigated. These are:

- 1) demodulation method for the detection of metal to metal friction caused by vibration of reactor internals;
- 2) impact period analysis for the detection of periodic impact sound in a reactor; and
- 3) amplitude-time difference method for location of impacts and rejection of false alarms.

The effectiveness of these methods were demonstrated through mockup testing and in-plant experiments for simulated impacts on a boiling water reactor.

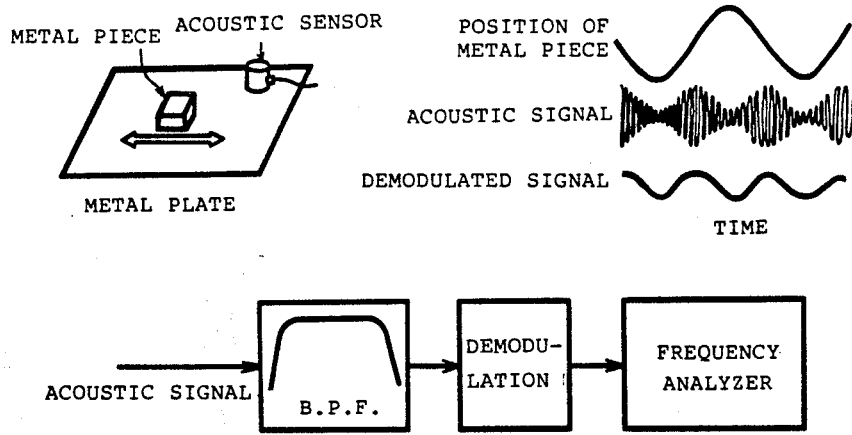


Fig. 1 Fundamentals of the demodulation method.

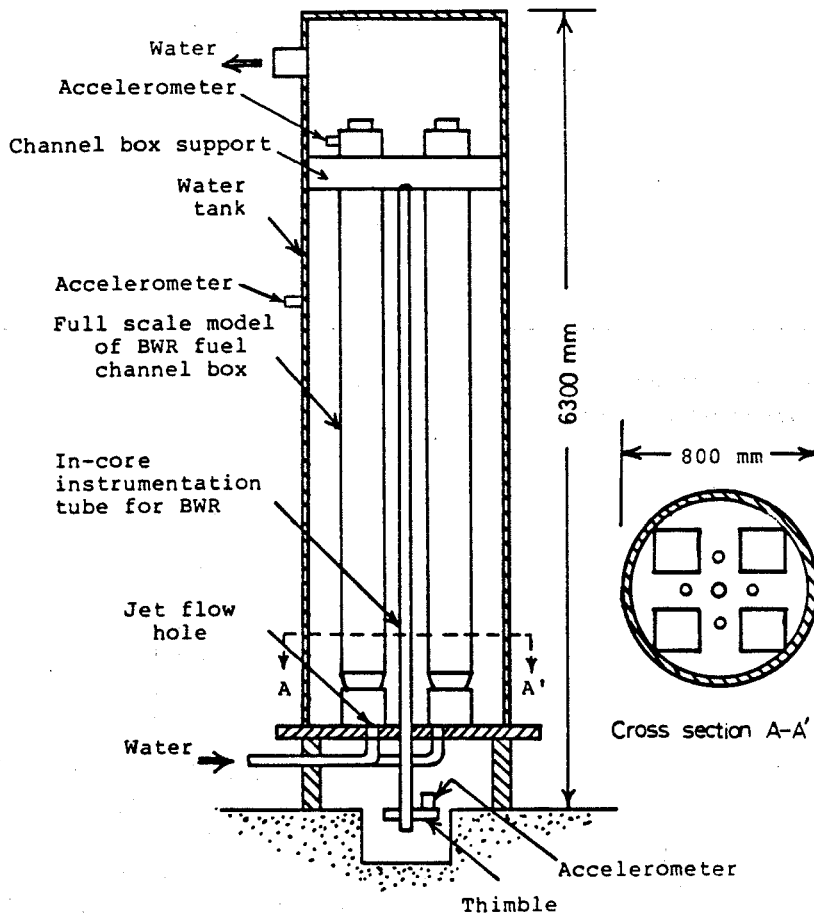


Fig. 2 Schematic cross sectional view of the flow induced vibration test facility.

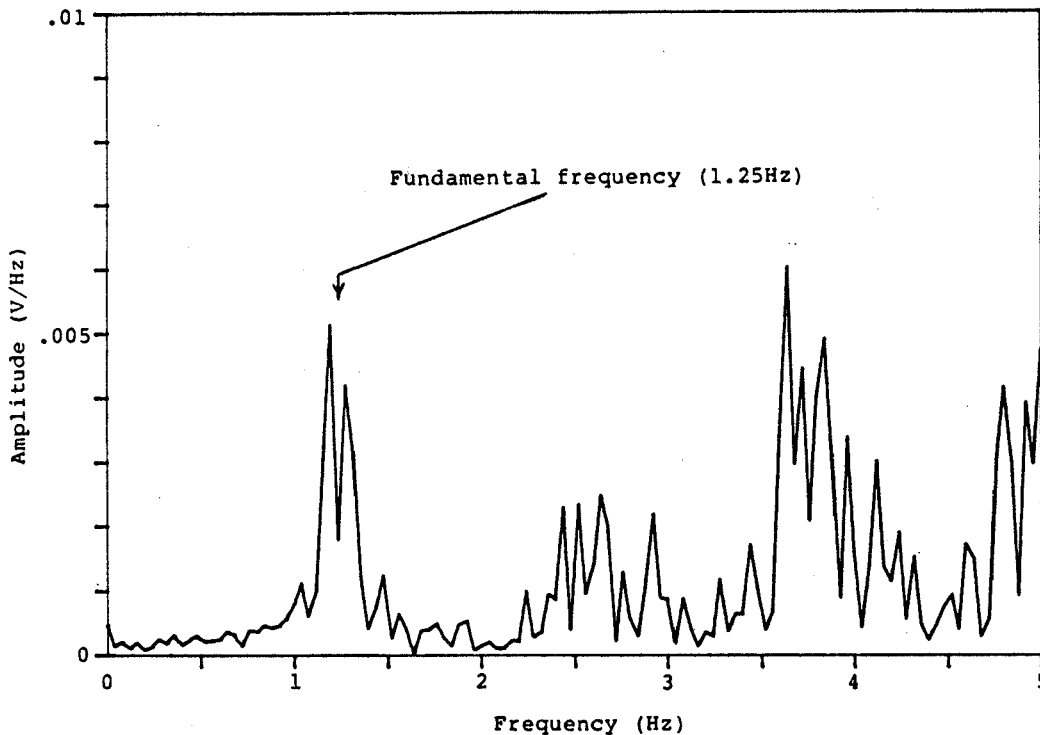


Fig.3-(a) Vibration spectrum of the fuel channel box.
(Analysis of the accelerometer signal on
the fuel channel box)

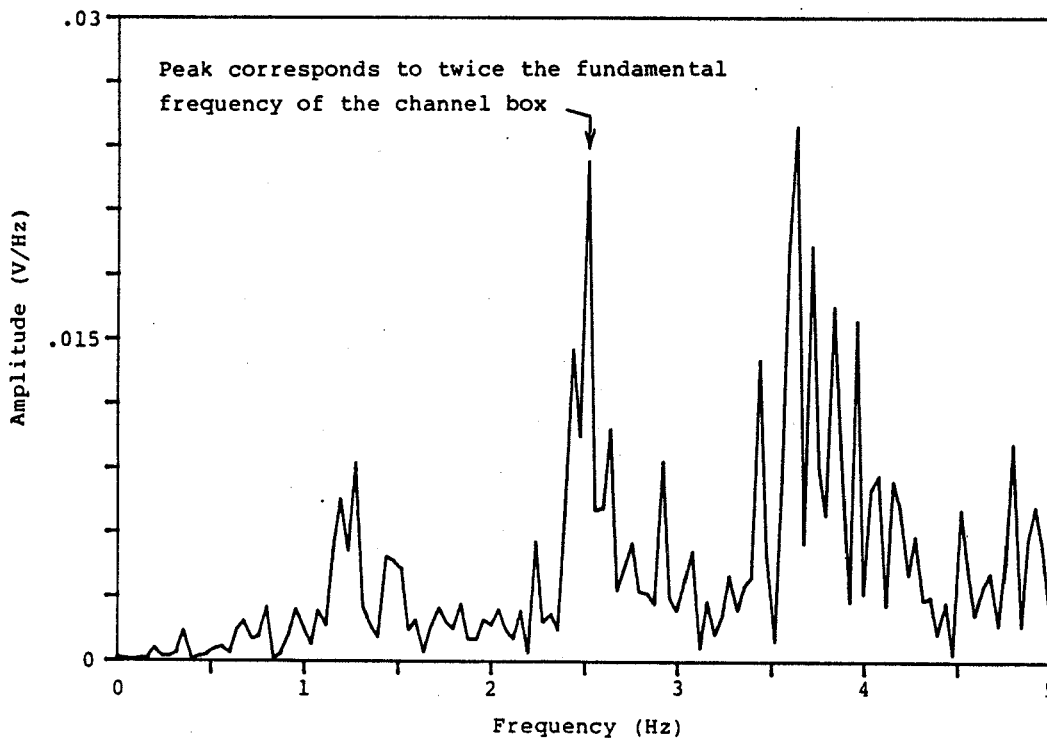


Fig.3-(b) Vibration spectrum of the fuel channel box
obtained by demodulation method.
(Analysis of the accelerometer signal on the
outside of the water tank.)

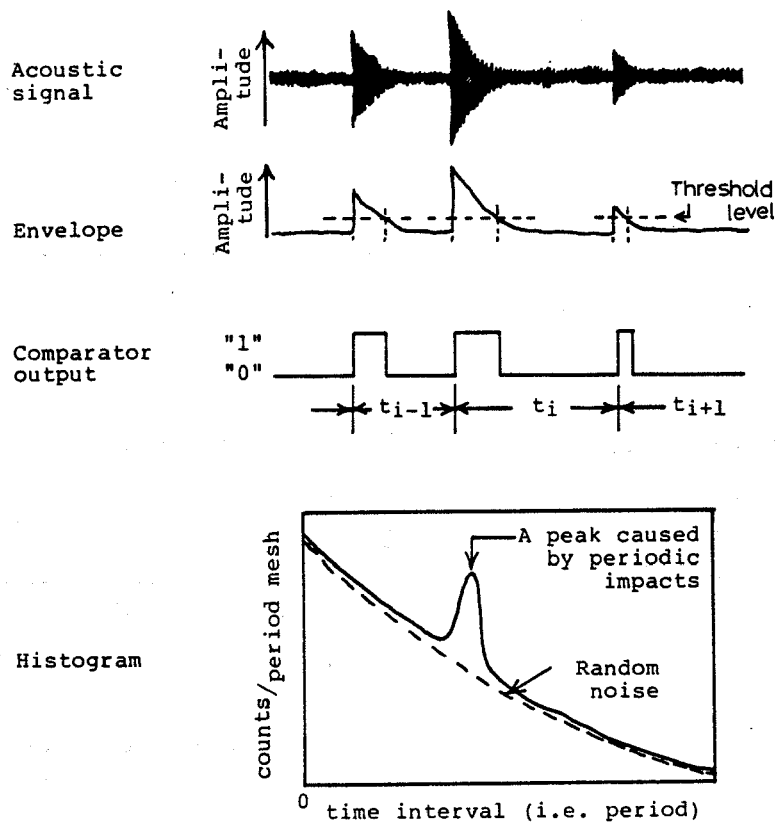


Fig. 4 Fundamentals of period analysis.

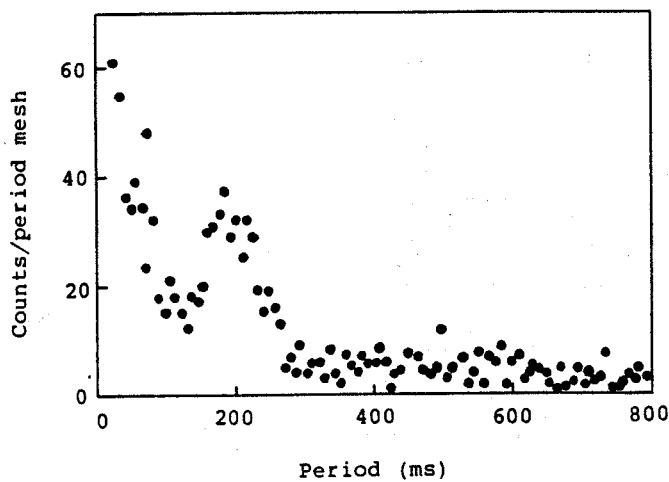


Fig.5 Period histogram of the in-core instrumentation tube impacts.

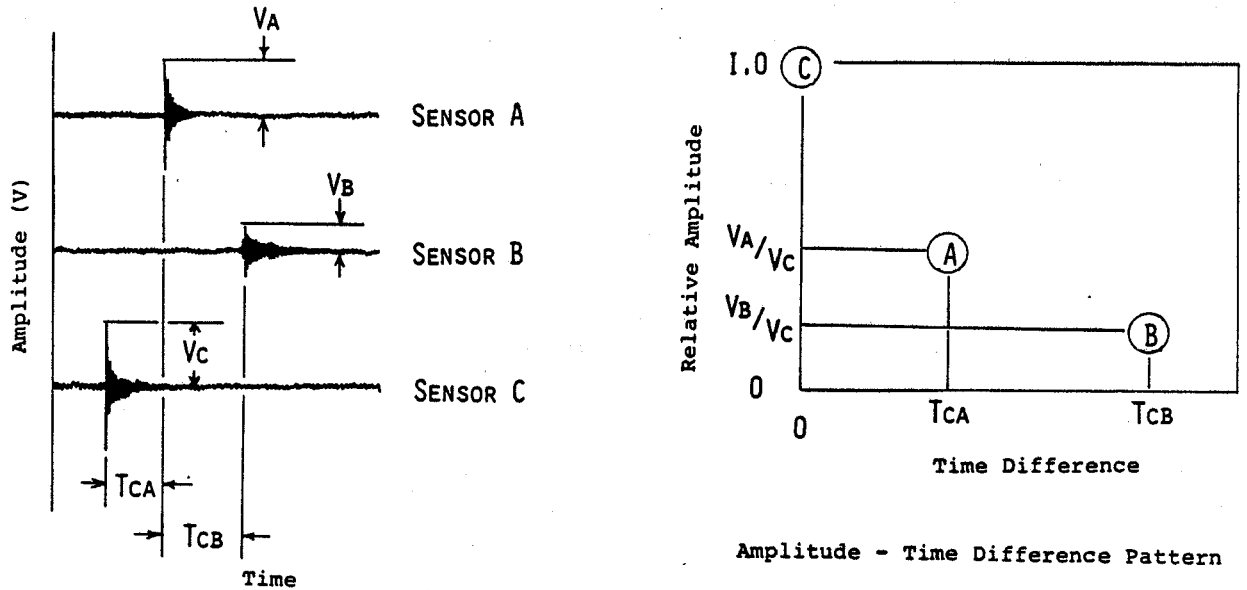


Fig.6 Fundamentals of amplitude-time difference method.

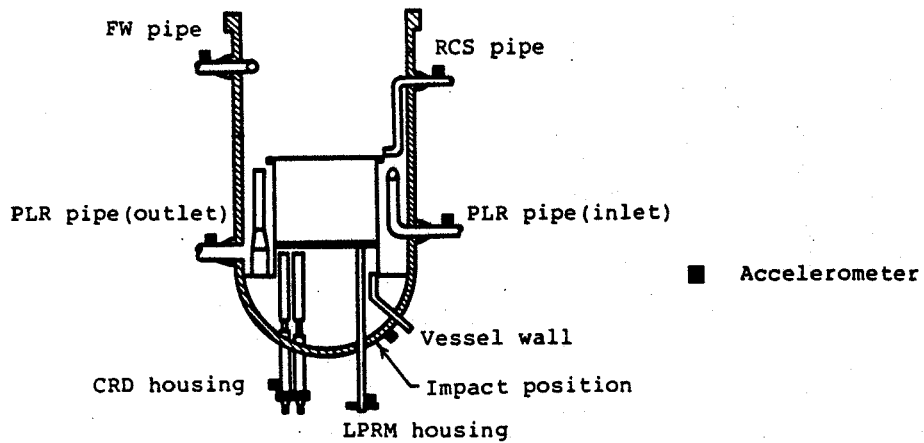


Fig. 7 Position of accelerometers on a BWR for impact testing.

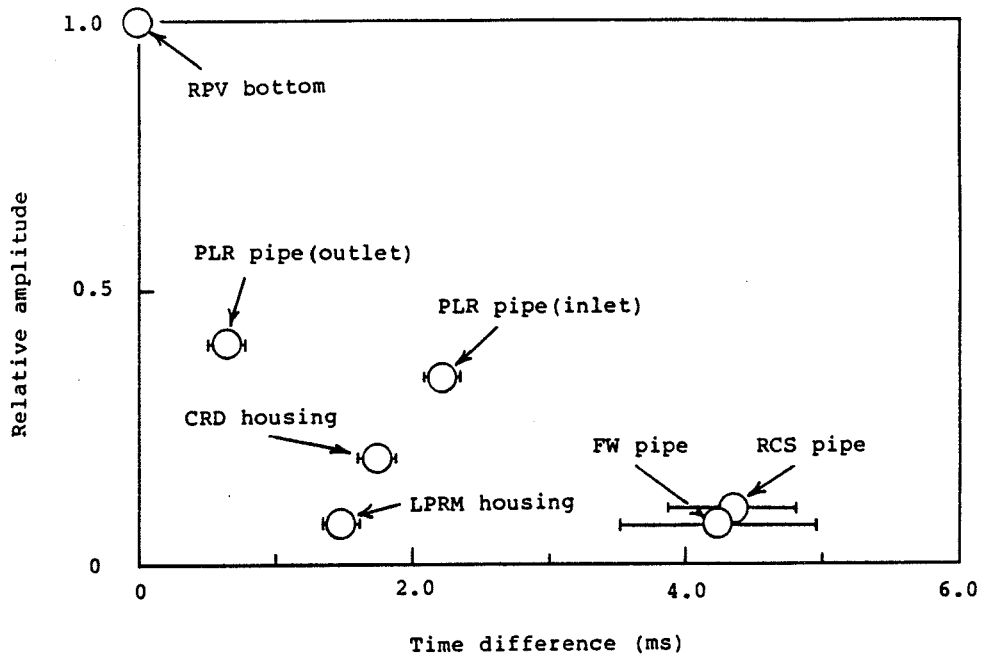


Fig. 8 Example of amplitude-time difference pattern of impacts on a BWR.

R. Assedo, P. Bernard, J.C. Carre, J. Cloue, A. Epstein
PWR NEUTRON NOISE SURVEILLANCE : NOISE SOURCES AND THEIR
EFFECTS

IAEA-NPPCI SPECIALIST MEETING

MUNICH, 5.7 DECEMBRE 1979

PWR NEUTRON NOISE SURVEILLANCE : NOISE SOURCES AND THEIR EFFECTS.

R. ASSEDO⁽¹⁾ - P. BERNARD⁽²⁾
J.C. CARRE⁽³⁾ - J. CLOUE⁽²⁾ - A. EPSTEIN⁽³⁾

(1) Société FRAMATOME - Tour FIAT - 92084 PARIS LA DEFENSE (France)

(2) C.E.A. - DEDR/DRE - CEN/CADARACHE
13115 - Saint Paul lez Durance (France)

(3) C.E.A. - DEDR/DEMT - CEN/SACLAY
B.P. n°2 - 91190 GIF sur YVETTE (France)

INTRODUCTION

Neutron noise analysis can be used as an efficient and simple mean of surveillance in PWRs, using existing detectors in a reactor in normal operating conditions.

For performing an effective surveillance, and clear diagnosis is important to have a good knowledge of the noise sources in PWRs and of their effects on the detectors' signals.

In this paper, we present an analysis of the potential or actual noise sources and experimental results of neutron noise measurements performed on three differently designed reactors. The consequences of these investigations are then applied to define principles of surveillance

I - POTENTIAL SOURCES OF NOISE IN PWRs

I-1. General principles.

Neutron noise sources in a PWR are related to its technological design, especially for the mechanical and thermohydraulic aspects. The effects of these perturbations and their propagation inside the reactor depends on the nuclear characteristics of the core, and particularly on its size.

Main physical origin of neutron noise are fluctuations of the nuclear characteristics of the media concerning the neutron transport.

We can distinguish two general categories of perturbations : transmission and direct flux effects.

I-1.1. Transmission

These effects concern fluctuations of the transport, in the non multiplying regions traversed by out going neutrons, and will induce fluctuations on excore detectors. The flux effect inside the core is weak.

I-1.2. Direct flux effect

This concerns phenomena that change the flux inside the core. A given perturbation will induce fluctuations of flux, manifesting themselves in different ways according to the size and shape of the core, as it has been studied by several authors /1/ to /4/.

For instance, a displacement of one assembly in a small core A (Fig.1) will induce flux fluctuations that will be strong throughout the core, although the same displacement of the same assembly in a large core B (fig. 1) will induce a much smaller effect, more or less limited to the perturbed region.

I-2. Noise sources

Physical and empirical considerations lead us to consider a set of possible neutron noise sources in a PWR working in steady state conditions.

These sources can exist in normal conditions or appear in some particular cases and sometimes in connection with a malfunction.

These sources, their effect on flux and the sensors associated to their detection are summarized in table 1.

I-2.1. Mechanical sources

Vibrations of internal structures (Fig. 2)

These important noise sources have been investigated by loop experiments and computations for 900 MWe PWR. Some shapes of deformation are presented in fig. 3.

The core barrel and the thermal shield have movements of mode 1 (pendulum movement) and higher modes, mainly mode 2 of the thermal shield and mode 3 of the two components.

The vessel has a pendulum movement too. The mechanical behaviour of internal structures for a PWR like FESSENHEIM is now clearly known (/5/ to /9/).

These sources mainly affect transmission, and they can lightly affect incore flux, by reflector variation induced by vibrating structures at the vicinity of fuel assemblies.

We show in table 2 the values of coefficients relating the fluctuations of excore detectors to the displacement of each structure, for a 900MWe reactor as FESSENHEIM. These computations have been performed with ANISN 1D transport code /10/.

The normalized APSD of neutron noise corresponding to internal structures (and fuel) vibrations is :

$$P(f) = \sum_{i=1, j=1}^3 h_i h_j P_{\Delta x_i \Delta x_j}(f)$$

where

Δ_{xi} is the displacement of the component i

$P_{\Delta x_i \Delta x_i}$ is the APSD⁽¹⁾ of the displacements of the component i

$P_{\Delta x_i \Delta x_j}$ is the CPSD⁽²⁾ of the displacements of the components i and j

h_i and h_j are the coefficients associated to the movements of components i and j.

An important observation is that movements of the core barrel or thermal shield, without any displacement of the fuel, can be observed on excore detectors.

Fuel vibrations

Beam modes of fuel assemblies are expected to induce neutron noise. For external assemblies, a radial displacement will induce two effects :

- change in transmission, because the source of neutron is nearer to the vessel, and so the thickness of the water is reduced.

- direct flux effect by reflector effect

Vertical movements can also induce flux perturbations, in case of fatigue, or breaking down of the top springs,

Control rods or burnable poison vibrations :

These vibrations will cause fluctuations of the flux inside the core.

I -2.2. Thermal sources

I-2.2.1. Effect of transmission

Fluctuations of water density caused by the temperature fluctuations in the water intervals between the core barrel and the vessel will change neutron transport from the core to excore detectors.

(1) APSD : Auto Power Spectral Density

(2) CPSD : Cross Power Spectral Density

I-2.2.2. Effect on incore flux

Every change in density and temperature of the moderator will induce change of the flux in the core. Several phenomena can induce fluctuations:

- Inlet temperature fluctuations
- Primary flow
- Fluctuating cross flows at different temperatures
- Boiling .

I -2.3. Other sources

. Detection noise

Random arrival of neutrons on the flux detector induce a quasi white noise, whose normalized DSP is equal to $(2/\text{counting rate of the detector})$.

. Inherent reactivity noise

This stochastic noise source is related to the white reactivity noise due to the discontinuous nature of the fissions. In power operating reactors, the normalized PSD of the fluctuations due to this source is about 10^{-5} of the value of the PSD of the white detection noise. So this source can be neglected.

. Primary pumps

The primary pumps induce on the PSD of the detectors resonances corresponding to the angular speed of the pump and its overtones.

. Movements of the detector

In certain conditions, vibrations of the detectors can induce fluctuations of its signal;

. Apparatus noise

The electronic device associated to the chambers induce a noise, that can be supposed constant in absolute units.

. Interferences

Other electrical devices at the vicinity of detection system can induce interferences on the recorded signal.

II - MEASUREMENTS ON SEVERAL PWRs

II-1. Presentation

We performed noise measurements on three different kinds of PWR :

- Reactor of CHOOZ. 1040 MWth, 310 MWe
First startup in 1967.
Definitive startup after repair in 1970.
- C.A.P. : "Chaudière Avancée Prototype" (Advanced Prototype Reactor)
set in the Nuclear Research Center of Cadarache.

The measurements were performed with a 12 17x17 assemblies core (see fig. 4)

- First serie of 900 MWe (Pth \approx 3000 MWth)

Measurements were performed on unit 1 and 2 of the FESSENHEIM plant and unit 2 and 3 of the BUGEY plant (the first unit is 600 MWe gas-graphite reactor).

Conception of internal structures and core disposal is shown in fig. 2.

II-2. Main characteristics of noise measurements

II-2.1. Reactor of CHOOZ

II-2.1.1. Experimental data.

Several series of noise measurements have been performed on this reactor and particularly at different power levels.

The signals from excore ion chambers are gaussian and r.m.s of fluctuations is about 1 %₀ at full power, for a (0.1 Hz, 40 Hz) frequency domain.

We show in fig. 5 the PSD of signal from an excore ion chamber, for a measurement at full power. We can observe :

- 2 peaks at 4,3 Hz and 5,4 Hz
- some other peaks less marked
- a strong low frequency contribution
- a white noise over 20 Hz
- a peak at 24,7 Hz corresponding to the frequency of the primary pumps
- a peak at 30 Hz corresponding to the aliasing of the 50 Hz network frequency (sampling frequency : 80 Hz)

The results of phase and coherence analysis show :

- for two opposite detectors, a strong coherence and a 180° phase shift at 4,3 Hz and 5,4 Hz (fig. 6) and a rather good coherence and 0° phase shift around 20 Hz. No good coherence elsewhere.
- the coherence and phase of CPSD of upper and lower signals of detectors are shown in fig. 7. The coherence is almost equal to 1 up to 15 Hz and there is no phase shift, excepted in the low frequency range where we can see a decreasing coherence and a phase shift.

When the power level decreases, the spectra changed as shown in fig. 8. The r.m.s. value in different frequency ranges, versus power, is shown in the same figure.

II-2.1.2. Interpretation

. Peaks at 4,3 Hz and 5,4 Hz correspond to pendulum movements of core barrel and fuel. The observed amplitudes (8σ) versus direction is shown in fig. 9, with estimated displacements. The reason why we observe two resonances must be that there exists a contact between the core barrel and the vessel on an inlet water nozzle.

. Other peaks must correspond to higher modes of vibrations of the core barrel. In particular 20 Hz must correspond to a second order ring mode (no phase shift for two opposite ion chambers).

. White noise over 20 Hz correspond to the white detection noise and its level versus power corresponds to the predicted formula.

. Low frequency noise is proportional to the power level. We believe that this noise is due to fluctuating cross flows in the core, inducing local temperature fluctuations of the water. The effect will be proportional to the radial temperature gradient and thus to the power level.

It seems that the temperature fluctuations induce a rather local effect on the flux. The peripheral temperature fluctuations will be first observed on the lower part of an excore detector and then on the upper part with a time lag τ_0 corresponding the transit time between this two detectors (0,4 s) So the phase shift of CPSD of upper and lower detector is proportional to the frequency. This can explain observed coherence and phase (fig. 7) :

Two contributions exist on detectors

$P_1(f)$: low frequency mechanical noise, with no phase shift for the upper and lower detectors

$P_2(f)$: temperature noise

The coherence will be

$$C(f) = \frac{P_1(f) + e^{-2\pi j f \tau_0} P_2(f)}{P_1(f) + P_2(f)}$$

and the phase shift

$$\varphi = \left(\text{Arg } P_1(f) + e^{-2\pi j f \tau_0} P_2(f) \right)$$

for $f \approx 0$, $C(f) \approx 1$, $\varphi \approx 0$

When f increases, φ becomes negative and $C(f)$ decreases
when f keeps increasing, $P_2(f)$ vanishes $\varphi \rightarrow 0^\circ$
and $C(f) \rightarrow 1$.

When the power level decreases, this phenomenon vanishes, as it was observed during a measurement at several power levels (fig. 10).

II-2.2. C A P

II-2.2.1. Experimental data.

The signal of incore and excore detectors have been recorded in different operating conditions. They have a gaussian distribution and their rms amplitude are about 3‰ at full power in the (0.1 Hz, 20 Hz) frequency domain.

The main characteristics of neutron noise measurements on this reactor is that the fluctuations of flux are global inside the core : every couple of incore or excore detector gives a coherence almost equal to 1 and in phase signals up to 12 Hz.

We show in fig. 11 the PSD of an excore detector. We can observe :

- a strong low frequency contribution
- damped peaks at 7 Hz and 1,5 Hz.

When the power changes, evolution of the PSD is shown in fig. 12.

II-2.2.2. Interpretation

. Following mechanical results, the part of the PSD independant of the power level must correspond to vibrations of fuel assemblies excited by the water flow. These vibrations induce flux fluctuations globally inside the core.

. Low frequency contribution, proportional to the power level must correspond to temperature fluctuations, induced by fluctuating cross flows as for the CHOOZ reactor. The rms amplitude of the corresponding reactivity is about 2×10^{-5} , which correspond to an homogeneous temperature fluctuation in the core of about 3×10^{-2} °C rms.

. No pendulum movement of internal structures was observed in the (0.1 Hz, 20 Hz) frequency range.

II-2.3. 900 MWe reactors

II-3.1. Experimental data.

Measurements have been performed on unit 1 and 2 of the FESSENHEIM plant and unit 2 and 3 of the BUGEY plant.

Excure detectors' signals were recorded and analysed. Signals are gaussian.

Figure 13 shows PSD obtained on unit 1 and 2 of FESSENHEIM. BUGEY 2 shows PSD identical to FESSENHEIM 1's one and BUGEY 3 to FESSENHEIM 2's one. Values of coherence and phase between detectors are indicated (couples of opposite detectors : 1-2, 3-4).

For FESSENHEIM 1, rms amplitude was 0.8 ‰ and 1 ‰ for FESSENHEIM 2 at full power, (0.6 Hz, 40 Hz) frequency domain.

Frequencies of peaks are different for the two reactors, and in particular the main peak is at 10,8 Hz on unit 1 and at 7,2 Hz on unit 2.

II-2.3.2. Interpretation

The different observed peaks correspond to vibrations of internal structures :

- vessel
- upper and lower core plates
- core barrel
- thermal shield
- fuel.

We show in fig. 14 to 16 the comparison between the PSD of excure neutron noise and accelerometers located on the vessel. There exists a good agreement of the frequencies for several resonances. Tables 3 and 4 summarize the existing movements.

Expected value for the main pendulum movement of internal was 7,2 Hz as observed on FESSENHEIM 2. The reason why this frequency is higher (11.5 Hz) on unit 1 is that there exist a contact on a radial support key, changing frequencies for this reactor,

3,2 Hz to 3,7 Hz correspond to fuel assemblies vibrations.

19 Hz and 33 Hz correspond to second order ring modes of thermal shield and core barrel. In such movements, the fuel is motionless. The presence of these peaks in the signals of excure detectors is a qualitative experimental verification of transport computation presented in part I.

Up to now, we did not perform measurements at several power levels, at the end of a cycle (where the temperature coefficient is maximum) and long enough to allow good low frequency analysis. So we can only suppose that the same temperature fluctuations do exist, as in reactor of CHOOZ and in the CAP.

II -3. Comparison of noise sources

It is interesting to compare results obtained on these three kinds of reactors. Table 5 shows this comparison.

- Internal vibrations

They are the main source on CHOOZ and 900 MWe reactors but do not exist on the CAP (the design of internal structures is quite different).

- Fuel vibrations

They have been observed on the CAP and 900 MWe reactors, in which the fuel has the same design. For CHOOZ, the fuel is in boxes and no frequency must exist below 30 Hz; this must be the reason why these phenomena were not observed in this reactor.

- Water temperature fluctuations

This phenomena must exist in all the three reactors.

It is important to note that for small cores like CAP the same noise sources induce in phase global and strongly correlated phenomena, but in large cores, local phenomena predominate.

Looking back to table 1's potential sources we can observe noise sources actually detected in the three reactors, under normal conditions.

III - APPLICATION TO REACTOR SURVEILLANCE

III-1. Principles

The previous analysis has shown the field of the phenomena that could be monitored by neutron noise.

Let us reconsider the main phenomena from a reactor surveillance point of view.

III-1.1. Mechanical phenomena

III-1.1.1. Vibrations of internal structures.

They are the main noise source on excore detectors under normal conditions. The functions of a surveillance methodology would be to :

- identify the vibratory behaviour of the system (main motion about 7 Hz for free vibrations and 11 Hz with contact on radial keys)
- check that amplitudes are correct
- detect important malfunctions at their beginning (loss of function of the hold down spring) in order to avoid damages.
- diagnosticate typical anomalies (thermal shield flexure broken...)

III-1.1.2. Vibrations of core components

- Fuel assemblies

- . beam modes : amplitudes must be limited
- . vertical movements : this anomaly is related to a rupture of top springs and must be detected

- Absorbers

Any important vibration of absorbers (control or burnable poisons) must be detected and considered as an anomaly.

III-1.2. Thermohydraulic phenomena

- Temperature fluctuations

- . Usual cross flows detected in PWRs must be considered as normal and related to hydraulic characteristics of the flow inside the vessel.
- . Abnormal cross flows, such as those induced by a clearance in the

in the baffle, and that could damage fuel rods, should be detected by these techniques.

Boiling

Boiling detection by neutron noise analysis is an interesting and important aspect of this technique. Systematic monitoring with fixed incore detectors would bring important informations. We do not deal with this aspect in the present paper.

III-1.3. Detectors

Noise techniques can detect incipient malfunctions of the detectors before that the CD is perturbed. This can be an interesting monitoring from an instrumentation maintenance point of view.

Remark

During a cycle there exist normal evolutions of noise sources and of their effects (burnup, temperature coefficients...) One must take into account these evolutions.

III - 2. Implementation considerations

Up to now, surveillance by neutron noise technique in France consisted in some periodic measurements by specialists and off line analysis. Some efforts to make this surveillance more systematic are on hand.

On the basis of the present analysis, and taking into account the complexity of signal processing involved in detailed treatments, we believe that the surveillance must include two complementary aspects :

- Use of a rather simple on-line system (1st level)
- Measurements by specialists periodically or in case of incipient anomaly detected by the on-line system (2nd level)

III-2.1. One line system (1st level)

This system must be designed to perform efficient monitoring of internal structures vibrations, fast detection, diagnosis and alarm in case of an important malfunction (loose of function of the hold down spring) in order to avoid damages of equipments, detection of unusual configuration and light anomaly suspected and in this case a specific measurement (2nd level) is required.

Among various solutions, a simple surveillance as

- band pass filtering of signals from excore ion chambers in appropriate frequency bands
- normalized r.m.s. and cross variance analysis of the corresponding filtered signals (or other methods : zero crossing...) and application of simple surveillance criteria should be convenient.

Signals from vessel accelerometers would be analysed at the same time by device. Probability of false alarm must be minimized.

Associated to this device, a simple channel spectrum analyser will give detailed frequency informations on the vibrationnal behaviour of the internal structures.

III-2.2. Specific measurements (2nd level)

In order to make the surveillance consistent, it is necessary to use specialized teams for :

1) periodical measurements (1 to 3 times a cycle) on incore and excore detectors, giving informations to adjust, if necessary (normal evolutions) the alarm levels of the on-line system, and to check that there is no anomaly associated to the corresponding phenomena :

- vibrations of the fuel assemblies, mainly vertical movements (use of incore signals)
- vibrations of absorbers
- abnormal temperature fluctuations

2) particular measurements for diagnosis in case of suspected anomaly.

CONCLUSION

Summarizing the experimental results in a few remarks, we can draw the following conclusions :

- Low frequency temperature fluctuations seem to be inherent in any PWR.
- Fluctuations induced by beam modes vibrations of assemblies is characteristic of the design of fuel assemblies with guide tubes and no box.
- Internal vibrations represent the most important noise source for excore detectors in reactors like CHOOZ and 900 MWe.
- The same phenomena induce strongly correlated fluctuations throughout the core for small reactors, while they cause lighter and local effects in large cores.

This knowledge of existing sources in normally working reactors associated to some effort to quantify the flux effect of the considered perturbing phenomena, give good understanding for reactor surveillance by noise analysis mainly concerning vibrations of internal structures and core components, and thermohydraulic phenomena.

REFERENCES

/1/ - D. WACH, G. KOSALY

"Investigation of the joint effect of local and global driving sources in incore neutron noise measurements".
Atomkernenergie 23, 244 (1974)

/2/ - K. BEHRINGER, G. KOSALY, L.S. KOSTIC

"Theoretical investigation of the local and global components of the neutron noise field in a boiling water reactor".
Eir-breicht Nr303.

/3/ - G. KOSALY

"Investigation of the local component of power-reactor noise via diffusion theory".
KEKI - 75-27

/4/ - K. BEHRINGER, G. KOSALY, I. PAZSIT

"Linear response of the neutron field to a propagating perturbation of moderator density (two-group theory of BWR-noise)".
Eir-Bericht Nr 359.

- /5/ - F. JEANPIERRE, M. LIVOLANT
Experimental and theoretical methods for assessment of flow induced vibrations of nuclear reactor internal structures.
3rd SMIRT Paper F1/5 LONDON (1975)
- /6/ - R. ASSEDO, M. DUBOURG, M. LIVOLANT
Model experimentation and analysis of flow induced vibrations of PWR internals.
Nuclear Engineering and Design Vol 27 n°3 July 1975.
- /7/ - R. ASSEDO, M. DUBOURG, A. EPSTEIN
Vibrations behaviour of PWR reactor internals model experiments and analysis.
3rd SMIRT Paper 1/6 LONDON 1975.
- /8/ - J. C. CARRE, R.J. GIBERT, F. JEANPIERRE, M. LIVOLANT
-PWR internals vibrations mode shapes calculation and test.
Progress in Nuclear Energy - Vol 1 p. 353 to 363 - 1977.
- /9/ - R. ASSEDO, A. EPSTEIN, R.J. GIBERT, F. JEANPIERRE, M. LIVOLANT
Hydroelastic model for PWR reactor internals SAFRAN 1
Validation of vibration calculation method
BNES- Vibration in nuclear plant. KESWICK May 1978.
- /10/- P. BERNARD, A. BRILLON, J.C. CARRE, S. SIGHICELLI
Neutron noise measurements on pressurized water reactors.
Progress in Nuclear Energy. Vol 1 p. 333 to 351 - 1977.
- /11/- P. BERNARD
Fluctuations neutroniques dans les réacteurs de puissance à eau sous pression.
Thèse PARIS 1978.

Table 1

SOURCE		EFFECT	SENSORS	ASSUMED POWER DEPENDENCE
VIBRATIONS OF INTERNALS		TRANSMISSION	EXCORE DETECTORS	CONSTANT
FUEL MOVEMENTS	BEAM MODES	TRANSMISSION + DIRECT FLUX EFFECT	EXCORE AND INCORE DETECTORS	CONSTANT
	VERTICAL MOVEMENTS	DIRECT FLUX EFFECT	INCORE AND EXCORE DETECTORS	CONSTANT
	INDIVIDUAL VIBRATIONS OF FUEL PINS	DIRECT FLUX EFFECT	INCORE AND EXCORE DETECTORS	CONSTANT
CONTROL RODS OR BURNABLE POISONS VIBRATIONS		DIRECT FLUX EFFECT	INCORE AND EXCORE DETECTORS	CONSTANT
FLUCTUATIONS OF WATER DENSITY IN NON MULTIPLYING REGIONS		TRANSMISSION	EXCORE DETECTORS	PROPORTIONAL TO THE POWER LEVEL
INLET TEMPERATURE FLUCTUATIONS		DIRECT FLUX EFFECT	INCORE AND EXCORE DETECTORS	PROPORTIONAL TO THE POWER LEVEL
PRIMARY FLOW FLUCTUATIONS		DIRECT FLUX EFFECT	INCORE AND EXCORE DETECTORS	PROPORTIONAL TO THE POWER LEVEL
FLUCTUATING CROSS FLOWS		DIRECT FLUX EFFECT	INCORE AND EXCORE DETECTORS	PROPORTIONAL TO THE POWER LEVEL
BOILING		DIRECT FLUX EFFECT	INCORE AND EXCORE DETECTORS	DEPENDING ON THE POWER LEVEL

*

*

*

* means that the source has been observed on a PWR.

Table 2

Nature of the movement	Coefficient h (cm ⁻¹)
Core barrel ring motion	0.02
Thermal shield ring motion	0.045
Fuel assembly displacement	0.06
Global pendular motion	0.12

$$\frac{\Delta\tau}{\tau} = - h_i \Delta x_i$$

τ : counting rate of the detector

Δx_i : displacement of component i (cm)

h_i : coefficient associated to component i (cm⁻¹)

Table 3

Frequency	Interpretation
3,2 Hz	Motion of the fuel
<u>10,8 Hz</u>	Main pendulum motion of internal structures
<u>13,5 Hz</u>	Main motion of the vessel
16,5 Hz	Motion of internal structures
19,2 Hz	Mode 2 of internal structures (core barrel)
24,8 Hz	Frequency of primary pumps

Interpretation of neutron noise and accelerometry measurements on FESSENHEIM 1

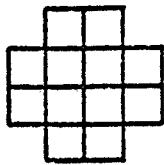
Table 4

Frequency	Interpretation
3,2 Hz	Motion of the fuel
<u>7,2 Hz</u>	Main pendulum motion of internal structures
11,6 Hz	Mode 2 of the thermal shield
13,5 - 14,6 Hz	Main movements of the vessel
18,3 Hz	Pendulum motion of the vessel
19,5 Hz	Mode 2 of the internal structures (core barrel)
23 Hz	Vertical movement of the vessel
24,8 Hz	Frequency of primary pumps

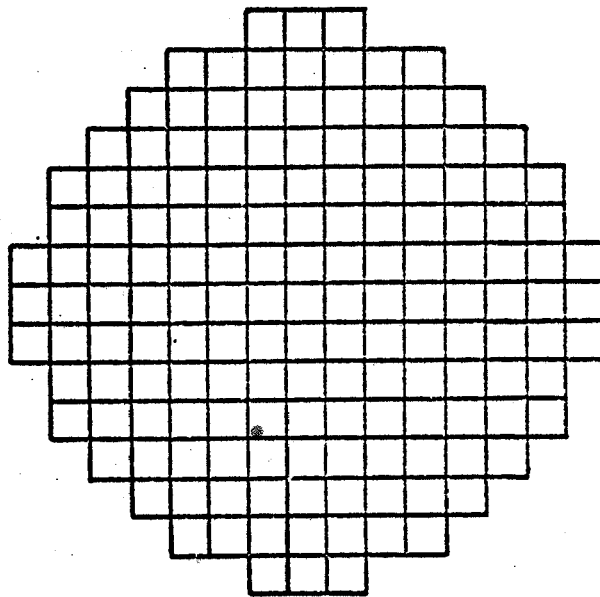
Interpretation of neutron noise and accelerometry on FESSENHEIM 2

Table 5

	CHOOZ	CAP	900 MWe
VIBRATIONS OF INTERNAL STRUCTURES	Yes	No	Yes
VIBRATIONS OF FUEL ASSEMBLIES	No	Yes	Yes
FLUCTUATION OF WATER TEMPERATURE (Cross flows)	Yes	Yes	Probable



CORE A



CORE B

Figure 1

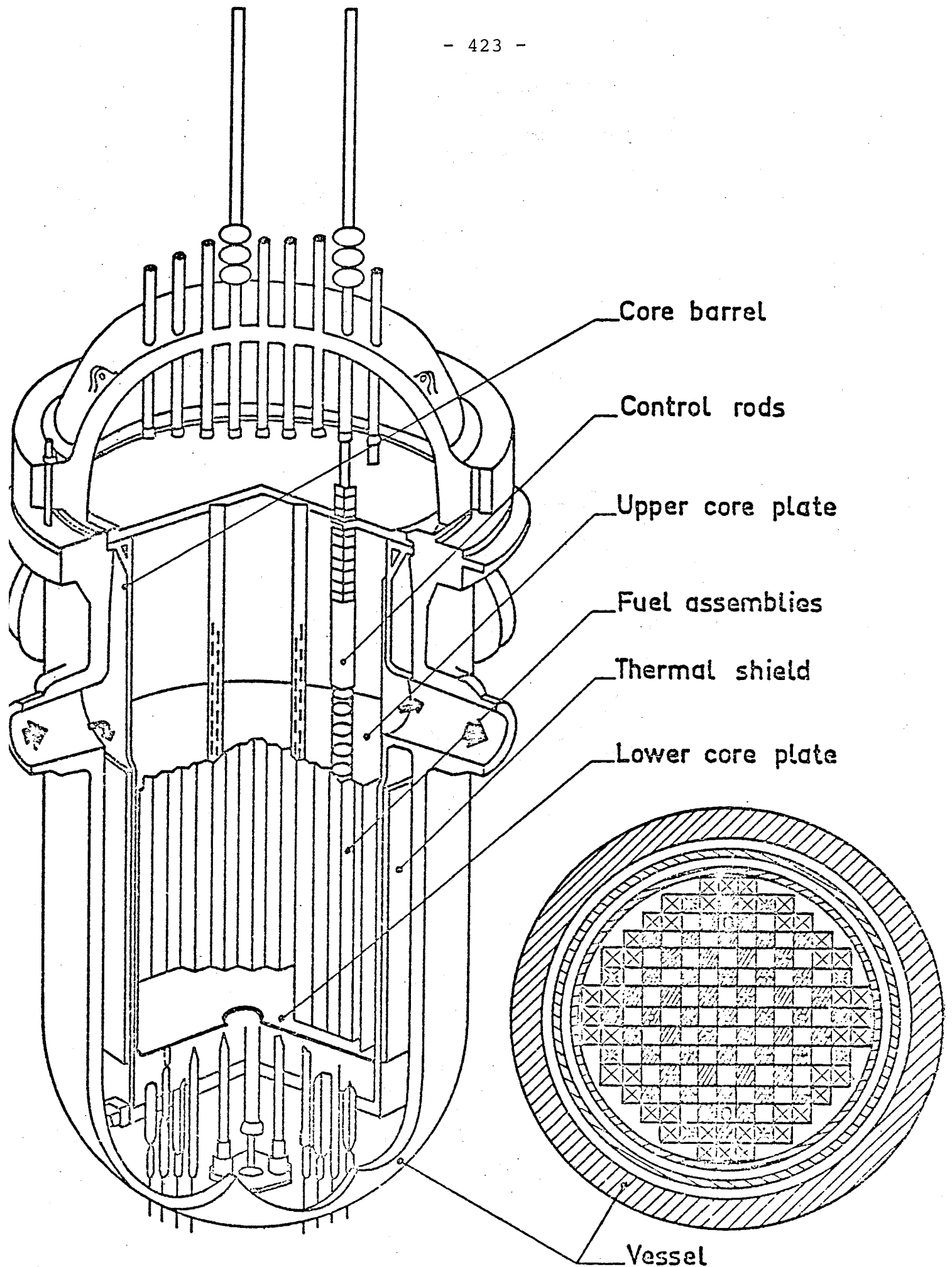
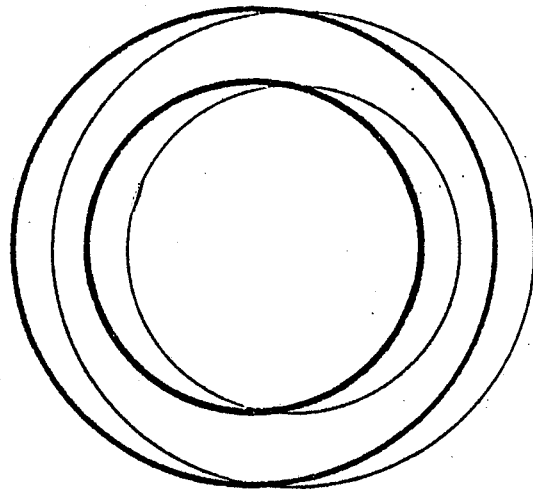
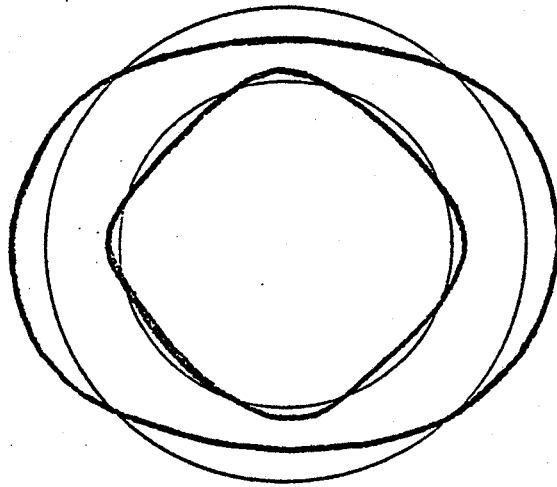


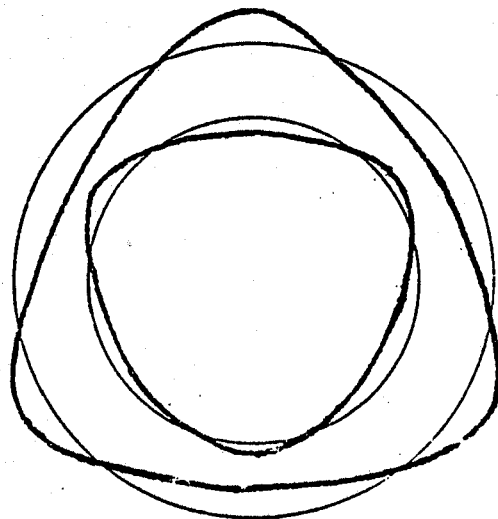
Figure 2 : FESSENHEIM : Vessel and internal structures



Mode 1
(pendular motion)



Mode 2



Mode 3

Figure 3 : Shapes of deformation of the core barrel and the thermal shield.

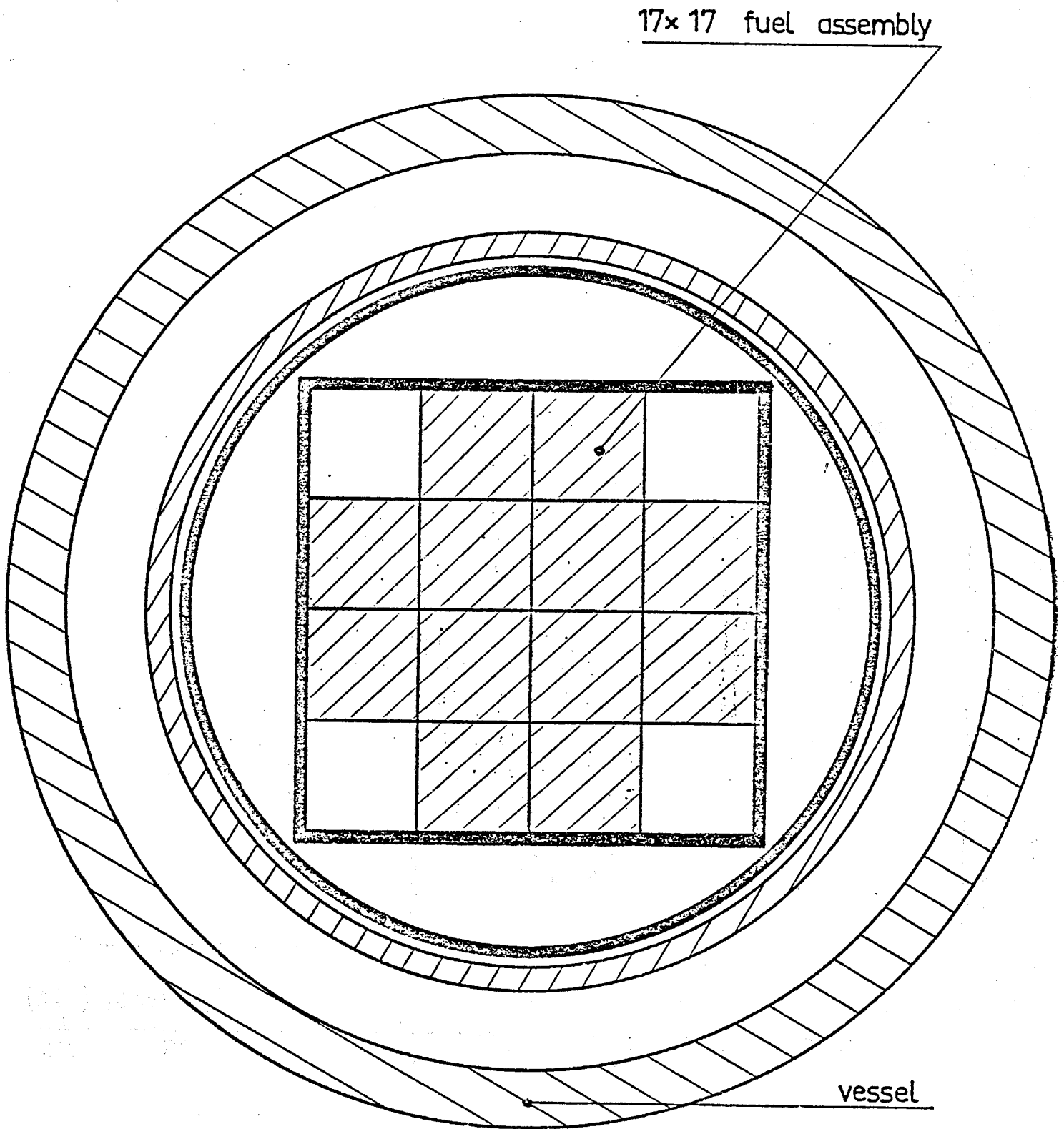


Figure 4 : Core of the C A P

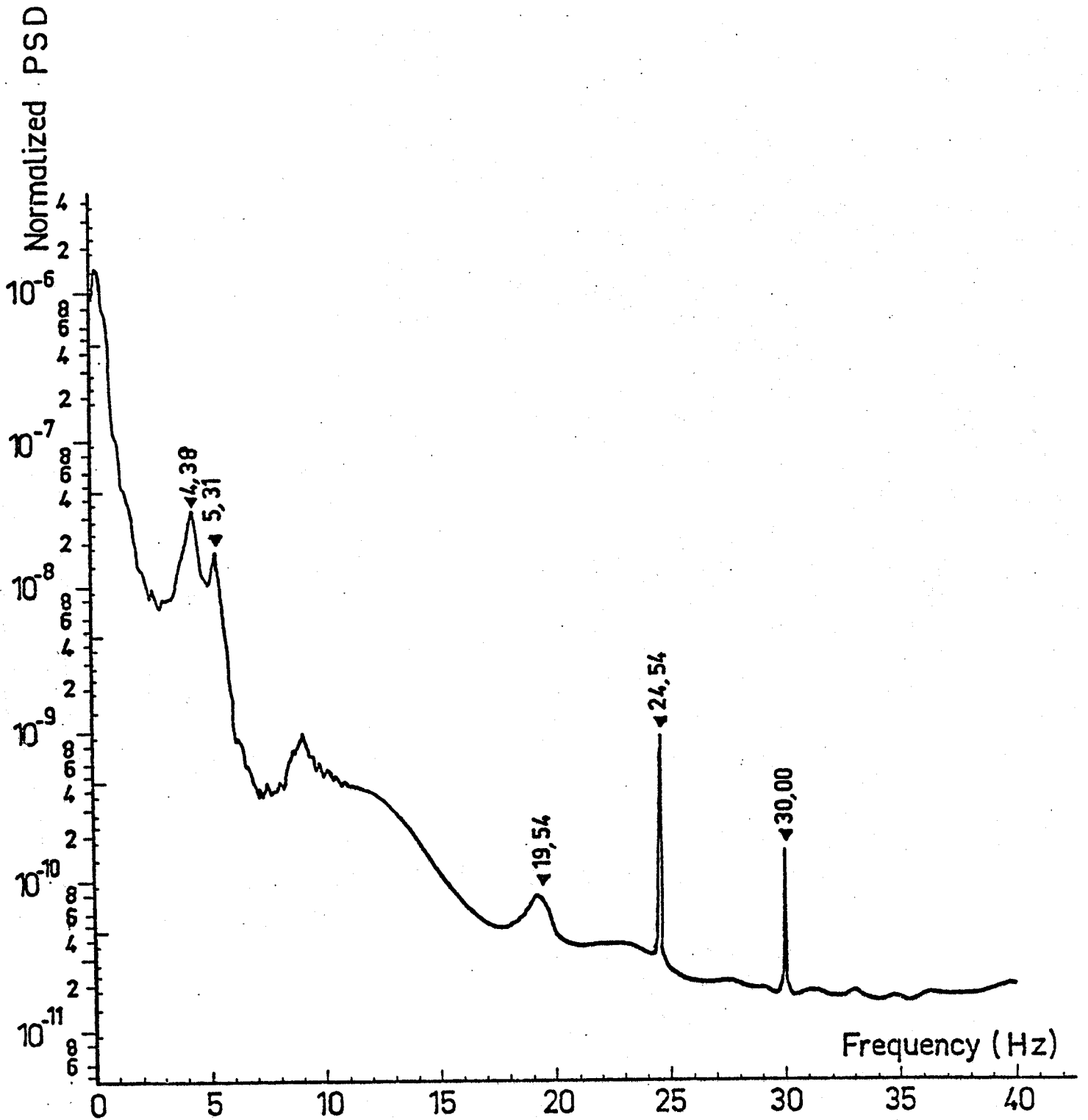


Figure 5 : PSD of an excore detector of the reactor of CHOOZ.

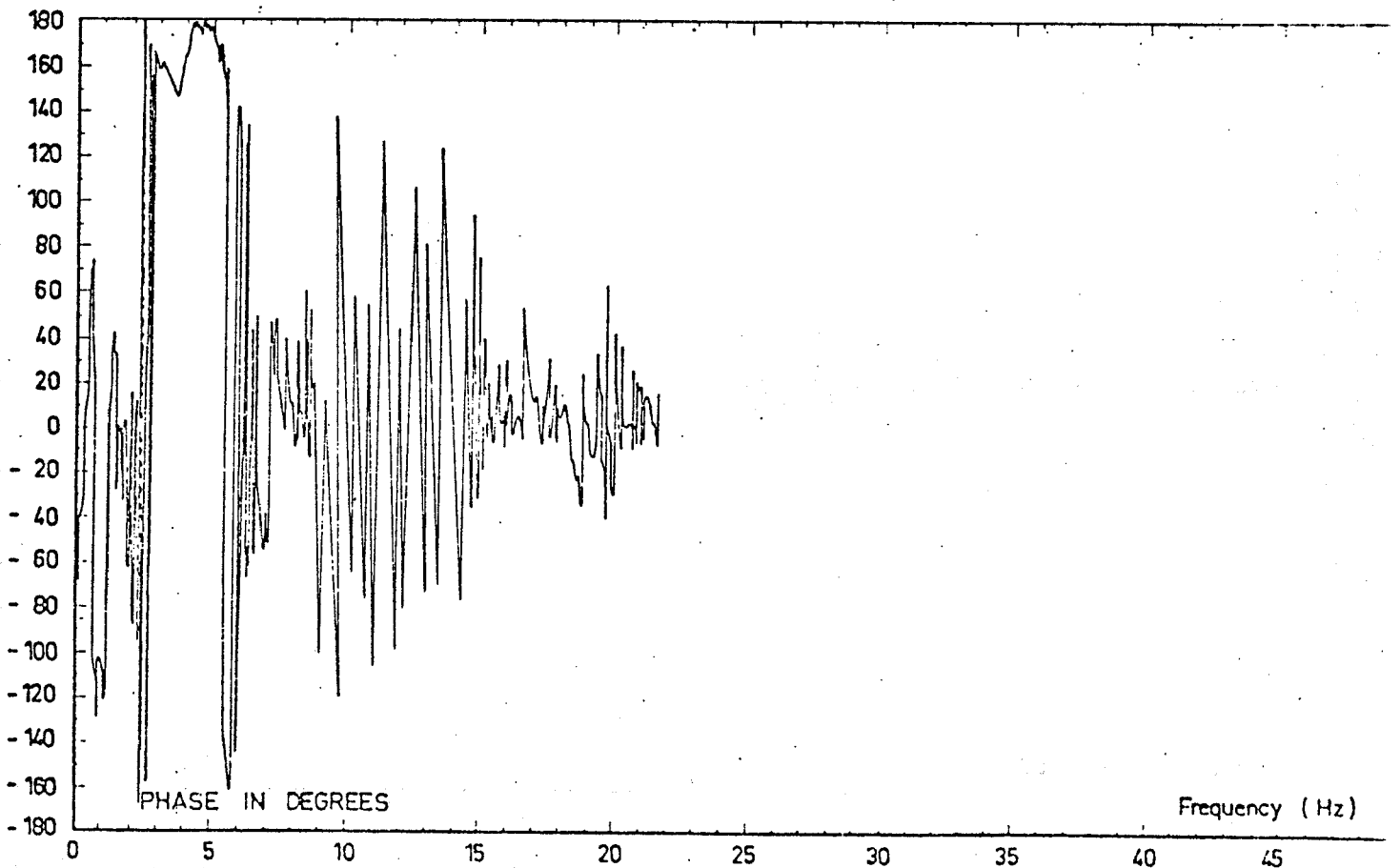
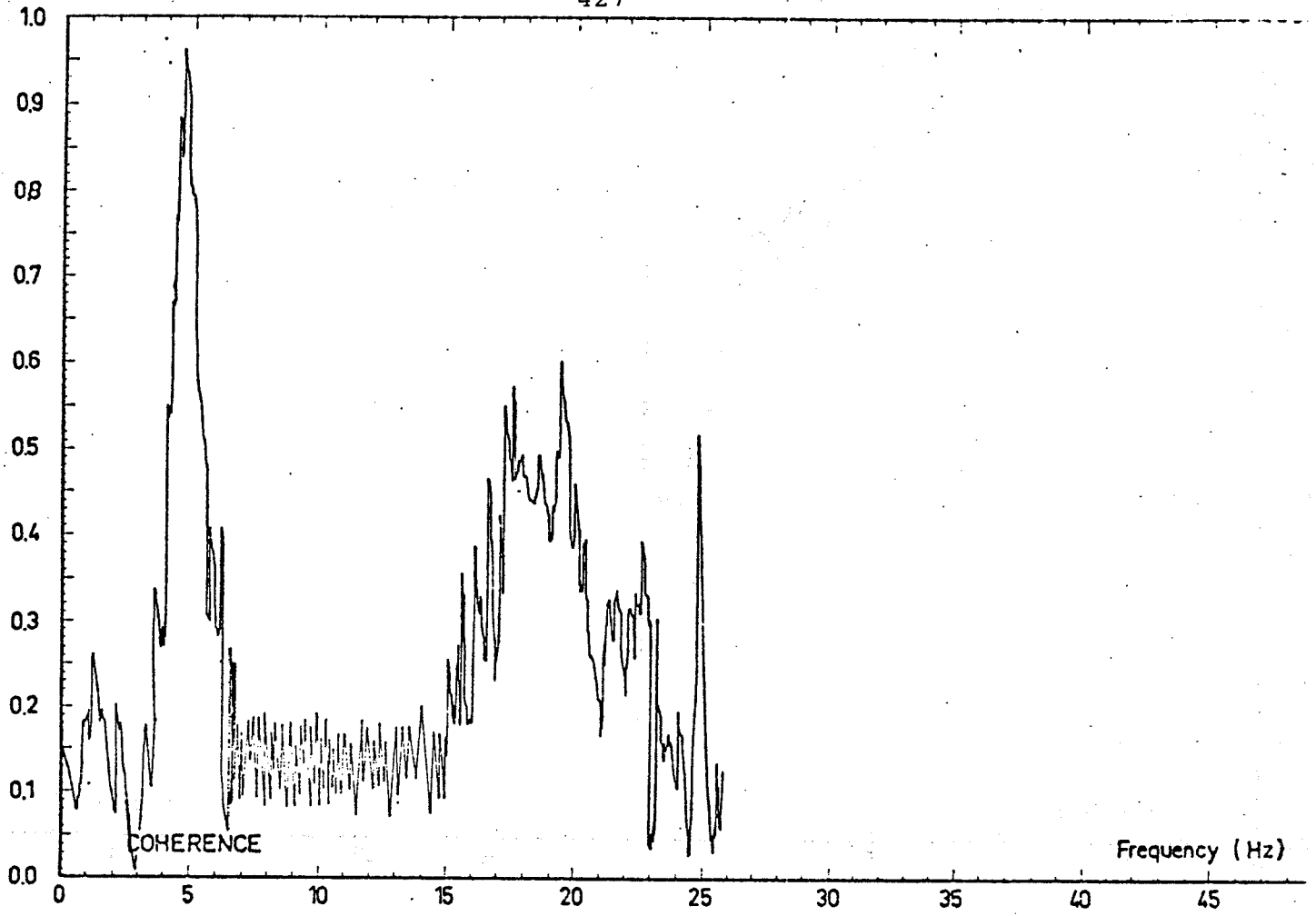


Figure 6 : Coherence and phase for two opposite detectors on the reactor of CRR

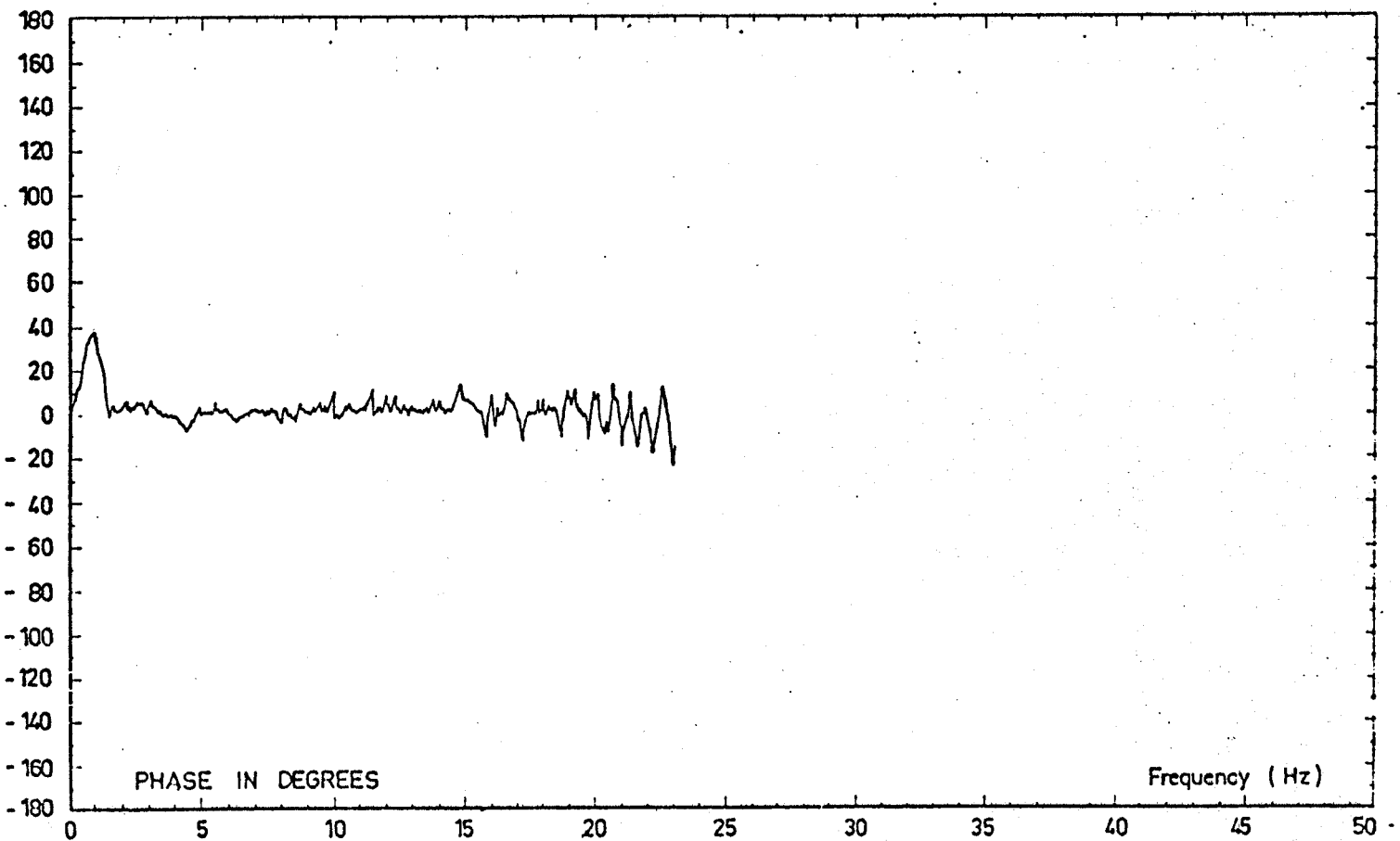
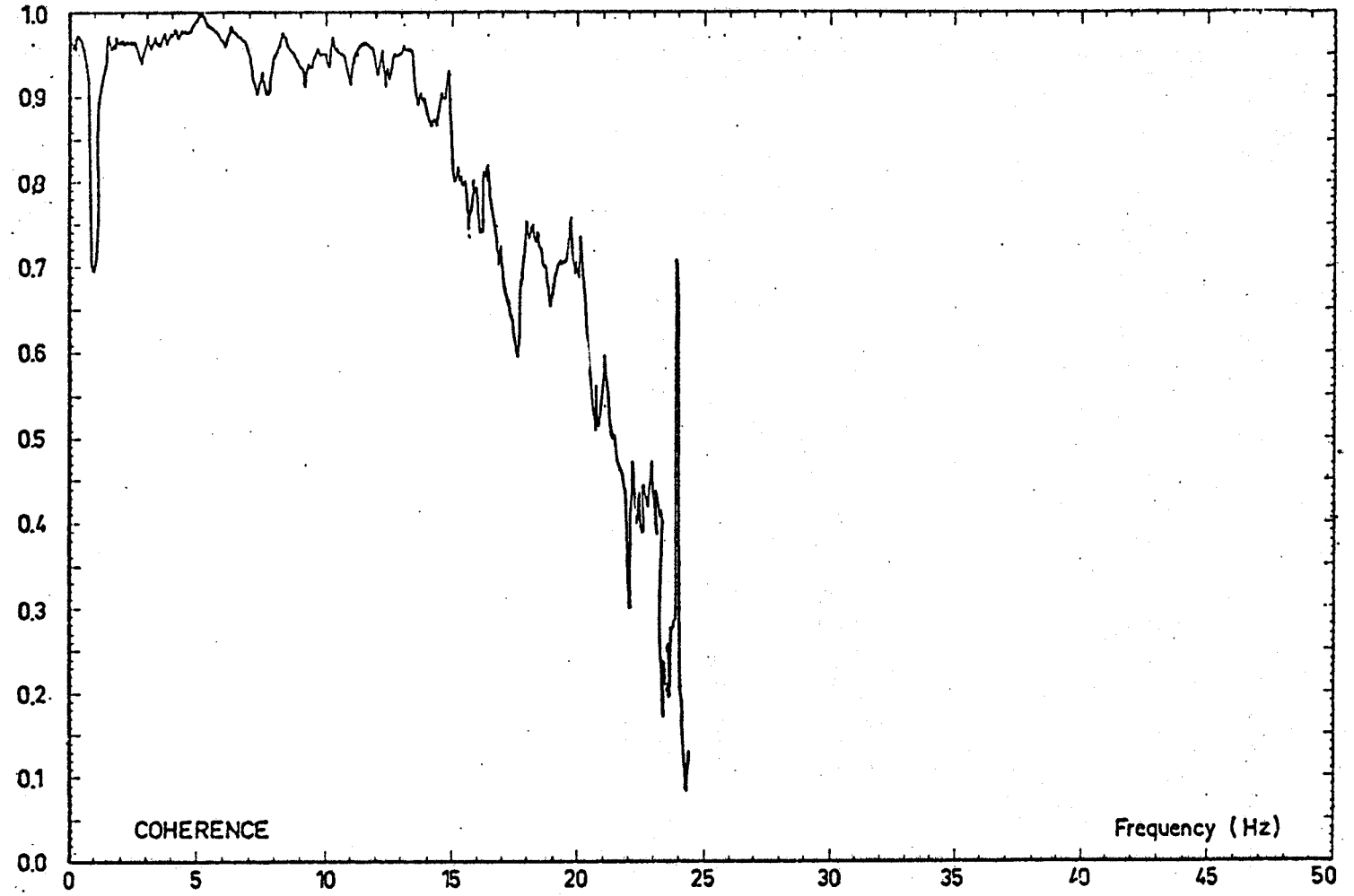


Figure 7 : Coherence and phase for upper and lower part of a detector on the reactor of CHOOZ.

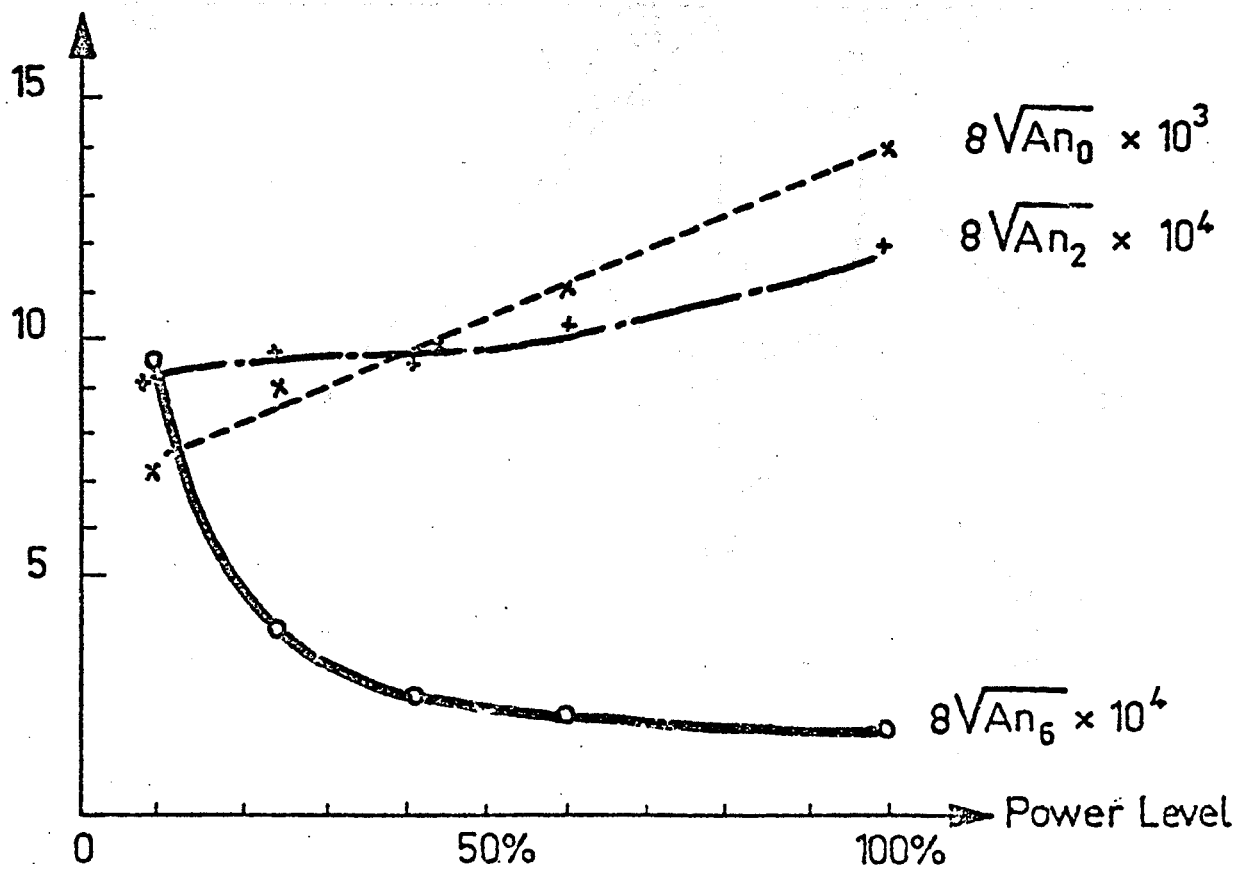
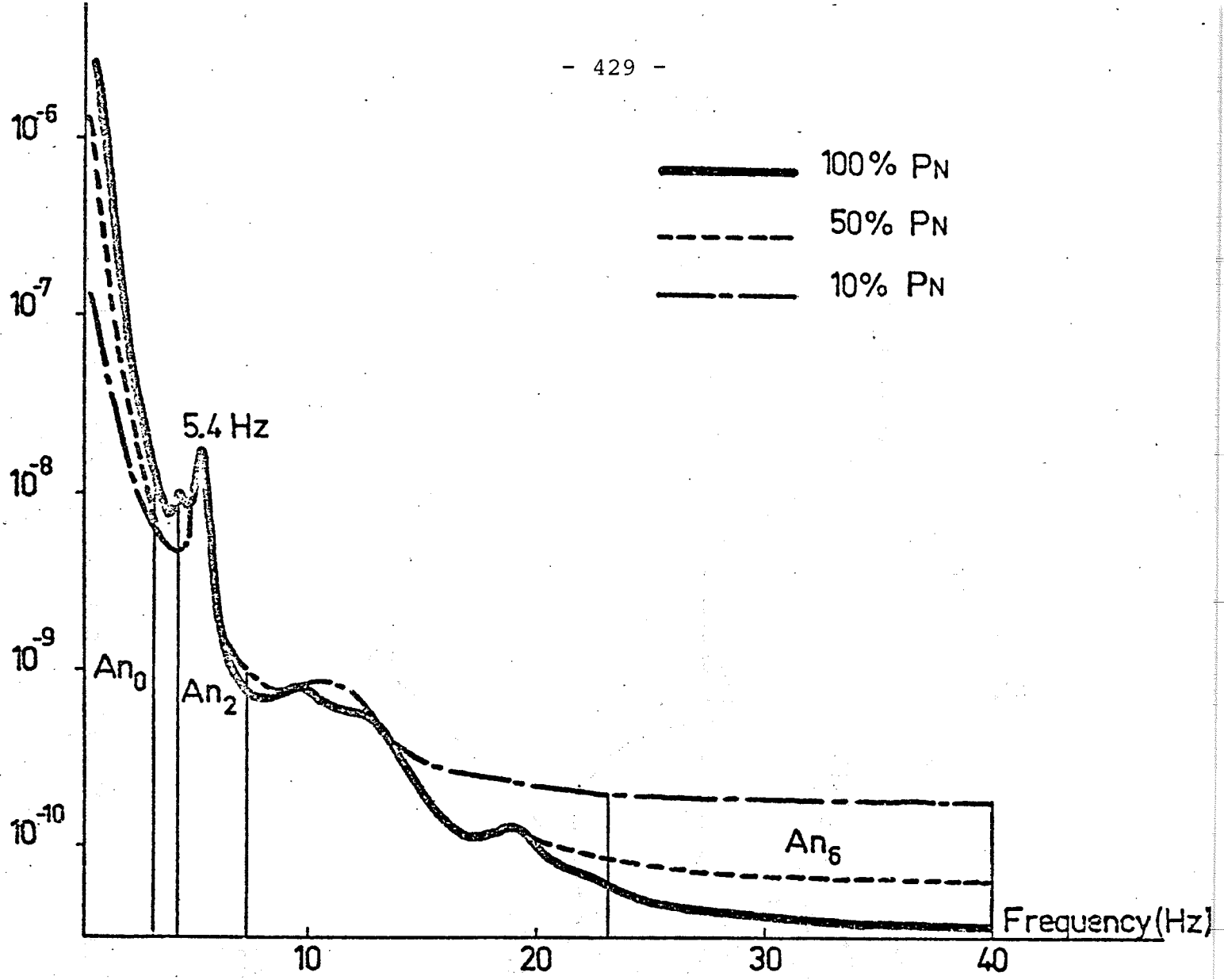


Figure 8 : Evolution of PSD against the power level, on the reactor of CHOOZ

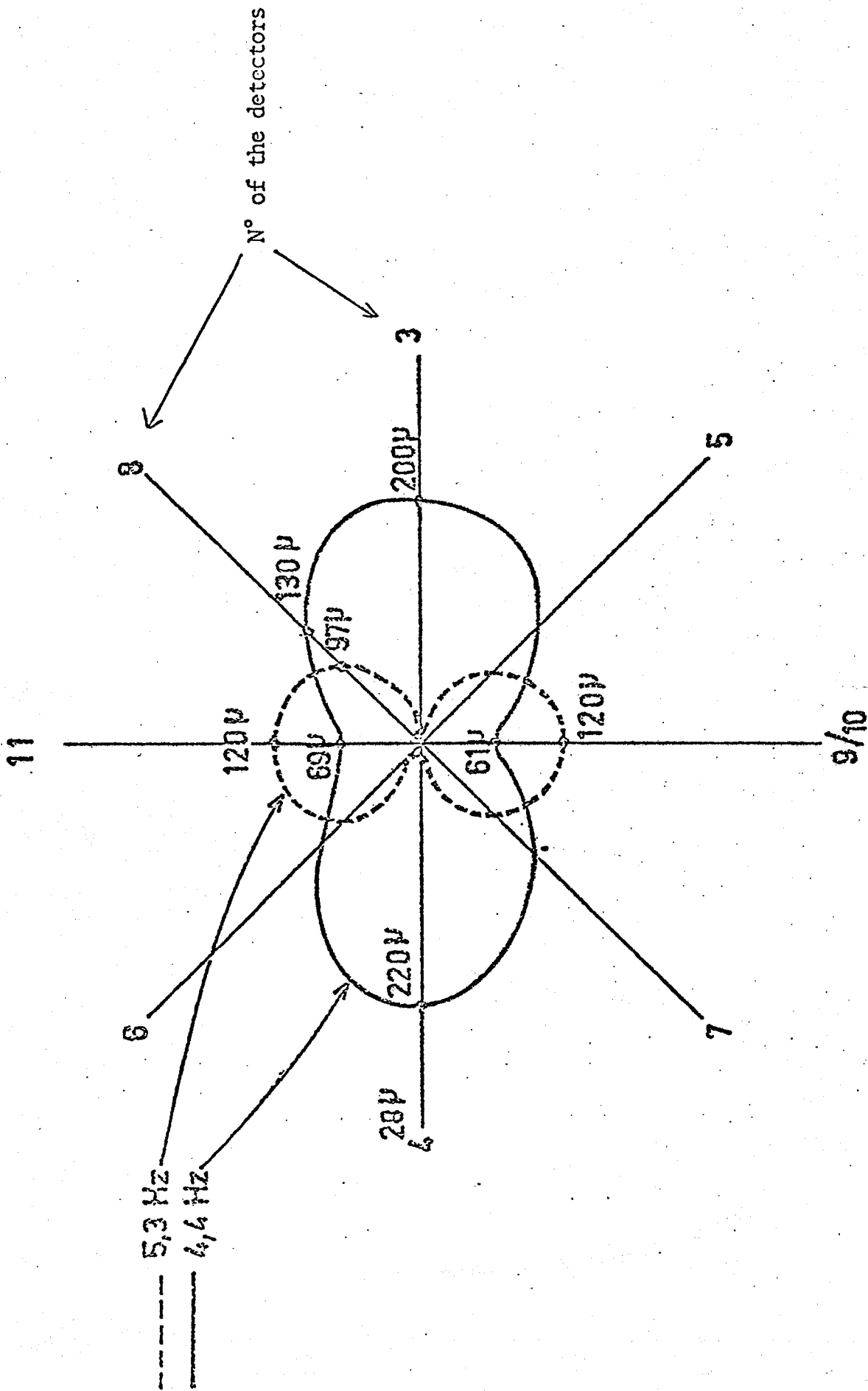


Figure 9 : Amplitude of displacements versus direction of detectors on the reactor of CHOOZ

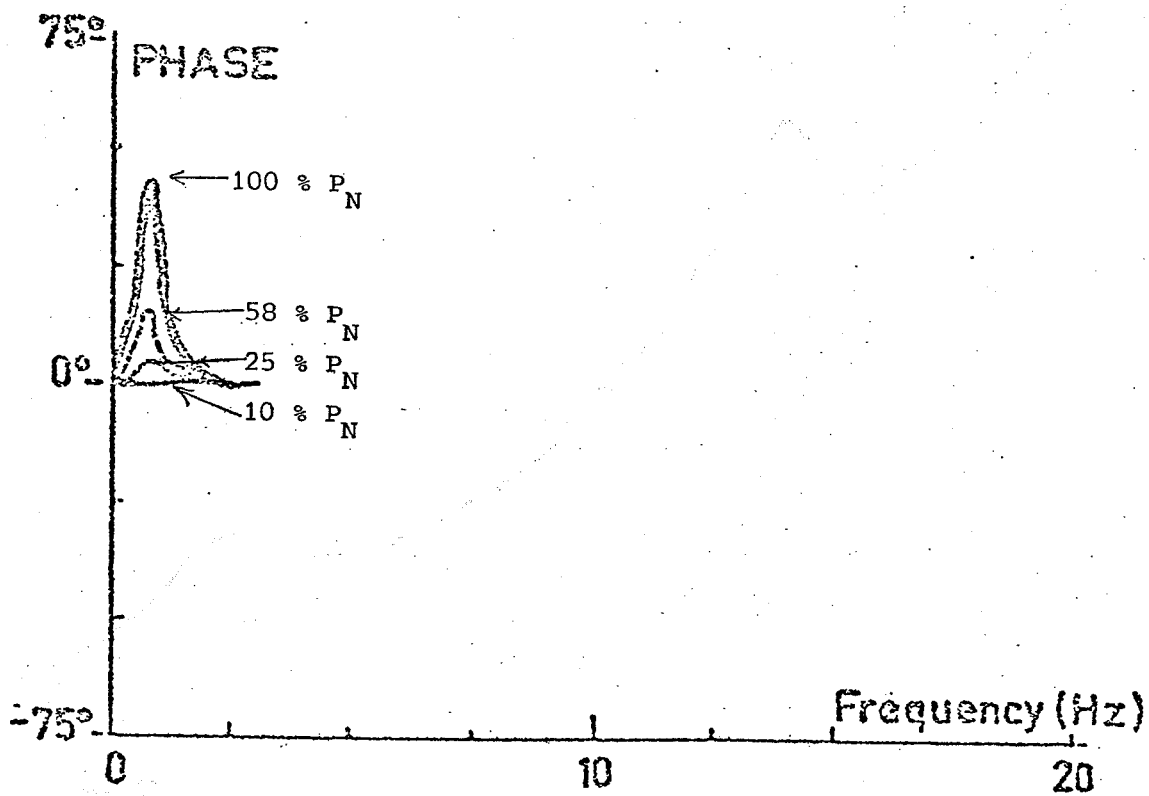
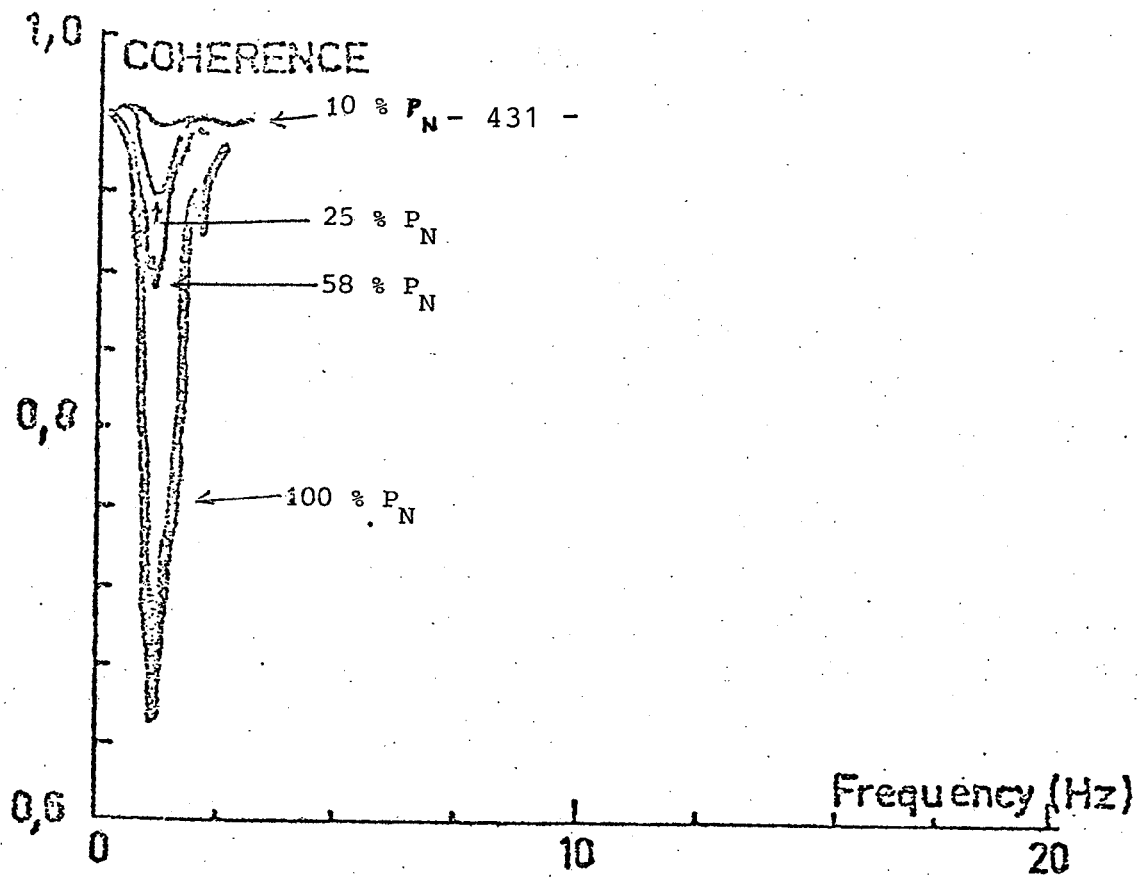


Figure 10 : Evolution of coherence and phase of upper and lower part of a detector, against the power level, on the reactor of CHCOZ.

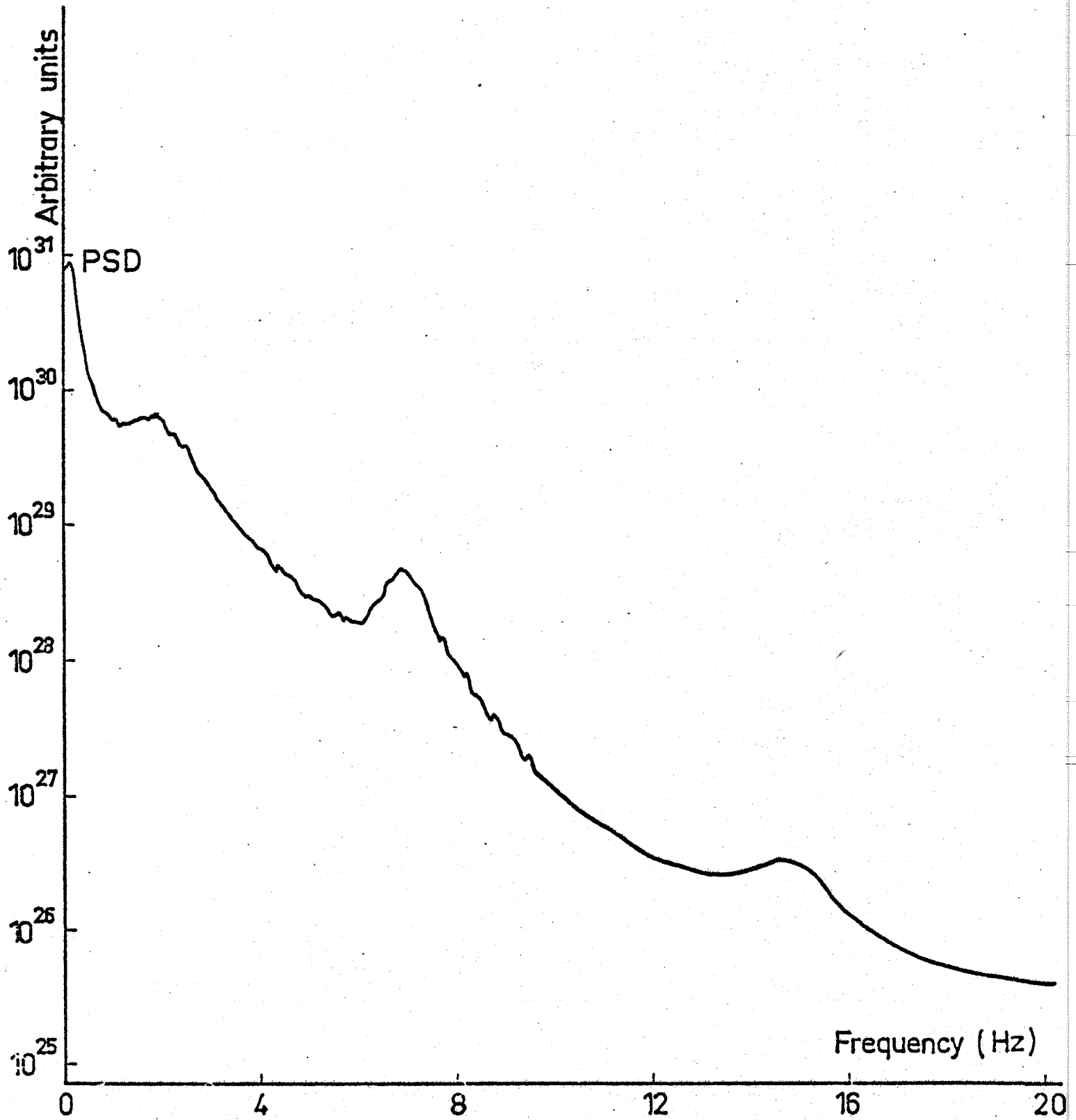


Figure 11 : PSD of an excore detector on the C A P.

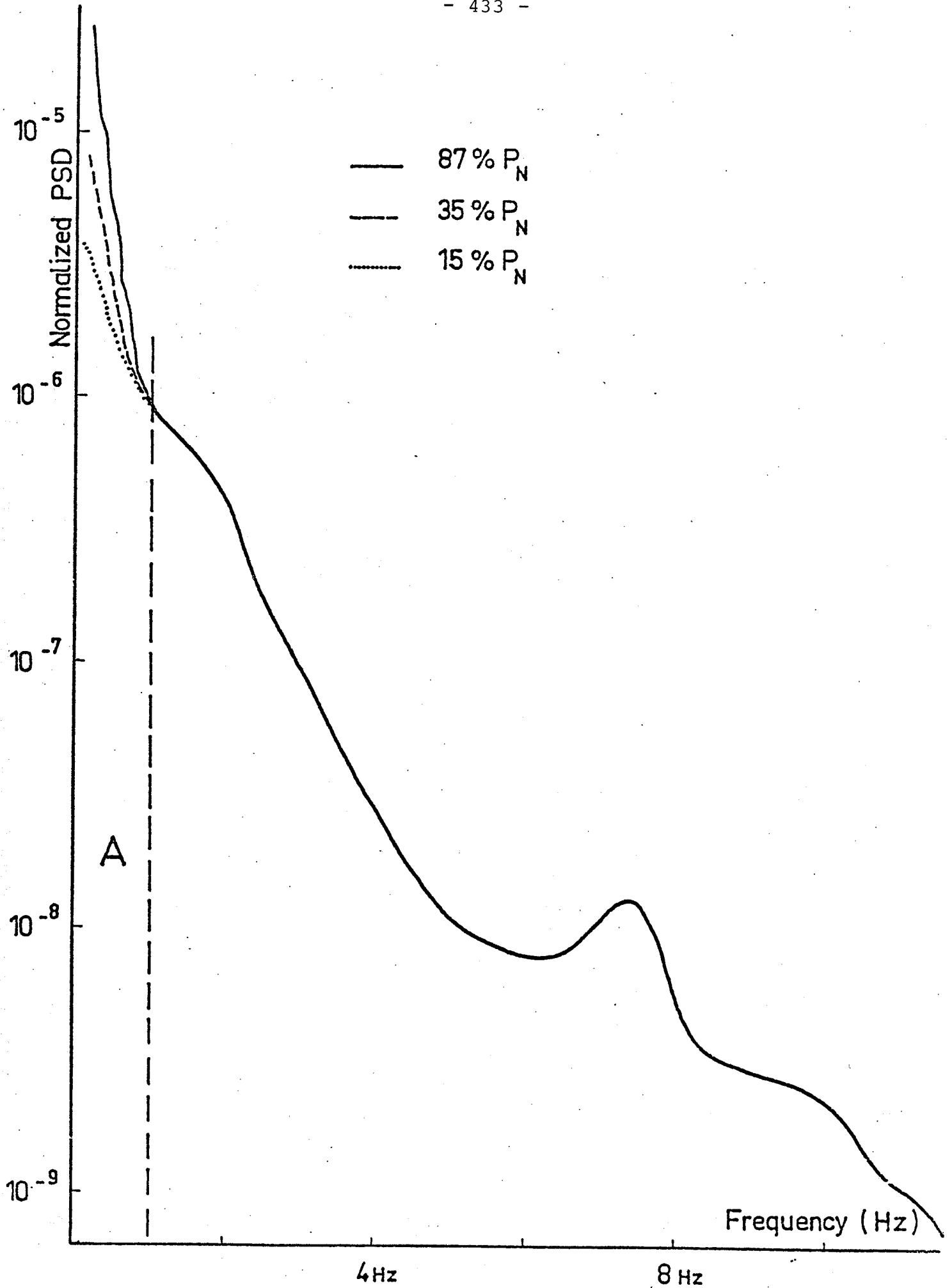


Figure 12 : Evolution of the PSD of a neutron detector against the power level, on the C A P.

C_{12} : Coherence for the detectors 1 and 2
 $C_{2,3}$: " " " 3 and 4
 φ_{12} : Phase of the PSD for the detectors 1 and 2 (in degrees)
 φ_{34} : " " " 3 and 4 (in degrees)

(Opposite detectors : 1 - 2)
 3 - 4) I FSH 1

 I FSH 2

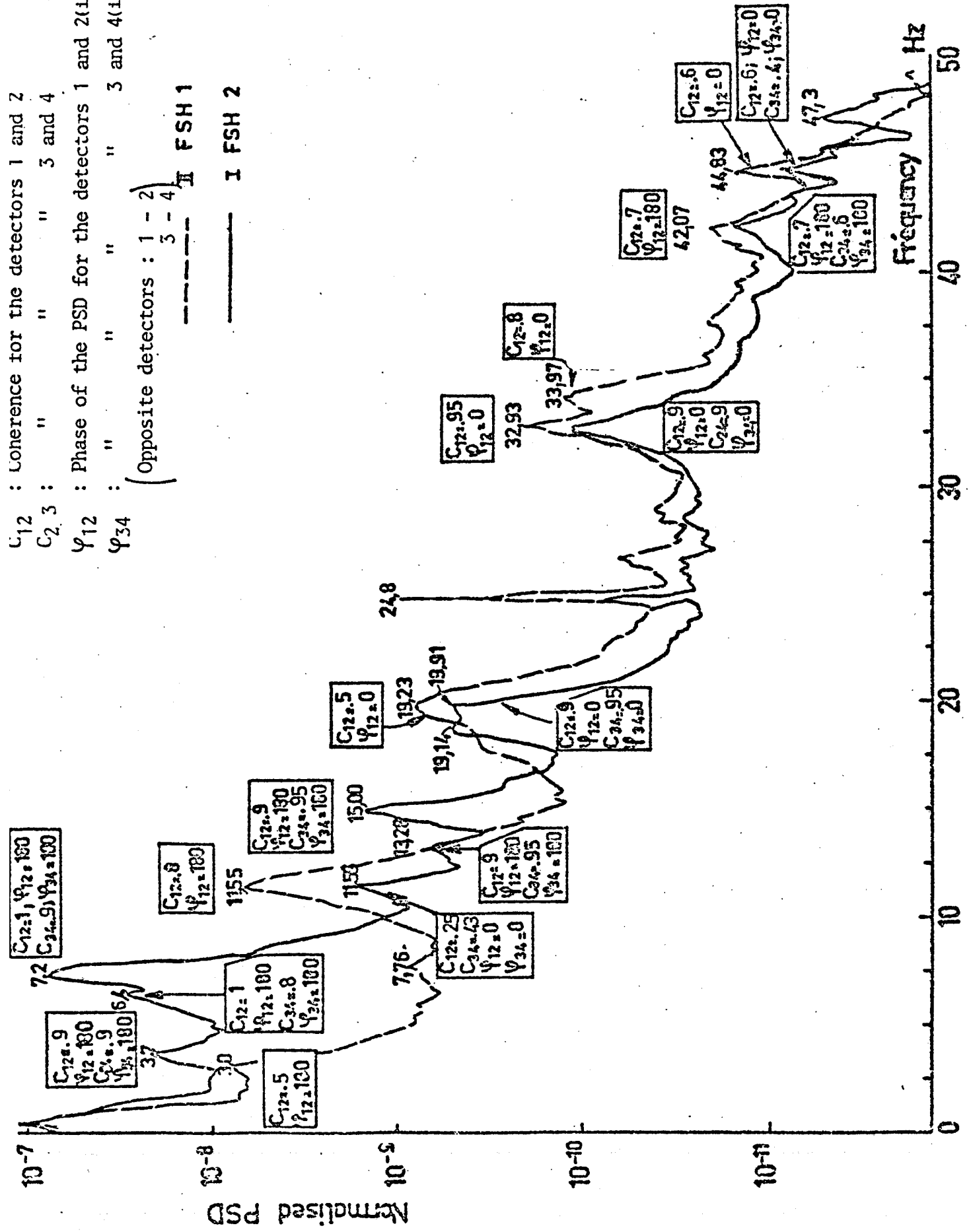


Figure 13: Compared PSDs of excore ion chambers on the reactor of FESSENHEIM 1 and 2.

FESSENHEIM I

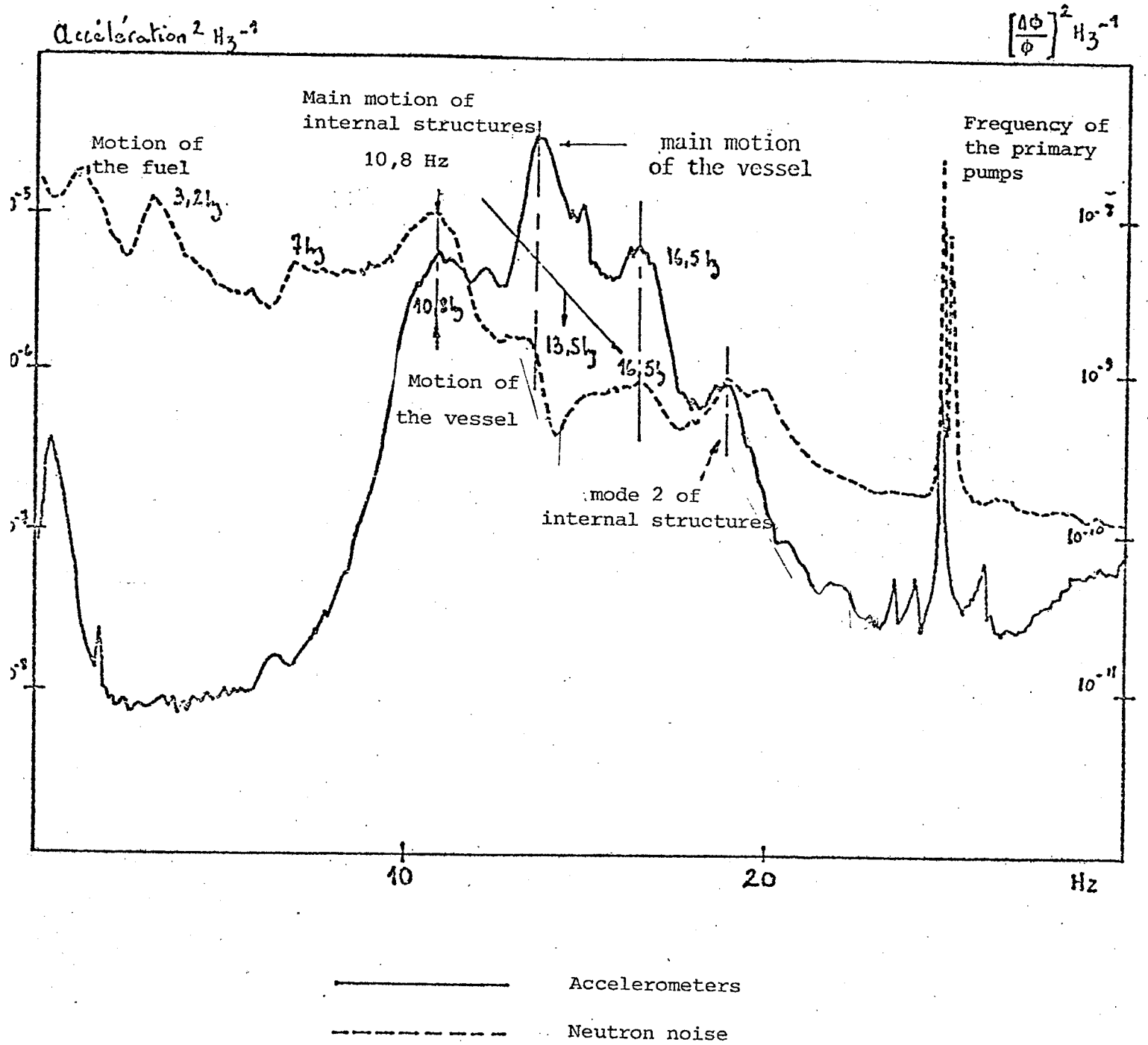


Figure 14 : FESSENHEIM I : comparison of PSD of excore neutron noise and accelerometers on the vessel.

FESSENHEIM 2

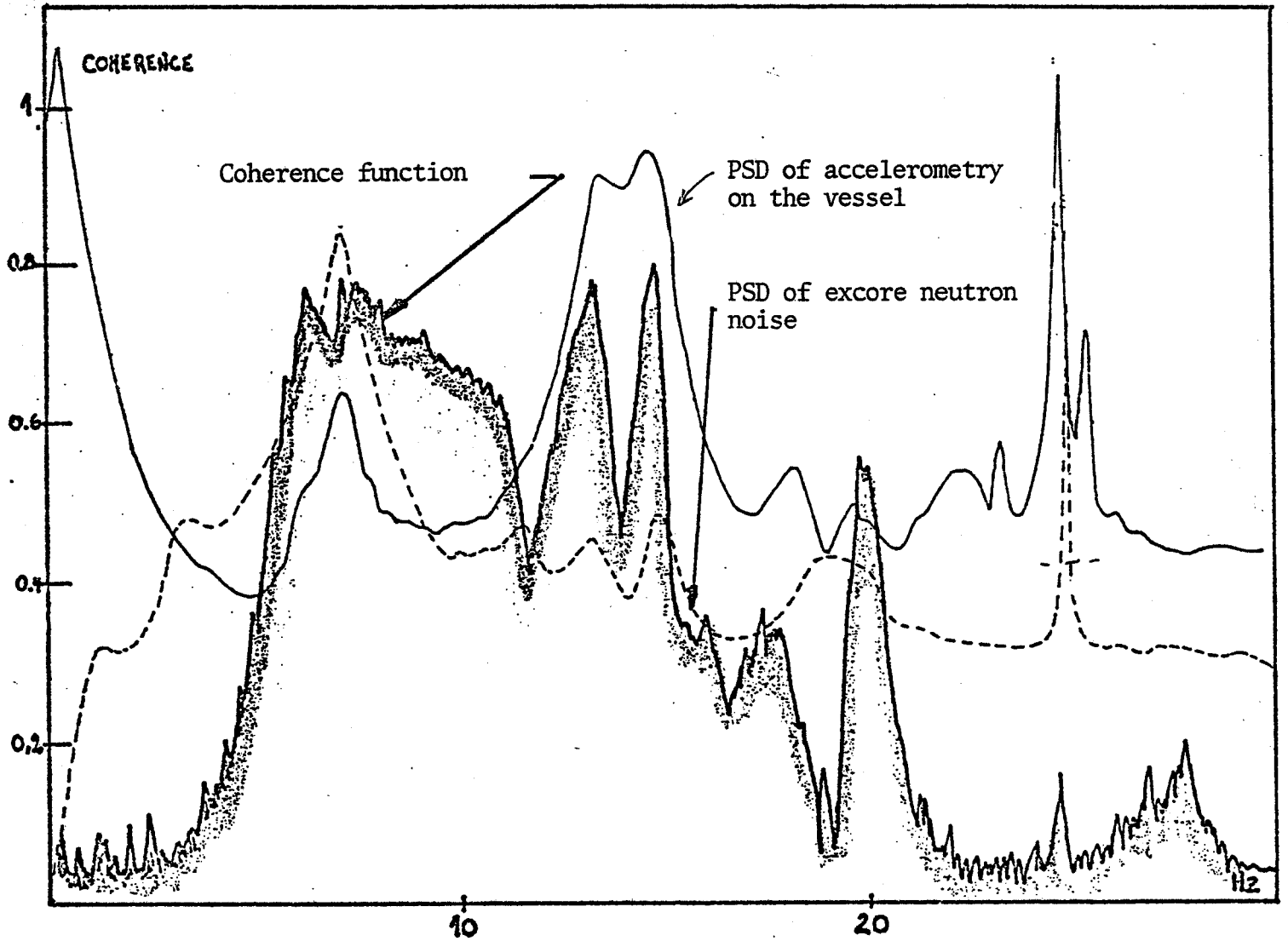


Figure 15 : FESSENHEIM 2. Coherence function between neutron noise and accelerometers.

FESSENHEIM 2

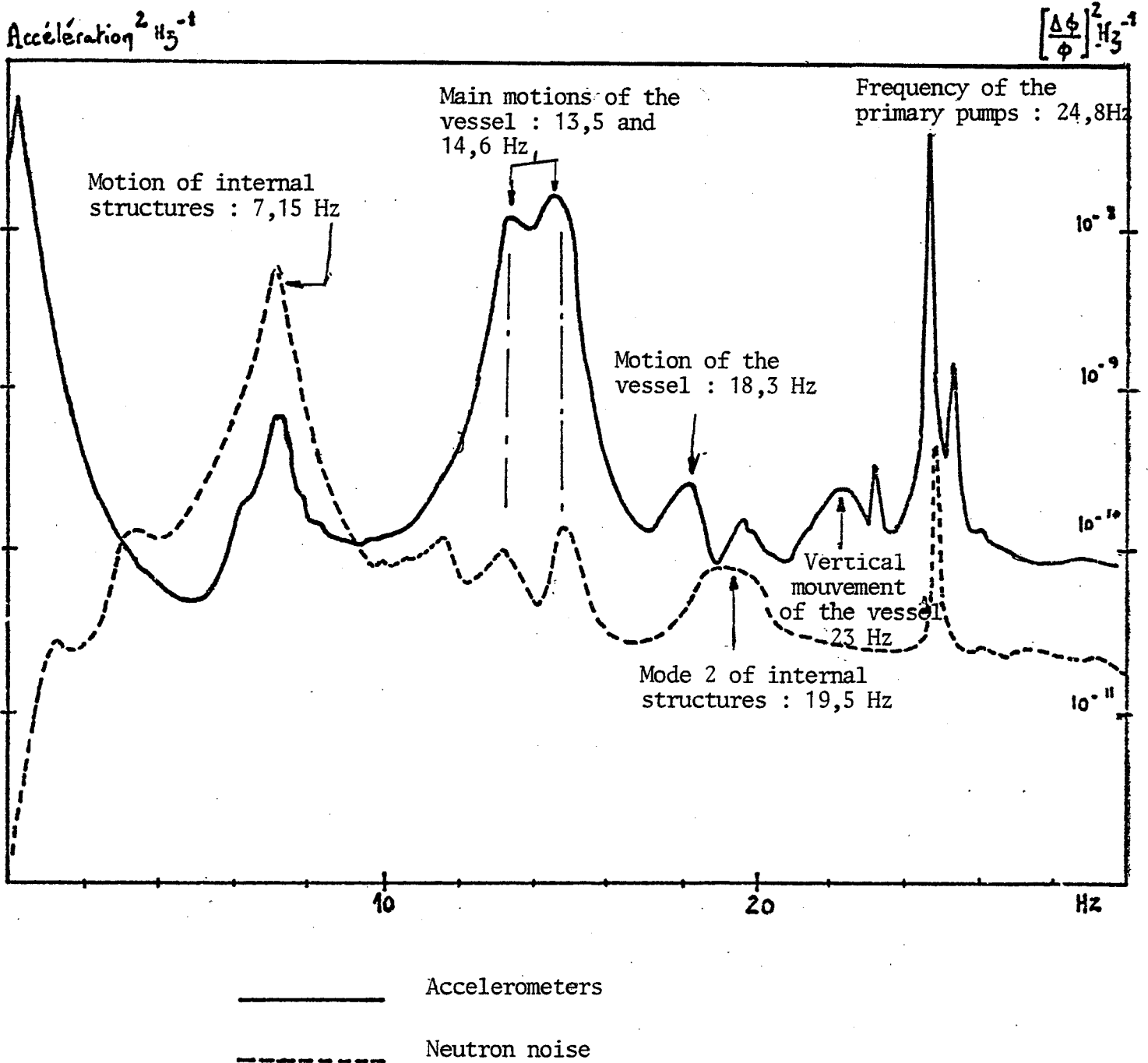


Figure 16 : FESSENHEIM 2. Comparison of PSD of excore neutron noise and accelerometers on the vessel.

G. Zwingelstein, M. Déat, Le Guillou

APPLICATION OF PATTERN RECOGNITION TECHNIQUES TO THE DETECTION
OF THE PHENIX REACTOR CONTROL RODS VIBRATIONS

IAEA-NPPCI-MEETING "PROCEDURES AND SYSTEMS FOR ASSISTING AN
OPERATOR DURING NORMAL AND ANOMALOUS NUCLEAR POWER PLANT OPERATION SITUATIONS"
IN MUNICH
5.-7. DEC.1979

APPLICATION OF PATTERN RECOGNITION TECHNIQUES TO THE
DETECTION OF THE PHENIX REACTOR CONTROL RODS VIBRATIONS

Zwingelstein G^{*}, Déat M^{*}, Le Guillou^{**}
French Atomic Energy Commission
Saclay ^{*}, Cadarache^{**}, FRANCE

APPLICATION OF PATTERN RECOGNITION TECHNIQUES TO THE DETECTION
OF THE PHENIX REACTOR CONTROL RODS VIBRATIONS

Zwingelstein G*, Déat M*, Le Guillou G**
French Atomic Energy Commission
Saclay*, Cadarache**, FRANCE

ABSTRACT

The incipient detection of control rods vibrations is very important for the safety of the operating plants. This detection can be achieved by an analysis of the peaks of the power spectrum density of the neutron noise. Pattern Recognition techniques were applied to detect the rod vibrations which occurred at the fast breeder Phenix (250MWe).

In the first part we give a description of the basic pattern which is used to characterize the behavior of the plant. The pattern is considered as column vector in n dimensional Euclidian space where the components are the samples of the power spectral density of the neutron noise.

In the second part, a recursive learning procedure of the normal patterns which provides the mean and the variance of the estimates is described.

In the third part the classification problem has been framed in terms of a partitioning procedure in n dimensional space which encloses regions corresponding to normal operations.

This pattern recognition scheme was applied to the detection of rod vibrations with neutron data collected at the Phenix site before and after occurrence of the vibrations.

The analysis was carried out with a 42-dimensional measurement space. The learned pattern was estimated with 150 measurement vectors which correspond to the period without vibrations. The efficiency of the surveillance scheme is then demonstrated by processing separately 119 measurement vectors recorded during the rod vibration period.

INTRODUCTION

During the past decade an extensive effort was made in the field of nuclear energy to develop methods able to achieve the surveillance and the diagnostic of the components of nuclear plants. The surveillance problem consists in classifying the operating modes in two classes : normal and abnormal. The diagnostic problem needs the identification of the causes of abnormality. This paper will be focused mainly on the resolution of the surveillance problem based on pattern recognition techniques. Pattern recognition techniques are widely applied to detect incipient failure of nuclear reactor components [1] - [4]. A surveillance system based on such a technique is reduced to characterize normal behavior and then to evaluate limits for abnormality.

Noise analysis techniques are applied to extract information from signal fluctuations. It could be shown that main failures detected on nuclear plants, such as loss of core mechanical integrity, loss of fuel element cooling or control rod drive mechanism failure induce changes in the random fluctuations of the neutron flux, coolant flow, pressure and displacement sensors.

The aim of this paper is to develop a method able to provide assistance to plant operators after a convenient data reduction and data processing. The method proposed utilizes results obtained by Piety [5]. The basic pattern is considered as column vector in an n -dimensional Euclidian space where the components are the samples of the power spectral density of the neutron noise. A recursive learning procedure of the normal pattern was chosen to estimate the mean and the variance of the normal pattern. The classification problem has been framed in terms of partitionning procedure in n -dimensional space and hyperellipsoids were retained as the partitionning surfaces. The original pattern is transformed by a change of coordinates defined by the eigenvalues of the covariance matrix. A statistical measure of distance is then defined to separate normal and abnormal patterns. Finally the method establishes alarm thresholds in accordance with false alarm criteria determined by the plant operator.

The performance of the pattern recognition method was evaluated with neutron noise data recorded at the Phenix plant to detect the malfunction of one control rod. As it will be demonstrated, the influence of this failure was not able to be detected by the instrumentation installed at the plant.

PROBLEM FORMULATION

The aim of this study was the development of a surveillance method which utilizes noise analysis techniques and which can be implemented on a mini-computer. Figure 1 represents the block diagram of the surveillance system based on pattern recognition techniques. The raw data conditioned first by the data acquisition system, are processed to construct the pattern. For the Phenix data, the processor is based on the Fourier analysis and a Fast Fourier Transform algorithm provides the discrete power density function : $A(f_i)$, $i = 1 \dots n$, where $f_1 \dots f_n$ are frequencies uniformly distributed in the interval (0 - 16 Hz). The pattern which characterizes the behavior of the plant is represented by an n -dimensional column vector denoted X , where the components are the $A(f_c)$. The output of this processor is then fed into the pattern recognition system in order to verify the normality of the updated computed pattern

The remainder of this paper is devoted to the description of the design of the pattern recognition system. The first task of the system is to learn the parameters which represent the normal behavior of the nuclear plant. This must be done automatically without operator assistance.

Once the initial learning is completed, the new patterns are analyzed to detect significant changes in the data characteristics during the pattern recognition step. A message of abnormality will be automatically displayed to the operator, according to an a priori false alarm probability criterion.

LEARNING PROCEDURE

The learning procedure is undertaken before the recognition step. During an observation period, the surveillance system learns what is the normal behavior by an analysis of the noise characteristics. This analysis leads to a statistical description of its normal behavior. For the Phenix case a recursive algorithm was applied to evaluate the mean and the covariance matrix of the learned pattern. The procedure is the following :

Let N be the number of spectra evaluated with the Fast Fourier Transform algorithm and $X_K = [x_{1k}, x_{2k}, \dots x_{nk}]$, the vector number K .

The mean vector M_{k+1} after $k+1$ computations is given by :

$$M_{k+1} = M_k + \frac{1}{k+1} [X_{k+1} - X_k]$$

The covariance matrix C_{k+1} of the $(k+1)$ vectors is evaluated by :

$$C_{k+1} = \frac{1}{k+1} [X_{k+1} - M_{k+1}] [X_{k+1} - M_{k+1}]^T + \frac{k}{k+1} [C_k - X_{k+1} X_{k+1}^T]$$

The knowledge of M_n and C_n will be later used to check the Gaussian distribution of the set of observed vectors. After this observation period which yields the learned pattern, two procedures can be used. The first procedure, referred to as the supervised learning procedure does not take into account any extra data to improve the learned pattern. The second procedure, called adaptative learning method, is updating the learned pattern every time a new normal pattern is detected. The first procedure only is considered in this study. Once this learning period is completed the surveillance system monitors the new observed set of data and indicates the occurrence of an anomaly.

PATTERN RECOGNITION PROCEDURE

This procedure will serve to determine if a new observed pattern corresponds to a normal or abnormal behavior. Simple and sensitive recognition schemes have to be designed to achieve rapidly the surveillance. To solve the specific problem of the Phenix control rod vibration, the classification problem of the pattern was solved by considering a region in n -dimensional space. To characterize the domain of normality, hyperellipsoïdes were chosen as particular surfaces. These surfaces are constructed with the initial vector X_k and have for equation :

$$(X_k - M_N)^T C_N^{-1} (X_k - M_N) = G_k^2$$

where M_N is the mean vector estimated during the learning period, and C_N is the associated covariance matrix.

The value of the constant G_k^2 determines the volume enclosed inside the surface. The eigenvectors and eigenvalues of the covariance matrix C_N give respectively the principal axes of the hyperellipsoïdes and the variances along the axes. The recognition procedure consists in determining the average volume characterizing the normal behavior and in checking if a given vector X_k is inside the hyperellipsoïd.

The pattern recognition problem can be interpreted as a measure of similarity between surfaces. In particular, the value G_k can be interpreted as a measure of the distance between the mean vector M_N and the observed X_k . In practice, as shown by Piety [5], the original Euclidean space is not the optimal space since the covariance matrix is not diagonal and consequently the elements of vector X_k may be correlated. In order to decorrelate the components of a vector X_k a decoupling transformation matrix ϕ is suggested, such as X_k is transformed into Y_k as $Y_k = \phi X_k$.

If the rows of ϕ are normalized eigenvectors of the covariance matrix C_N , the transformed covariance matrix \hat{C}_N of the transformed vector Y_k is a diagonal matrix whose elements \hat{C}_{kj} represent the variances $\hat{\sigma}_{kj}^2$ along the transformed coordinate direction. This result is valid only when the data are Gaussian and a statistical test has to be made to verify this property. An interesting result associated with the decoupling transformation is that the volume included in the hyperellipsoids remains identical :

$$(X_k - M_N)^T C_N^{-1} (X_k - M_N) = (Y_k - \hat{M}_N)^T \hat{C}_N^{-1} (Y_k - \hat{M}_N) = G_k^2$$

where \hat{M}_N represents the mean vector of Y_k , $k = 1 \dots N$
 \hat{C}_N is the covariance matrix of Y_k .

G_k^2 can also be expressed by : $(X_k - M_N)^T \phi \phi^T (X_k - M_N)$

Moreover, if the initial data set is Gaussian the transformed data set is also Gaussian. This hypothesis was tested for the Phenix case by using the Kolmogorov-Smirnov goodness-of-fit test. In practice, the Gaussian hypothesis was tested by checking that the variable Z defined by :

$$Z = (X - M_N)^T C_N^{-1} (X - M_N)$$

is a random variable having a distribution function of a Chi-Square variate with n degrees of freedom (n : number of components of vectors Y_k and X_k). One sample of the Kolmogorov-Smirnov variable is expressed by :

$$D = \max_Z |F_N(Z) - F(Z)|$$

D is the maximum of the differences between the postulated and measured distribution functions, $F_N(Z)$ is the calculated distribution function of Z , $F(Z)$ is the Chi-Square distribution function of a variable with n degrees of freedom.

The Kolmogorov-Smirnov goodness-of-fit test considers that the hypothesis that the sample set is governed by the assumed density function is true if $D < D(\alpha, N)$, where α is the significance level. The values of $D(\alpha, N)$ such as $P(D > D(\alpha, N))$ are tabulated for various values of N and α in [6].

The surveillance problem consists in determining if a particular measurement belongs to the mean of the data set. This is accomplished by calculating the term G_k^2 and the decision is made by comparing the value obtained to a preassigned threshold S_0 . The determination of a value S_0 for a specified false alarm probability, requires in the general case the exact knowledge of the probability density function of Z . For an n -variate Gaussian distribution with known mean vector M_N and covariance matrix C_N , the variable $Z = (X_k - M_N)^T C_N^{-1} (X_k - M_N)$ is a Chi-Square variate with n degrees of freedom. Let α be the false alarm probability acceptable for the surveillance system. The hyperellipsoïde specified by :

$$(X_k - M_N)^T C_N^{-1} (X - M_N) = \chi^2 (1 - \alpha)$$

will enclose $100\alpha\%$ of the multivariable population.

For instance, if $n = 40$ and $\alpha = 0.05$, the hyperellipsoïde is defined by $Z = 55.8$.

For a false alarm probability α , the observed pattern X_k will be classified as normal when $Z_k < \chi^2(1 - \alpha)$, otherwise the pattern is considered as non acceptable and an alarm is activated.

APPLICATION TO PHENIX DATA

The performance of the surveillance scheme was evaluated to detect a control rod malfunction which occurred at the Phenix site. This fast breeder sodium cooled reactor has a 250 MWe power. It is located in Marcoule in the south of France. The raw data are the neutron fluctuation given by the neutron detector. These fluctuations were amplified and recorded on an analog tape recorder to be processed off-line on the surveillance system, implemented on a minicomputer. Two sets of signals were recorded on the plant : the first set corresponds to the normal behavior of a control rod, the second set was observed after the failure of a control rod.

The power spectral density was computed with and without failure. The set of power density spectra without anomaly constituted the learning set and 150 PSDs were evaluated during this learning period. The abnormal set of PSDs contained 119 PSDs. Each pattern X_k was formed by a vector with 42 components from 0.4 Hz to 16.8 Hertz at 0.4 Hz interval.

Figure 2 represents the 30 first normal PSDs. Figure 3 shows the 30 first abnormal PSDs. These two plots demonstrate that it is impossible to visually detect an abnormality and consequently a pattern recognition scheme must be used. The surveillance system was first trained with 150 PSDs and in figure 4 the shape of the mean vector is represented. The covariance matrix C_{150} was recursively computed according to the procedure described previously. The Kolmogorov-Smirnov goodness-of-fit test was applied to check the Gaussian properties of the data. The histogram of the density probability function of Z was evaluated and is plotted in figure 5.

Table 1 gives the theoretical and computed repartition of the Chi-Square variable with 42 degrees of freedom and the absolute value of the difference $|F_N(Z) - F(Z)|$

χ^2	F	$F_N(Z)$	$ F_N(Z) - F(Z) $
22.2	0.005	0.008	3.10^{-3}
23.7	0.01	0.013	3.10^{-3}
26.	0.025	0.0 18	7.10^{-3}
28.2	0.05	0.031	$1.9.10^{-2}$
30.8	0.10	0.082	$1.8.10^{-2}$
35.5	0.25	0.256	6.10^{-3}
41.3	0.50	0.547	3.10^{-3}
47.7	0.75	0.781	$3.1.10^{-2}$
54.	0.90	0.926	$2.6.10^{-2}$
58.1	0.95	0.960	$1.0.10^{-2}$
61.7	0.975	0.991	$1.6.10^{-2}$
66.2	0.99	0.994	4.10^{-3}
6 9.3	0.995	0.995	0

TABLE 1 : Values of F and $F_N(Z)$

To check the pattern normality during the recognition procedure, a false alarm probability was chosen equal to 0.05. The associated threshold S_0 is 58.124 according to the χ^2_{48} (0.95) distribution. In order to obtain a satisfactorily detection rate of the abnormal patterns, it was necessary to compute the average of 5 consecutive Z_k before the comparison to the threshold S_0 . With this procedure among the 23 clustered sets, 4 failed the test and 19 were recognized as abnormal. With a false alarm probability equal to 0.1 all the patterns passed the test. The relative low sensibility of the surveillance scheme can be explained by the fact that the normal and abnormal patterns are very close together as it can be seen in figure 6 which represents the mean vectors for the normal and abnormal case.

The surveillance scheme and the associated algorithms were implemented on a 16 bit standard mini computer SOLAR 16-40 having 32 K memory size.

CONCLUSION

The experimental results obtained by the surveillance system with data collected at the Phenix site shows that pattern recognition techniques can be used to detect satisfactorily an abnormal behavior of a plant. In addition the surveillance can be easily implemented on a minicomputer.

Future work will test a larger data base in order to increase the sensitivity of the surveillance system. In addition, a portable surveillance system will be develop around a Hewlett Packard 9845 system coupled to an FFT analyzer.

REFERENCES

- [1] R.C. Gonzalez, D.N. Fry, and R.C. Kryter
"Results in the Application of Pattern Recognition Methods to Nuclear Reactor Core component Surveillance" - IEEE Trans. Nucl. Sci. 21 (1), 750-756 (1974)
- [2] J.A. Thie, "Reactor-Noise Monitoring for Malfunctions", Reactor Technol. 14 (4), 354-65 (1972).
- [3] D.N. Fry, "Experience in Reactor Malfunction Diagnosis Using On-Line Noise Analysis" - Nucl. Technol. 10, 273-282 (March 1971).
- [4] D.N. Fry, R.C. Kryter and J.C. Robinson, "Analysis of Neutron-Density Oscillations Resulting from Core Barrel Motion in the Palisades Nuclear Power Plant", ORNL-TM-4570 (May 1974).
- [5] K.R. Piety "On line reactor surveillance based on multivariate analysis of noise signal", PH.D. dissertation, University of Tennessee, Knoxville, Tennessee (1976).
- [6] D.B. Owen, Handbook of Statistical tables - Pergamon Press, 1962.

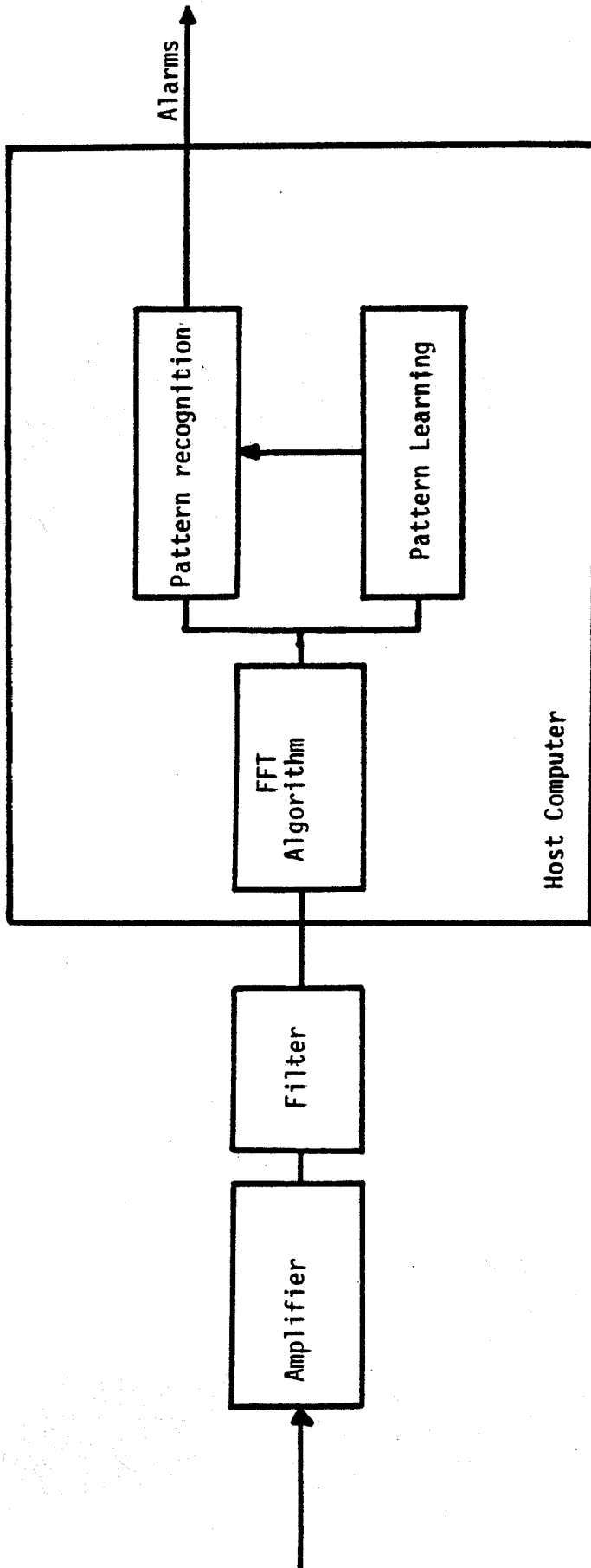


FIGURE 1 : DIAGRAM OF THE SURVEILLANCE SYSTEM

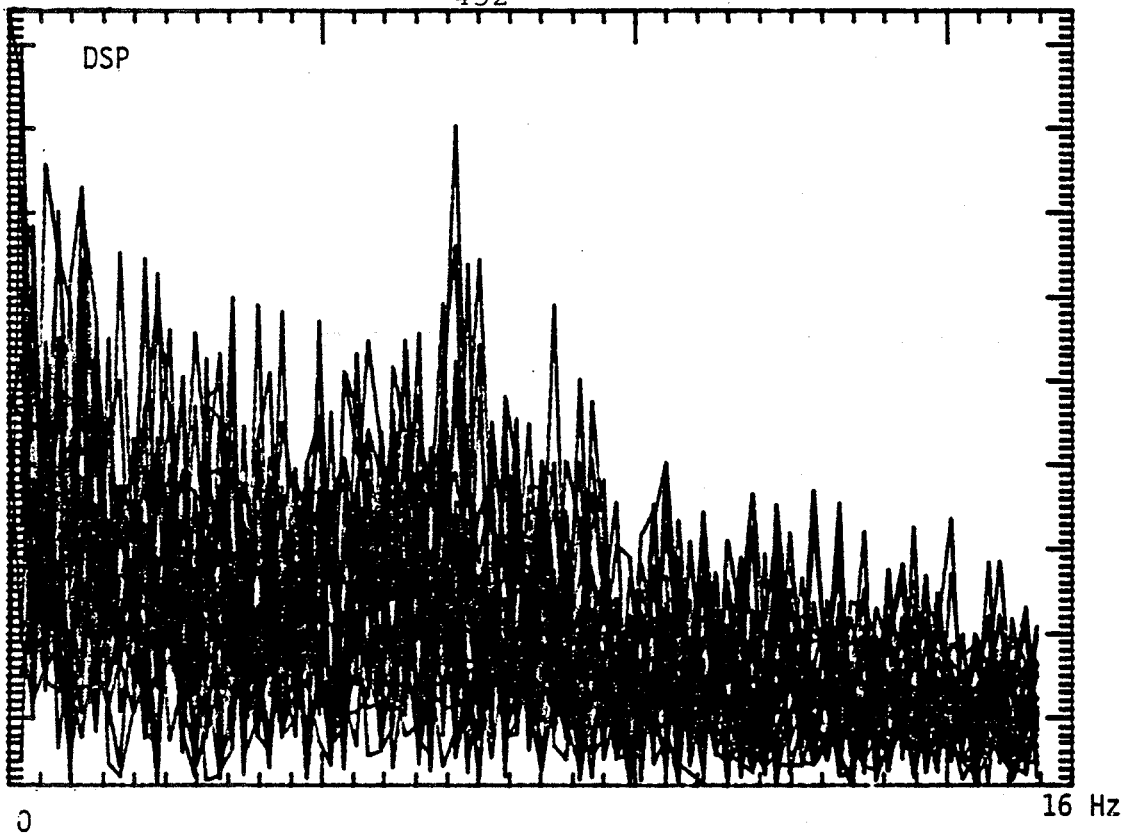


FIGURE 2 : 30 NORMAL SPECTRA

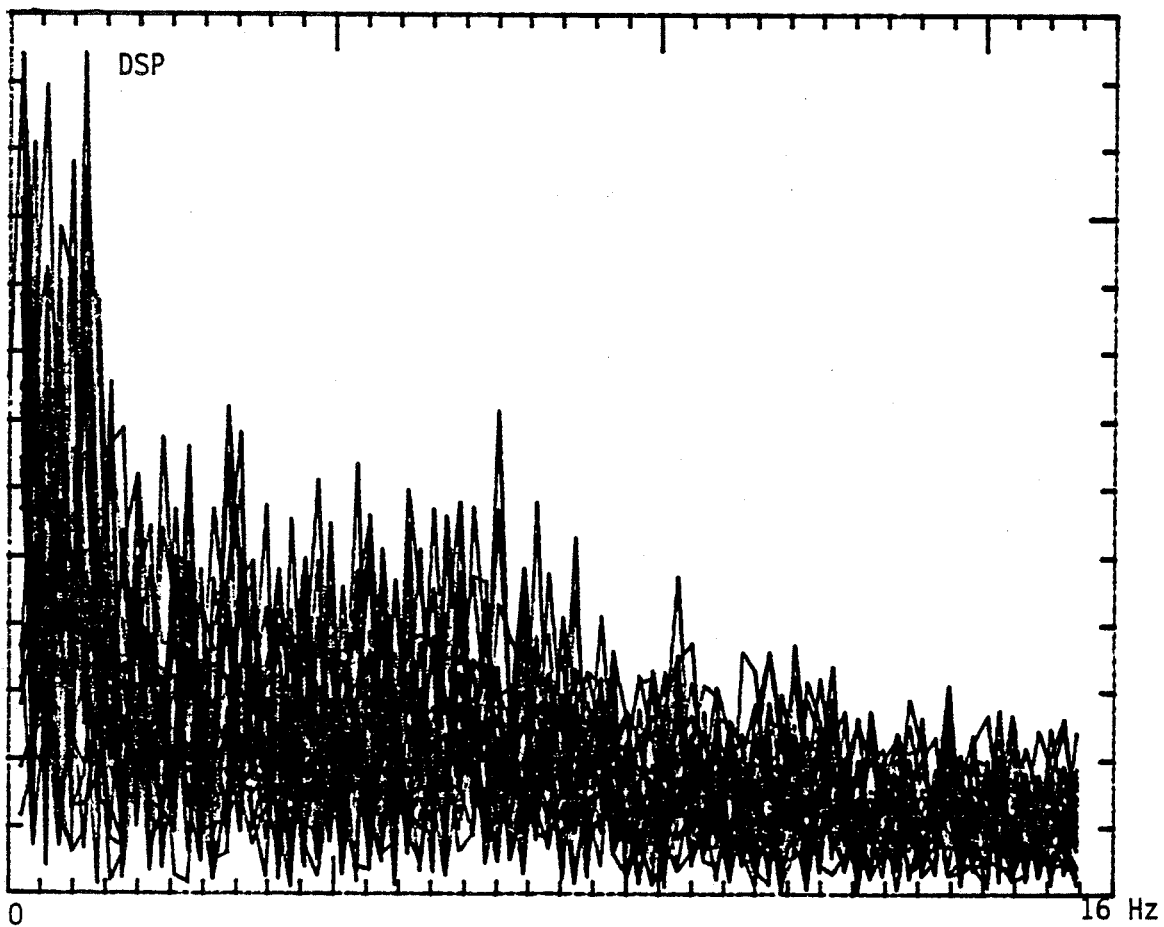


FIGURE 3 : 30 ABNORMAL SPECTRA

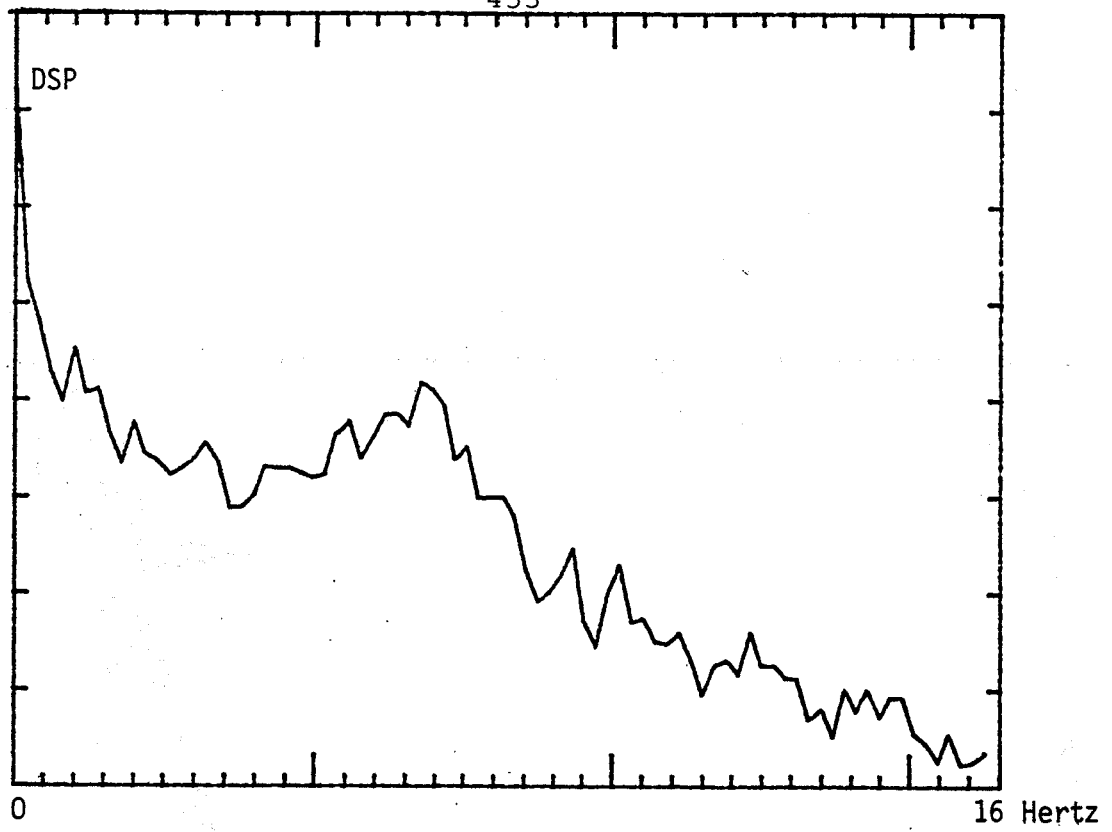


FIGURE 4 : MEAN SPECTRUM OF 150 ELEMENTS

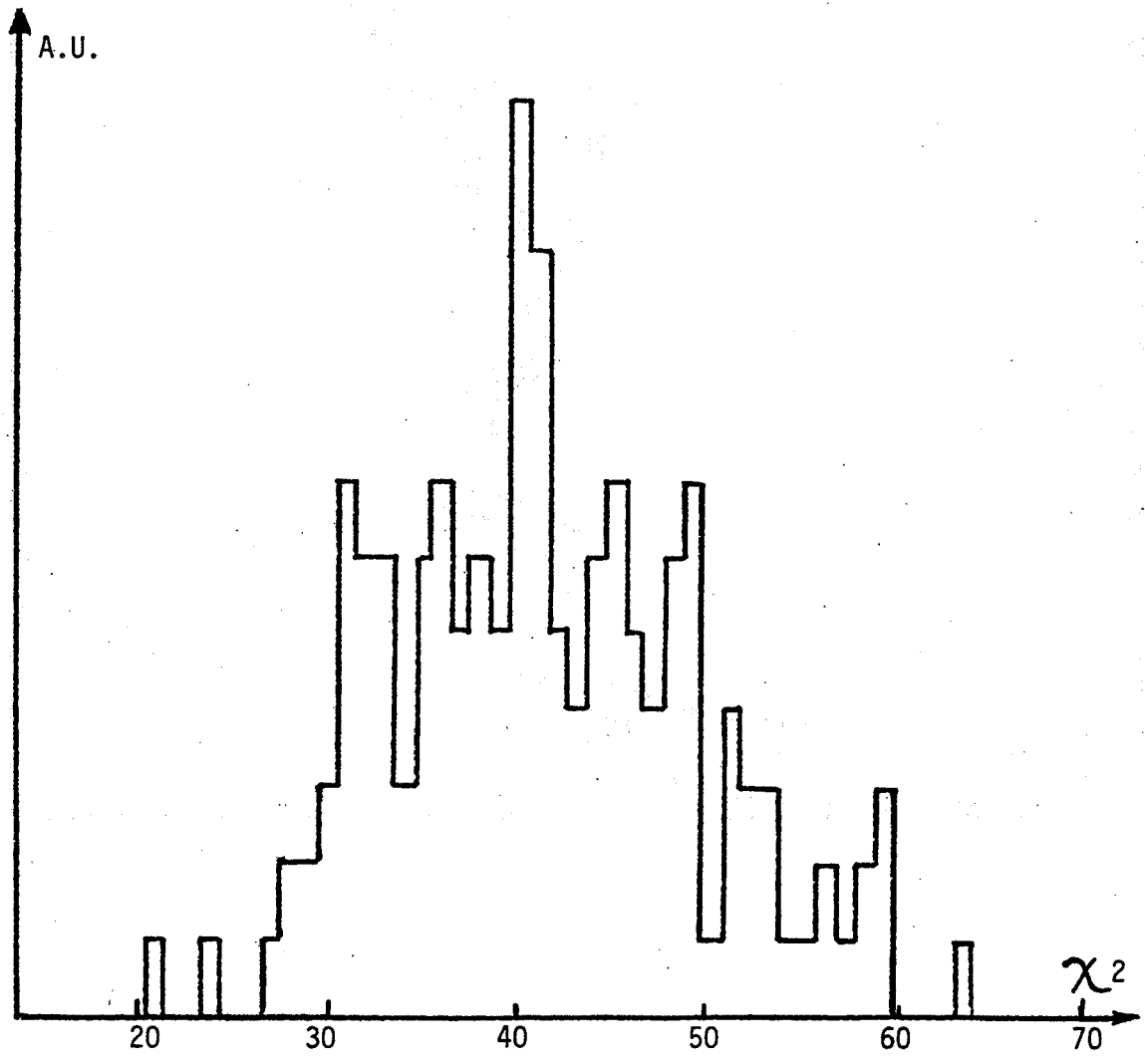


FIGURE 5 : HISTOGRAMM OF THE PROBABILITY DENSITY OF Z

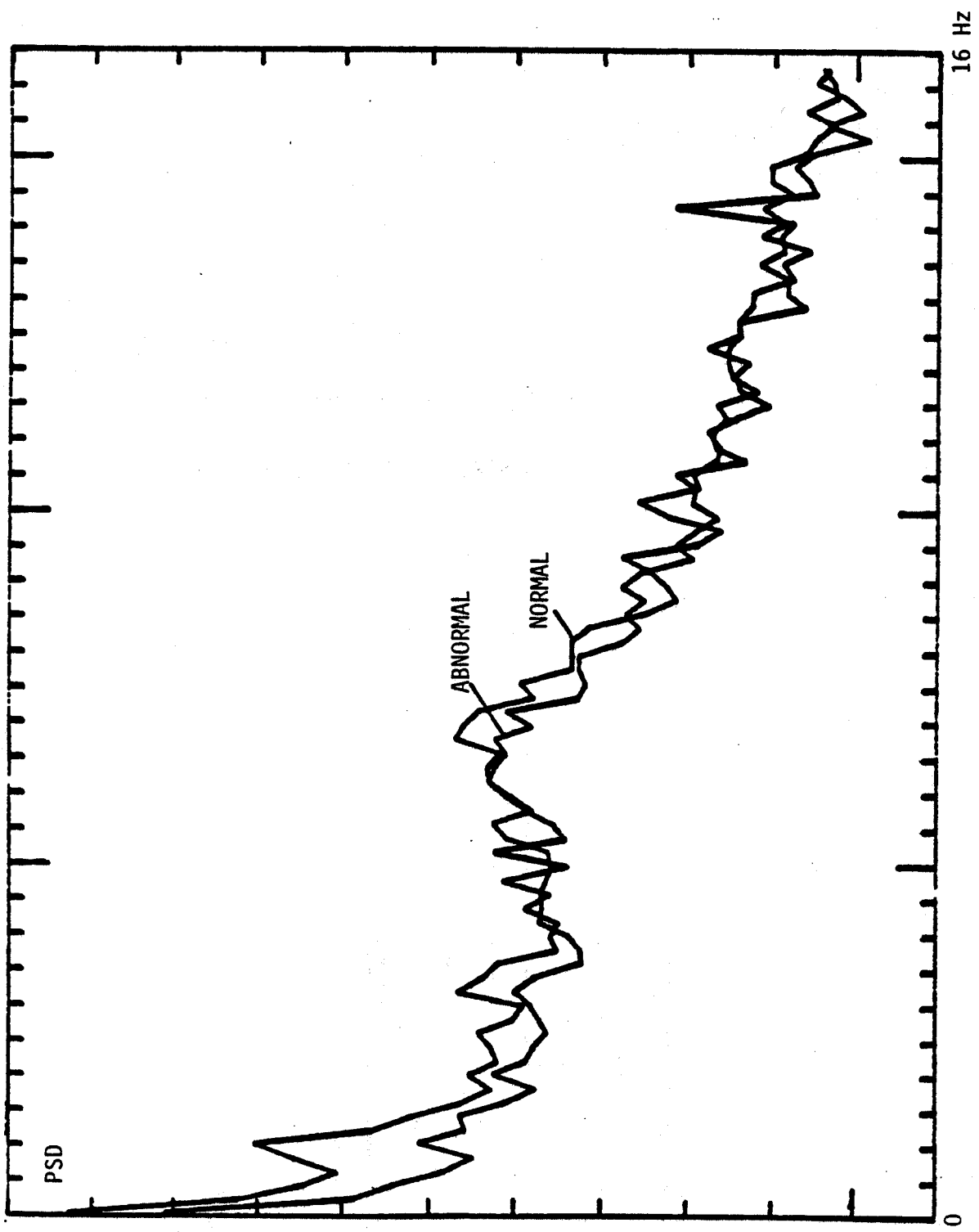


FIGURE 6 : COMPARISON OF NORMAL AND ABNORMAL MEAN VECTORS

M. Edelmann

SIMULATION OF FUEL ELEMENT THERMAL HYDRAULICS FOR SENSITIVE
MONITORING OF COOLANT FLOW

KERNFORSCHUNGSZENTRUM KARLSRUHE

Institut für Neutronenphysik und Reaktortechnik

Simulation of Fuel Element Thermal Hydraulics for
Sensitive Monitoring of Coolant Flow

M. Edelmann

Paper to be presented at
the IAEA/NPPCI Specialist's Meeting on

Procedures and Systems for Assisting an Operator during
Normal and Anomalous Nuclear Power Plant
Operation Situations
to be held at Munich , December 5-7, 1979

Abstract

Intercomparison of signals from a mathematical plant model and true signals from a power plant is a well-known principle of reactor surveillance. This paper deals with the application of this technique for monitoring individual coolant flow of the subassemblies with respect to cooling disturbances.

On one hand, due to the high power density in LMFBR's local loss of flow within a fuel element may cause fuel failure with serious consequences for the whole core. On the other hand, the conventional measurement of sub-assembly outlet temperatures is not sensitive enough to detect local flow obstructions or blockages before pin failure occurs. This is true because the additional pressure drop due to a local blockage is very small and causes a little reduction in the total subassembly flow only. The sensitivity of outlet temperatures for cooling disturbances can be improved significantly by eliminating temperature noise and variations of the temperature rise of a subassembly due to inlet temperature and power noise or control of the reactor power level. This has been demonstrated at the sodium cooled 58 MWth KNK II reactor at Karlsruhe.

The different types of KNK fuel elements were modeled by individual combinations of two first-order low-pass filters, one for the fuel element and one for the thermocouple. Using a neutron detector signal as input for these filters provides simulated outlet temperature signals for comparison with the measured signals. Under stationary conditions of reactor operation these signals agreed within less than 1 K.

For non-stationary conditions a more general model of the fuel element was applied. In this model time-dependent thermal hydraulic parameters could be used. In this way a cooling disturbance consisting of gas bubbles in the sodium was simulated. A sensitivity study showed that gas bubbles of 1 % of the sodium volume in the fuel region could be detected at KNK II in spite of the power drop caused simultaneously by the negative sodium void effect.

1. Introduction

Fast reactor fuel elements due to their high power densities are sensitive to cooling disturbances. In future LMFBR's therefore the coolant flow rate through the subassemblies will be monitored indirectly by individual temperature instrumentation. However, with conventional monitoring narrow tolerance bands are not feasible for individual fuel element outlet temperatures because of significant changes of outlet temperatures under normal operating conditions. This is due to power and inlet temperature noise, load variation and burn-up.

On the other hand, local cooling disturbances within a fuel element, i.e. local blockages, swelling or bowing of fuel pins, may lead to thermal overload of fuel or cladding without producing a significant additional pressure drop. In this case the total flow rate of coolant and therefore also the outlet temperature would not change significantly.

Consequently, the coolant flow through the subassemblies has to be measured with high precision to detect local cooling disturbances. For this measurement simple and reliable techniques are required. At present only temperature instrumentation seems to be practicable in commercial fast breeder reactors. Individual redundant flow instrumentation for all subassemblies is prohibitive for technical and economic reasons. Therefore, the only way to detect local loss of cooling in a fast reactor subassembly before local boiling of sodium or pin failure occurs will be by more sophisticated surveillance of outlet temperatures. Several different techniques are investigated in this respect as, for instance, using dynamic references for outlet temperatures [1] or the analysis of outlet temperature noise [2].

In an earlier paper [3] a new method for monitoring subassembly coolant flow rates with high precision and quick response using outlet temperature signals was proposed. It is based on eliminating the outlet temperature fluctuations present under normal reactor operating conditions. From the normal outlet temperature signals, a neutron detector signal proportional to subassembly power and an inlet temperature signal "balanced temperature"

signals can be formed in a simple way. These signals depend on the coolant flow rate only. It was shown that for the KNK-I reactor at Karlsruhe a change of less than 1 % in the coolant flow rate should be detectable with extremely low false alarm rates.

This method uses electronic models simulating the thermal hydraulic properties of the subassemblies. For KNK-I only time shifting of an appropriately normalized neutron detector signal was necessary to obtain simulated outlet temperature signals. Simulated and measured outlet temperatures differed by less than 1K under stationary conditions of reactor operation.

Although sodium cooled, KNK I was a thermal reactor. KNK-II consists of a central fast test zone of LMFBR type fuel elements and an annular driver zone having an intermediate neutron spectrum. In this paper simulation of the different KNK-II fuel elements with respect to sensitive monitoring of coolant flow is reported. Particular interest is dedicated to simulating short-time flow perturbations to study the thermal effects of gas bubbles in the coolant.

It should be pointed out here that the used fuel element simulators not only provide a means for sensitive monitoring of coolant flow relative to sub-assembly power. They also can be applied to measure fuel element parameters such as absolute coolant flow and power as well as average fuel temperature and heat transfer coefficients by fitting simulator outputs to actual plant signals. No special or additional instrumentation is needed for these measurements. They are based on the inherent noise of reactor power only and use only normally available plant signals. Therefore the measurements can be performed at any time during normal reactor operation. The change of fuel element parameters with time and reactor operating conditions can also be measured in this way. However in this paper only the application to coolant flow monitoring is dealt with.

2. Thermal hydraulic fuel element model

The theoretical model used to describe the fuel element thermal hydraulics is the same as developed in [3]. Only different approximations of the resulting power-to-outlet temperature transfer function are used to simulate KNK-I and KNK-II fuel elements.

In the model a fuel element consists of two regions. One is representing the fuel rod bundle being the heat source, the other one, the heat sink, is comprising the coolant and all subassembly structure with negligible heat generation. In the following only the active zone of the subassembly is considered. Axial blankets and subassembly structure is not accounted for. The system is completely determined by the temperatures and heat capacities of the two regions, an integral heat transfer coefficient between them and the heat generation rate as well as by the heat removed per unit time by the coolant. The heat balance between the two regions is given by the following equations,

$$C_f \dot{T}_f(t) = P(t) - k(T_f(t) - T_c(t)) \quad (1)$$

$$C_c \dot{T}_c(t) = k(T_f(t) - T_c(t)) - 2hF(T_c(t) - T_i(t)) \quad (2)$$

with

T_f mean temperature of fuel region

$T_c = \frac{T_o + T_i}{2}$ mean coolant temperature

T_i, T_o inlet and outlet temperature

C_f, C_c heat capacity of fuel and coolant region

P subassembly power

k overall heat transfer coefficient between fuel and coolant region

h specific heat of coolant

F coolant flow rate

For stationary operating conditions only inlet temperature and power are independent variables of time. Non-stationary conditions can be included to a first approximation by allowing small variations of the parameters in the stationary solutions.

The Laplace transforms of Eq. (1) and (2) can be solved explicitly. For the mean coolant temperature one obtains in the frequency domain

$$T_c(j\omega) = H(j\omega) \cdot \frac{P(j\omega)}{2hF} + H_i(j\omega) \cdot T_i(j\omega) \quad (3)$$

wherein

$$H(j\omega) = \frac{1-\gamma}{(1+j\omega\tau_1) \cdot (1+j\omega\tau_2)^{-\gamma}} \quad (4)$$

$$H_i(j\omega) = (1+j\omega\tau_1) \cdot H(j\omega) \quad (5)$$

$$\gamma = \frac{k}{k+2hF} \quad (6)$$

$$\tau_1 = \frac{C_f}{k} \quad (7)$$

$$\tau_2 = \frac{\gamma C_c}{k} = \frac{C_c}{k+2hF} \quad (8)$$

The relationship between the coolant temperature T_c and subassembly power and inlet temperature are described by the two transfer functions (4) and (5) representing modified (feedback) low-pass characteristics of second and first order, respectively. The two time constants defined in Eqs. (7) and (8) are assigned to the fuel and coolant region, respectively, because of their proportionality to the corresponding heat capacities. The model parameter γ given by Eq. (6) also has a physical meaning. For the stationary mean values of fuel and coolant temperatures, \bar{T}_f and \bar{T}_c , it follows directly from Eq. (2)

$$\frac{\bar{T}_c - \bar{T}_i}{\bar{T}_f - \bar{T}_i} = \gamma \quad (9)$$

The third parameter (6) of the transfer function (4) therefore represents the ratio of average stationary temperature rises in coolant and fuel.

From the quantities in Eq. (3) only T_c and T_i can be measured directly. Subassembly power and coolant flow rate in general are not available in absolute units. Only the ratio of their stationary mean values $P(o)/2hF$ is known through the temperature rise $T_c(o) - T_i(o)$. In a fast reactor the signal of a power monitor can be considered proportional to subassembly power, too. The corresponding calibration factor needs not to be known explicitly. Its value relative to the outlet temperature signals is automatically accounted for by relating the temperature signals to a neutron detector signal instead of the original physical quantities. The other model parameters can be calculated according to Eqs. (6) through (8) if the necessary fuel element data are known with sufficient accuracy. This is not true for the heat transfer coefficient k . This parameter strongly depends on the heat conductance between fuel and cladding which is known only with very low certainty.

The model parameters can also be determined experimentally by fitting Eq. (4) to a measured transfer function. The power-to-outlet temperature transfer function of a fuel element can be measured easily by noise analysis techniques [4] during normal reactor operation if there is sufficiently high power noise in the relevant frequency range. Otherwise the power fluctuations had to be increased by external reactivity modulation. This is also possible during normal power operation because only small amplitude reactivity oscillation is required. Since the fuel heat capacity is known fairly well the over-all heat transfer coefficient k can be obtained from the fitted fuel time constant τ_1 . From this coefficient in turn the specific heat conductance between fuel and cladding (gap conductance) can be determined if the other heat conductances (fuel, cladding, cladding/coolant) are given. This method has the further advantage that all thermal parameters remain unchanged during the measurement because the power and temperature fluctuations are very small in comparison to their stationary mean values.

In this paper only the model parameters (6) through (9) were considered. For KNK it turned out that not all of them could be measured for two reasons: One, the power noise in the frequency range $f > 1$ Hz relevant for the coolant time constant τ_2 was too low. Two, the response of the thermocouples measuring the outlet temperatures was too slow. The thermocouples used at KNK-II have time constants in the order of 1 second. Calculated parameters for two types of KNK-II fuel elements are given in Table I. The coolant and fuel time constants differ by more than a factor of 15 from each other in both cases. In Fig. 1 the power spectral densities of neutron noise are

shown for KNK-I and II. It is seen that the power noise for frequencies $f > 1$ Hz is much lower than in the frequency range around f_0 relevant for the fuel time constant. Inlet temperature noise is limited to still lower frequencies. Whereas the lack of high frequency content in power and inlet temperature noise imposes difficulties in determining both time constants it favours simple approximations of the transfer functions (3) and (4). For KNK-II at frequencies $f \ll 1$ Hz second-order terms of ω can be neglected and the transfer functions H and H_i to a good approximation are given by

$$H(j\omega) \approx \tilde{H}(j\omega) = \frac{1}{1+j\omega\tau_0} \quad (10)$$

and

$$H_i(j\omega) \approx \tilde{H}_i(j\omega) = \frac{1+j\omega\tau_1}{1+j\omega\tau_0} \quad (11)$$

wherein

$$\tau_0 = \frac{\tau_1 + \tau_2}{1-\gamma} \quad (12)$$

Thus, the power to outlet temperature transfer function is reduced to a first-order low-pass characteristics with the time constant τ_0 . The corresponding corner frequency $\frac{1}{2\pi\tau_0}$ is indicated in Fig. 1. At KNK-II there is a rather high level of power noise around f_0 . Therefore the time constant τ_0 can be obtained from the gain of the transfer function. However, since the power noise around 1 Hz is very low the magnitude of the outlet temperature fluctuations at KNK will depend on the fuel time constant τ_1 only and the term with the coolant time constant τ_2 can be neglected in Eq. (4). The high frequency contributions of power noise to temperature noise will be further reduced in the measured signals by the band-limiting effect of the slow thermocouples used at KNK. For these reasons the time constant obtained by fitting the gain of the transfer function (4) to measured curves would be

$$\tau_0 = \frac{\tau_1}{1-\gamma} \quad (13)$$

rather than that defined in Eq. (12). For similar reasons $H_i(j\omega) = 1$ is a good approximation in practical applications.

From the Eqs. (6) and (13) we find the relationship

$$k = \frac{C_f}{\tau_o - \frac{C_f}{2hF}} \quad (14)$$

which can be used to determine the over-all heat transfer coefficient from the measured time constant, calculated heat capacity of the fuel rod bundle and nominal coolant flow rate of the subassembly.

For completeness, it should be mentioned here that at KNK-I as shown in ref. [3] a further simplification was applied to Eq. (10) because of a too low level of power noise around the fuel corner frequency f_o . For the lower frequency noise the gain of the transfer function is not frequency dependent, only a linear phase shift representing a time delay according to the time constant (12) is left. This delay is not attenuated by a slow thermocouple like the magnitude of the temperature fluctuations. On the contrary, the time delay is increased by the time constant of the thermocouple. From the measured delay time between power and outlet temperature noise signals the fuel time constant and therefore the heat transfer coefficient can be obtained, too if the time delay of the thermocouple and the involved signal channels are known.

If the measurements are performed with slow thermocouples having time constants not much smaller than those of the fuel element the thermocouple has to be included in the theoretical model as well as in the fuel element simulator. To a good approximation the transmission properties of a thermocouple can be described by a first-order low-pass characteristics

$$G(j\omega) = \frac{1}{1+j\omega\tau} \quad (15)$$

with the time constant τ . Thus, we finally obtain for the simulated outlet temperature signal T_s

$$T_s(j\omega) = U(j\omega) \frac{P(j\omega)}{hF} + G(j\omega) \cdot T_i(j\omega) \quad (16)$$

with

$$U(j\omega) = G(j\omega) \cdot \hat{H}(j\omega) = \frac{1}{(1+j\omega\tau)(1+j\omega\tau_o)} \quad (17)$$

For the fast fuel element at the central core position of KNK-II the various transfer functions were calculated from the parameters given in Table I (type A). They are shown together in Fig. 2 for illustration of the quality of the discussed approximations. The transit time of the coolant from the point subassembly located near the core midplane to the thermocouple is not included in the theoretical model. It is accounted for separately in the time domain only when measured and simulated temperature signals are compared. The transit time of the coolant between the thermocouples at the reactor inlet and subassembly outlet causes a delay of the inlet temperature component in the outlet temperature signals relative to the inlet temperature signal. For the extremely low frequencies of inlet temperature noise this difference is negligible in general and in the second term of Eq. 16 we can set $G(j\omega) \equiv 1$.

3. Fuel element simulation

In which way a fuel element is to be simulated depends on the intended application. For monitoring of stationary coolant flow the simplified transfer function (10) or possibly a pure time delay is sufficient to derive an outlet temperature signal from a neutron detector signal. Which one of these possibilities has to be chosen depends on the required sensitivity and false alarm rate of a balanced temperature signal with respect to changes of coolant flow as well as on the spectral composition of power noise and on the actual values of the fuel element time constants. This interdependence is described in [3] in more detail.

The balanced outlet temperature signal is formed by subtracting the simulated signal from the measured one. The simulated outlet temperature signal is obtained by filtering and amplifying a neutron detector signal in a single active low-pass filter with the time constant τ_0 and adding an inlet temperature signal. If necessary an additional low-pass filter is used to simulate the thermocouple.

For simulation of the non-stationary behaviour of fuel elements the original model has to be used instead of the simplified one because in the latter the original four parameters of the model are reduced to a single one, τ_0 . In the original model parameters can be changed independently. A fuel element simulator then should be an electronic device which integrates the equations (1) and (2) using a neutron detector signal and a core inlet temperature

signal for input of subassembly power and inlet temperature. How such a device has been realized follows directly from the integral form of Eqs. (1) and (2),

$$T_f(t) = \frac{1}{C_f} \int dt [P(t) - k (T_f(t) - T_c(t))] \quad (18)$$

$$T_c(t) = \frac{1}{C_c} \int dt k [T_f(t) - T_c(t)] - 2hF [T_c(t) - T_i(t)] \quad (19)$$

In a real simulator the quantities in these equations are represented by voltages and gain factors which can be changed individually to model a situation of interest.

In Fig. 3 the block diagram of a simulator is shown in which a simultaneous variation of the coolant flow and the heat transfer between fuel and coolant can be simulated. This corresponds to a situation where the coolant contains gas bubbles. If the gas bubbles are so small that the coolant can be considered to be homogeneous the heat transfer coefficient might not be changed and only the coolant flow rate and the heat capacity of the coolant inside of the subassembly will be reduced according to the gas content in the coolant. Leaving the heat capacity unchanged, too corresponds to a flow reduction without gas in the coolant. A larger amount of gas in the coolant however, will have an influence on the heat transfer coefficient even if the two components are mixed homogeneously.

A heterogeneous mixture of gas and coolant is simulated by switching the flow rate and the heat transfer coefficient between their nominal values and zero according to the sequence of coolant and gas in the cooling channel. The coolant heat capacity has to be reduced in accordance to the mean gas fraction in the coolant. In most cases however, the coolant heat capacity has a minor influence on the thermal effects and needs not to be changed in the simulator. As a limiting case, all parameters can be kept zero for a certain time interval to simulate a complete interruption of cooling by a large gas bubble.

The temperature of fuel and coolant in Eqs. (18) and (19) do not depend on the number (and length) of the fuel pins. Therefore, in principle, an individual treatment of single fuel rods with their cooling subchannels is possible if an interaction between adjacent subchannels can be taken into account or even can be neglected. For example, a situation could be simulated where gas bubbles are flowing only through a fraction of the cooling channel whereas in the rest of the fuel element full cooling capacity remains preserved. The fuel pins then would have different temperatures. The two coolant streams having different (time-dependent) temperatures will be mixed in the upper part of the subassembly and the thermocouple at the outlet would measure an attenuated thermal effect of the gas. In this case the change of mean coolant temperature and thermocouple output caused by gas in the coolant would be obtained by multiplying the corresponding simulator outputs by the ratio of the cross sections of the perturbed and unperturbed coolant streams.

In Fig. 4 the wiring diagram of the simulator used for the measurements is shown. The relationships between fuel element and simulator parameters given also in the figure can be obtained easily by an intercomparison of Eqs. (18), (19) with a similar set of equations describing the simulator. It can be seen that for equal relative changes of the coolant flow rate, coolant heat capacity and heat transfer coefficient only the resistors R_2 and R_6 have to be changed. This is accomplished by switching the serial resistors R_{22} and R_{66} on and off. If the heat transfer coefficient has to be kept constant only the resistor R_3 has to be varied. Resistor R_4 needs not to be changed in a first approximation because it is shunted by R_5 which in general is small compared to R_4 because $2hF \gg k$. Switching of the resistors was controlled by a timer or a function generator.

4. Results

The sensitivity of a balanced outlet temperature signal with respect to short-time cooling disturbances was determined in two steps. At first different types of gas and coolant mixtures were simulated as described in the last paragraph to determine the thermal effect of gas injections into the coolant. For this purpose the neutron detector signal was replaced by a dc signal equal to the mean value of the neutron signal to get rid of the noise from the signals. In this way a variety of idealized temperature responses to possible cooling disturbances by gas bubbles in the coolant was obtained. Two different time intervalls, 1s and 3s, were chosen for the duration of the disturbance.

In the second step a noise-balanced outlet temperature signal was generated using the noise components of an inlet and outlet temperature signal and the simulated temperature noise produced by a second-order low-pass filter from the neutron noise. For this signal which is suitable to monitor the coolant flow the maximum amplitude of the remaining fluctuation in the short-time range of some ten seconds was determined which defines the lower limit of detectable temperature effects by cooling disturbances of short duration. The gas bubbles observed at KNK-II were primarily detected by a negative peak in a neutron detector (reactivity) signal caused by the sodium void effect. In the normal subassembly outlet temperature signals the bubbles could not be seen because the power drop overcompensates the loss-of-cooling effect.

Some of the results obtained are shown in Figs. 5 through 11. For simulation of outlet temperatures the calculated model parameters given in Table I were used because measured values were not available. Measurement of time constants of all KNK-II fuel elements is now in progress.

In Fig. 5 the fuel and coolant temperature response to a total loss of cooling is shown. Two sets of curves are shown corresponding to cooling disturbances of 1 and 2.8 s duration. No heat is removed during this time from the fuel. All heat generated is stored in the fuel. Therefore the fuel temperature increases linearly with time whereas the coolant temperature at the subassembly outlet remains constant during the loss of cooling. Only when the cooling resumes again the outlet temperature responds to the disturbance. This is an important aspect of this kind of cooling disturbances besides of

the high temperature increase. They cannot be detected in time by outlet temperature measurements. Fortunately, this type of cooling disturbances is not very likely to occur. After the disturbance the coolant temperature at first increases according to its time constant and then decays together with the fuel temperature with the fuel time constant as the excess heat is removed from the fuel. In the signal of a slow thermocouple the temperature response is further delayed and also reduced.

The results shown in Fig. 6 are representative for a partial loss of cooling where only in a fraction of 10 % of the cooling channel cross section a cooling disturbance of the same type as in Fig. 5 is assumed. The only difference to Fig. 5 is the reduction of the mean outlet temperature response by a factor of 10. For the perturbed subchannel the results in Fig. 5 are still valid whereas in the unperturbed zone fuel and coolant temperatures remain unchanged. Only the change ΔT of temperatures instead of their total amount is shown in this and the following figures.

In Fig. 7 and 8 the results for a more realistic situation are shown. Here a gas content of 10 % in the coolant was simulated in two ways. In both cases the coolant flow rate and heat capacity were reduced by 10 % for about three seconds. The curves in Fig. 7 are obtained when the heat transfer coefficient is also reduced by 10 % whereas the results in Fig. 8 are obtained when the heat transfer coefficient is kept constant. From the comparison of the two figures it follows that the heat transfer coefficient has a strong influence on the magnitude of the fuel temperature response. The coolant temperature responds faster and with a slightly increased amplitude when the heat transfer coefficient is not reduced.

In the last example shown in Fig. 9 a "bubbly" flow of coolant and gas was simulated in 20 % of the cooling channel cross section. In the perturbed zone the heat transfer between fuel and coolant as well as the coolant flow rate were periodically switched between their nominal values and zero. In the figure the fuel temperature response in the perturbed zone is shown together with the mean outlet temperature and thermocouple response. The coolant temperature response in the perturbed zone would be higher by a factor of 5. The switching frequency was 50 Hz. Thus, 10ms periods of cooling and no cooling succeeded one another. For a flow velocity of 3 m/s

this corresponds to a bubble length of 3 cm. In this way cooling of the perturbed zone in the average was reduced by 50 % whereas total cooling of the subassembly was reduced by 10 % only. Therefore the different types of cooling disturbances are mutually comparable.

For the cooling disturbances of 1 second duration the temperature responses have significantly lower amplitude values. In Table II the maximum values of the temperature changes for about 1 and 3 sec. lasting cooling disturbances of different types in the whole cooling channel are listed for comparison.

The results from the simulation of cooling disturbances can be summarized by the following statements:

1. The magnitude of the outlet temperature responses does not depend strongly on the type of the disturbance. It is essentially determined by the degree and duration of the flow reduction.
2. The fuel temperature response into addition strongly depends on the change of the heat transfer coefficient.
3. The shape of the outlet temperature response is affected by the type of cooling disturbance.
4. Slow thermocouples decrease the sensitivity of outlet temperature signals for short-time cooling disturbances besides of the well-known increase of response time. Also information on the type of the perturbation might be lost in slow temperature sensors.

For testing the validity of the thermal hydraulic fuel element model and its approximations the power-to-outlet temperature transfer functions of KNK-II subassemblies were measured and compared to calculated transfer functions using Eq. (17). Fig. 10 shows two examples. Measured and fitted theoretical curves agree fairly well confirming the applicability of the theoretical model. However, the fitted time constants differ significantly from the calculated values given in Table I. It is suspected that the uncertainty of the heat transfer coefficient is responsible for this discrepancy. It was calculated from parameters of fresh fuel some of which change with burn-up.

To illustrate the capability of balanced outlet temperature signals to detect small cooling disturbances an example is shown in Fig. 11. A neutron detector (P) and outlet temperature (T_m) signal were measured when some cover gas was carried through the core by the coolant producing a negative power peak. The resulting dip in the neutron and outlet temperature signal is clearly seen in Fig. 11. The balanced signal represented by the lowest curve ($T_m - T_s$) is not changed by the event. It is fluctuating less than $\pm 1K$ which is equivalent to less than $\pm 0.5\%$ change of the coolant flow rate. Consequently, 1 % gas in the coolant should be detectable with high probability. This was confirmed by adding a simulated temperature response caused by a 1 % gas content of 4s duration to the normal and balanced outlet temperature signal. It is evident from the resulting signals also shown in Fig. 11 that 1 % gas in the coolant would have been reliably detected by the balanced outlet temperature signal in this case.

5. Conclusions

The thermal response of a fast reactor fuel element to small power variations under normal and perturbed cooling conditions can be obtained to a good approximation from a simple theoretical model.

Adjusting model parameters by fitting model outputs to measured outlet temperatures provides thermal parameters of the fuel element. It is expected that the large uncertainty of the heat conductance between fuel and cladding (gap conductance) can be reduced in this way. The method is applicable on-line during normal reactor operation. Thus, also the change of thermal fuel element parameters with operating conditions and increasing degree of burn-up could be measured continuously.

Comparison of actual subassembly outlet temperatures with signals from adopted fuel element simulators enables monitoring of individual subassembly coolant flow with high precision and quick response. Fuel element simulators can be realized by simple analog devices.

Acknowledgement

The author gratefully acknowledges the valuable comments and suggestions on analog signal processing by W. V ath.

References

- /1/ S. Jacobi, K. Schleisiek, D. Smidt, M. Straka
Kühlungsstörungen in Brennelementen natriumgekühlter Reaktoren und
davon abgeleitete Anforderungen an das Brennelement-Schutzsystem,
Tagungsbericht DATF Reaktortagung Düsseldorf, 1976, Deutsches Atom-
forum e.V., Bonn (1976)
- /2/ G. Weinkötz, H. Martin, L. Krebs
Detection of cooling disturbances in the fuel elements of an LMFBR
by temperature fluctuation analysis. Proc. this conference
- /3/ M. Edelmann
Noise and DC Balanced Outlet Temperature Signals For Monitoring
Coolant Flow in LMFBR Fuel Elements
Proc. SMORN-II, Gatlinburg, Tenn. U.S.A.,
Sept. 19 -23, 1977
in: Progress in Nucl. En. Vol.1, No. 2-4 (1977), 543-552
- /4/ H. Schlitt, F. Dittrich
Statistische Methoden der Regelungstechnik
B.I. - Hochschultaschenbücher Nr. 526, Bibliogr. Inst.
Mannheim/Wien/Zürich (1972)

Table I

Parameters of KNK-II fuel element models.

	Type A	Type B
C_f [J/K]	8717	11018
C_c "	3025	3552
k [W/K]	4470	4050
F [Kg/s]	10.94	5.11
γ [1]	0.14	.24
τ_1 [s]	1.94	2.72
τ_2 "	.095	0.18
τ_o "	2.27	3.58
τ "	1.0	1.0

Table II

Maximum temperature responses to cooling disturbances

Disturbance		ΔT_f [K]	ΔT_c [K]	ΔT_s [K]
10% Reduced flow and heat transfer	1s	45	9	8
	3s	87	24	20
10% Reduced flow only	1s	7	27	17
	3s	12	29	27
Bubbly flow (whole channel)	1s	202	53	35
	3s	480	129	103

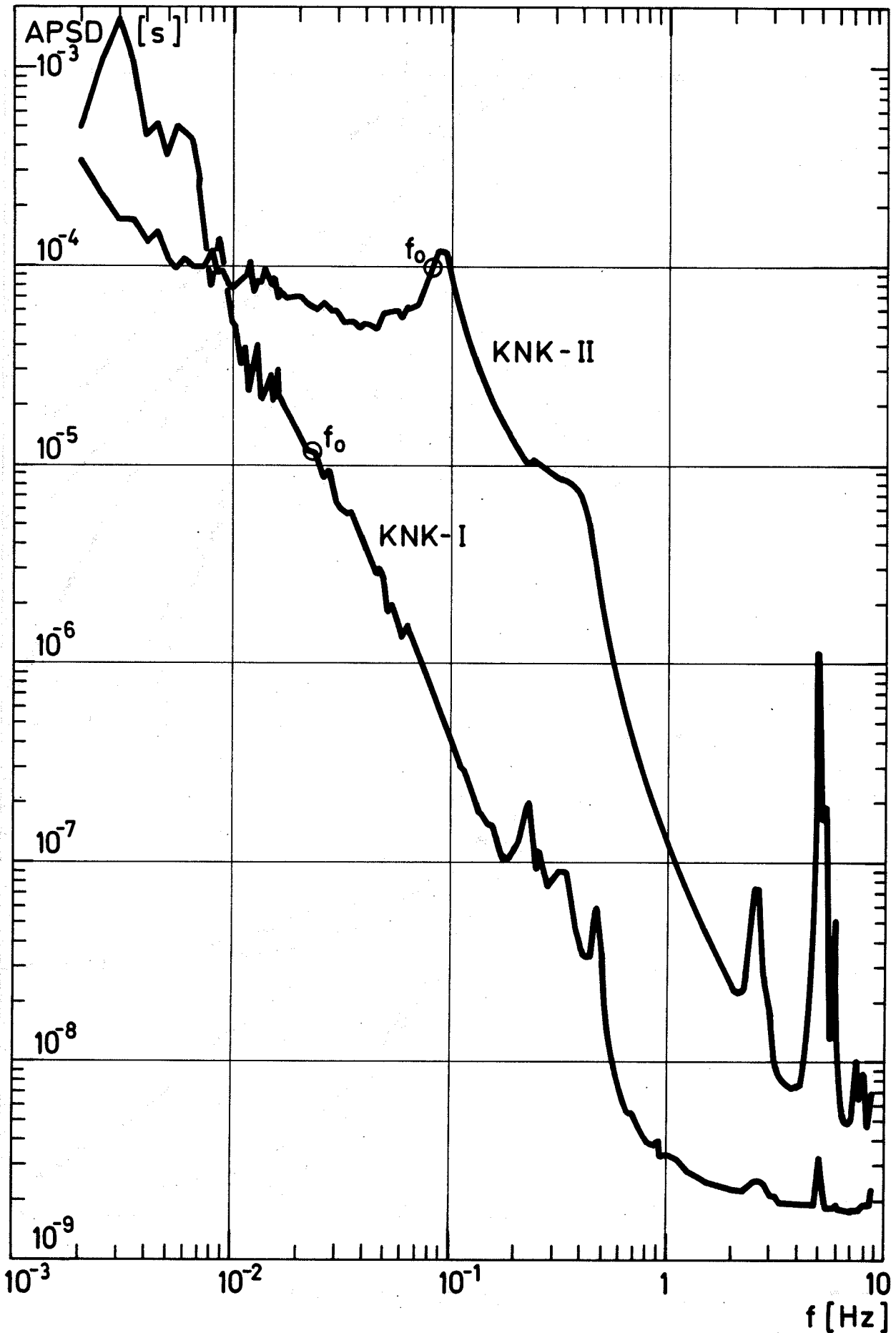


Fig. 1 Normalized power spectral densities of neutron noise of KNK

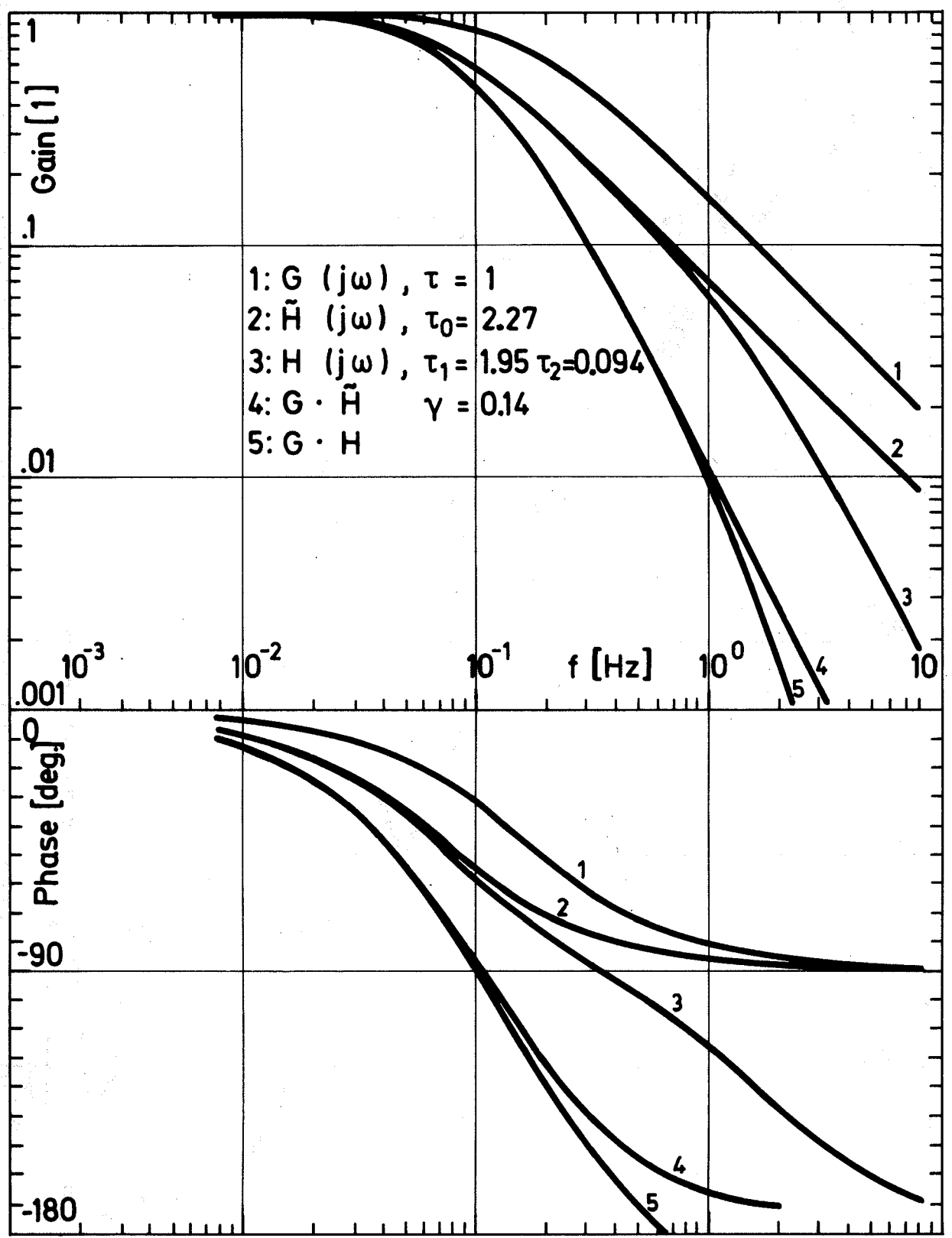


Fig.2 Calculated transfer functions

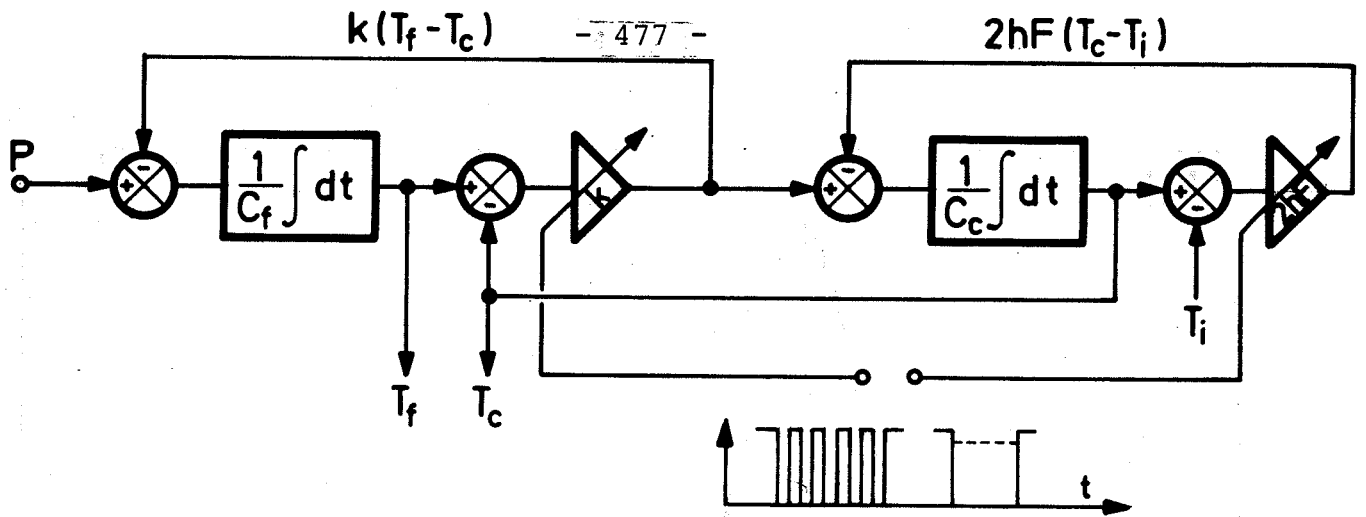
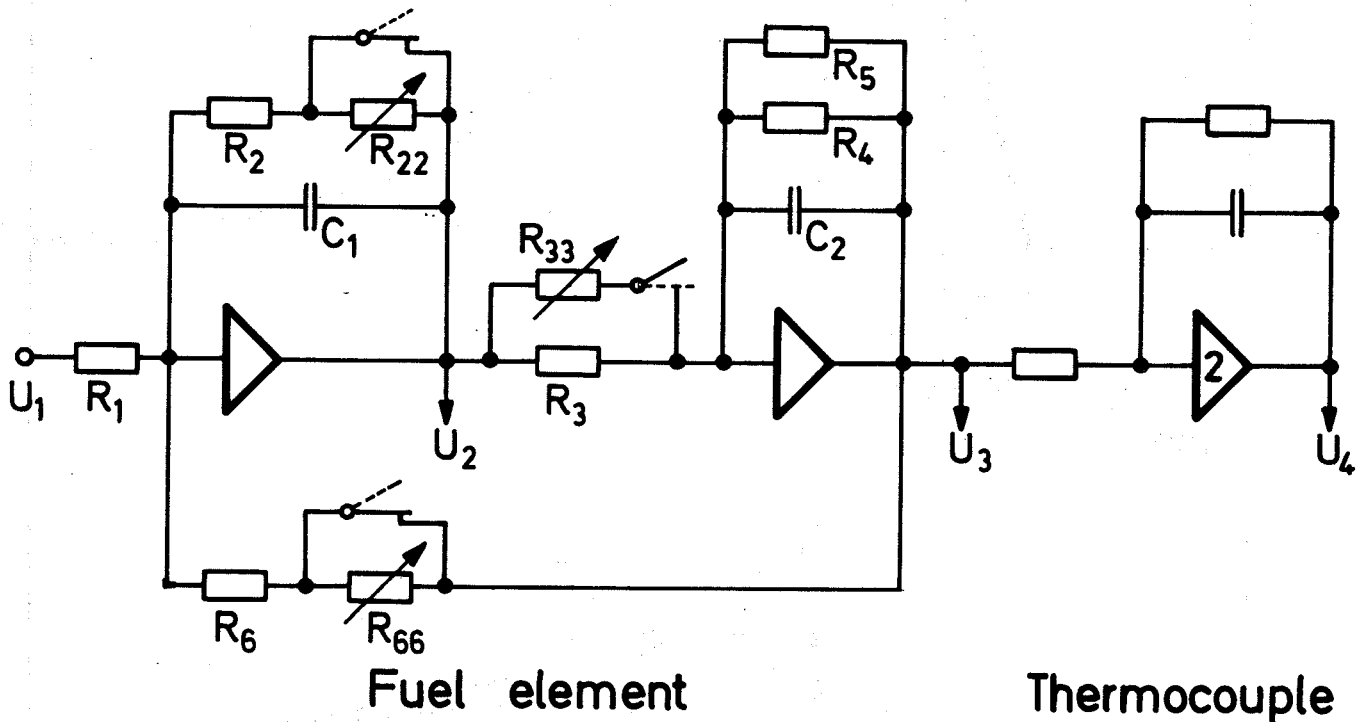


Fig.3 Block diagram of fuel element simulator



$$R_1 = X \frac{C_f}{C_1} \quad R_2 = R_6 = \frac{C_f}{kC_1} \quad R_3 = R_4 = \frac{C_c}{kC_2} \quad R_5 = \frac{C_c}{2hFC_2}$$

$$U_1 = Z \cdot P(t) \quad U_2 = -Y \cdot [T_f(t) - T_i] \quad U_3 = Y [T_c(t) - T_i] \quad U_4 = -Y [T_s(t) - T_i]$$

X, Y, Z = Scaling Factors, $Z = X \cdot Y (=10^{-6}, Y = 0.01)$

Fig.4 Wiring diagram of used simulator

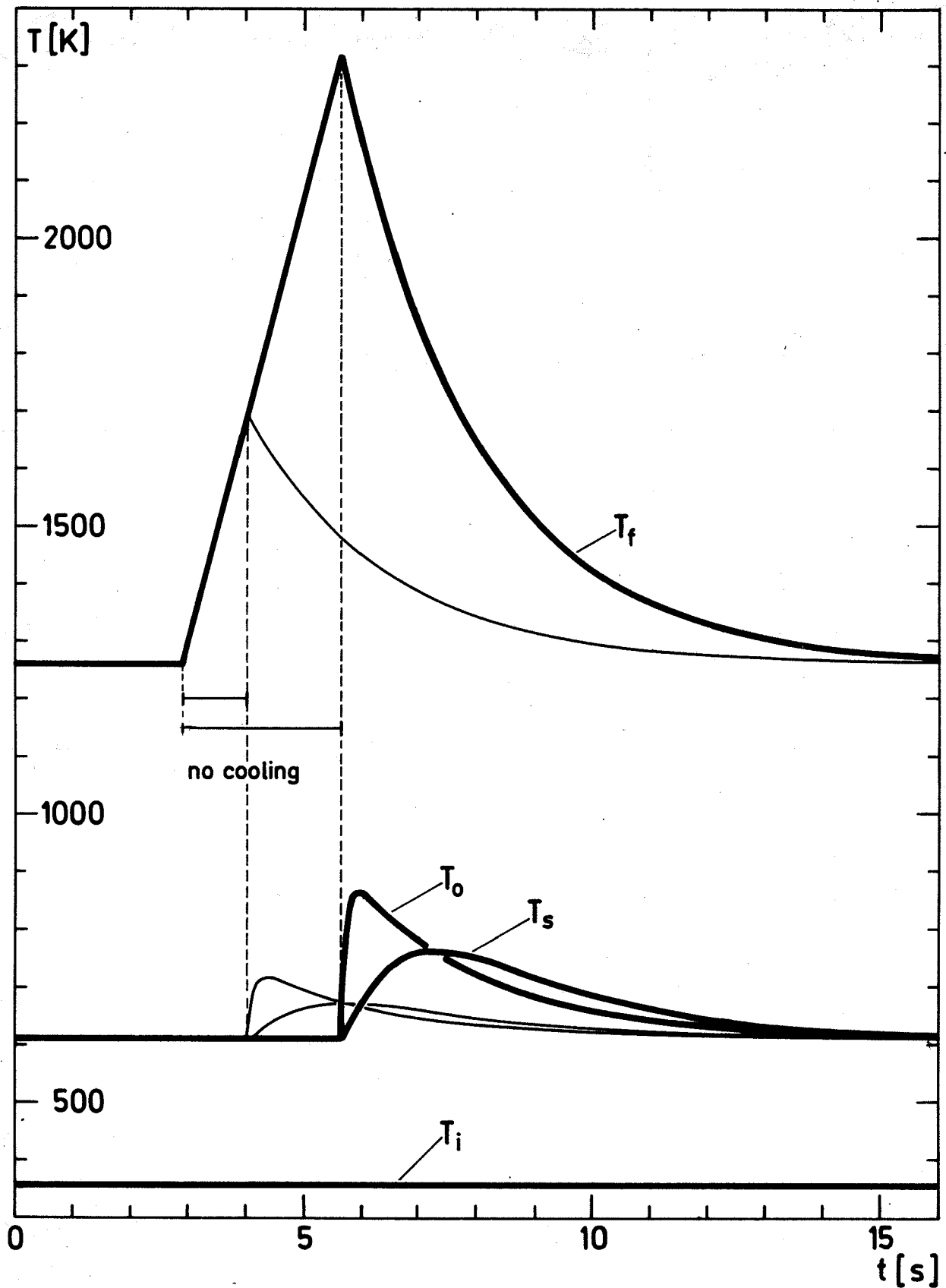


Fig.5 Simulated temperature response to total loss of cooling

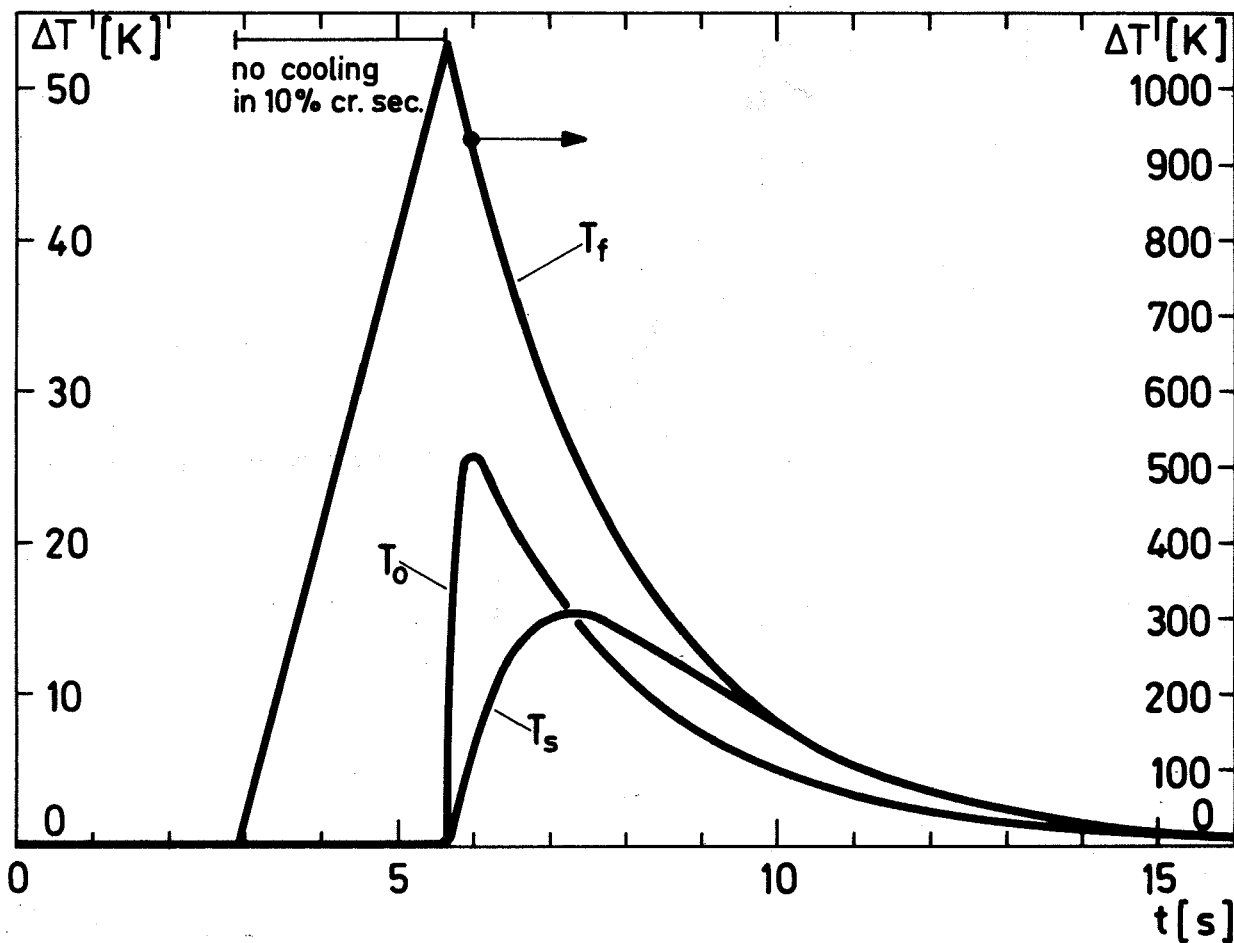


Fig.6 Temperature response to partial loss of cooling

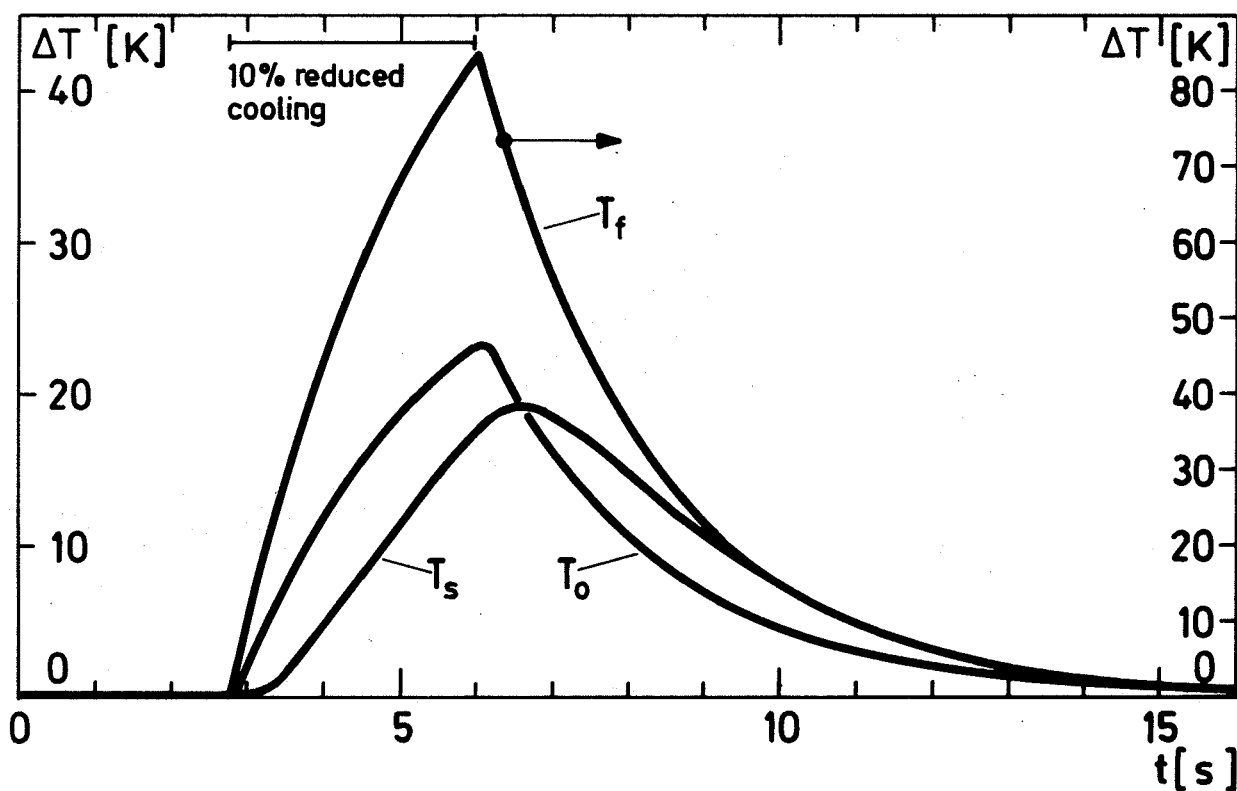


Fig.7 Temperature response to reduced cooling (F, k, C_c)

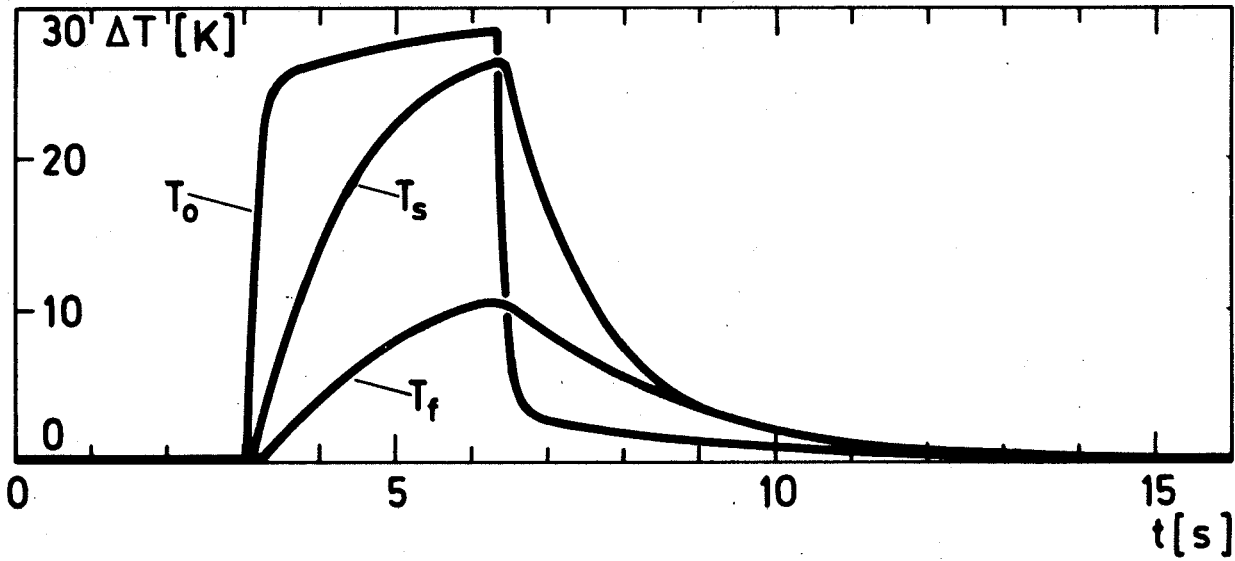


Fig.8 Temperature response to 10% reduced cooling (F, C_c)

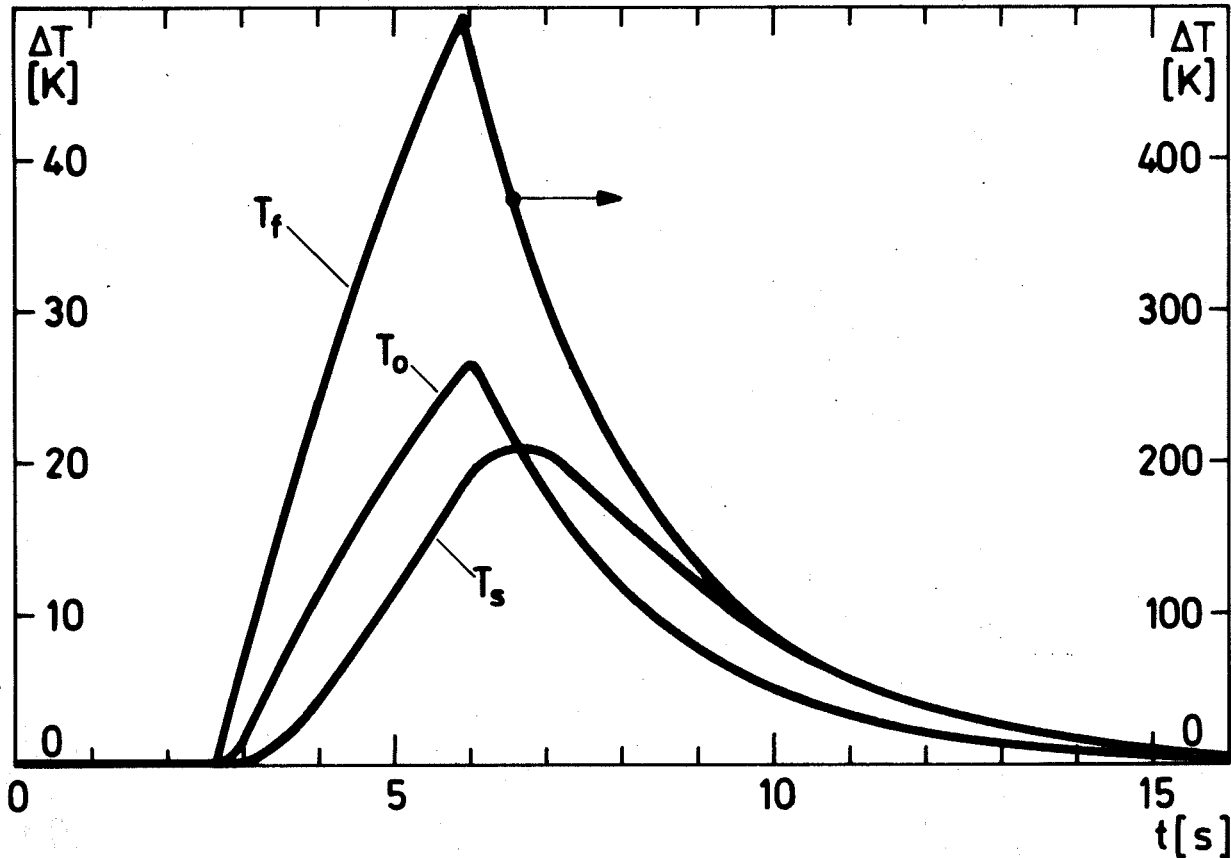


Fig.9 Temperature response to chopped coolant flow

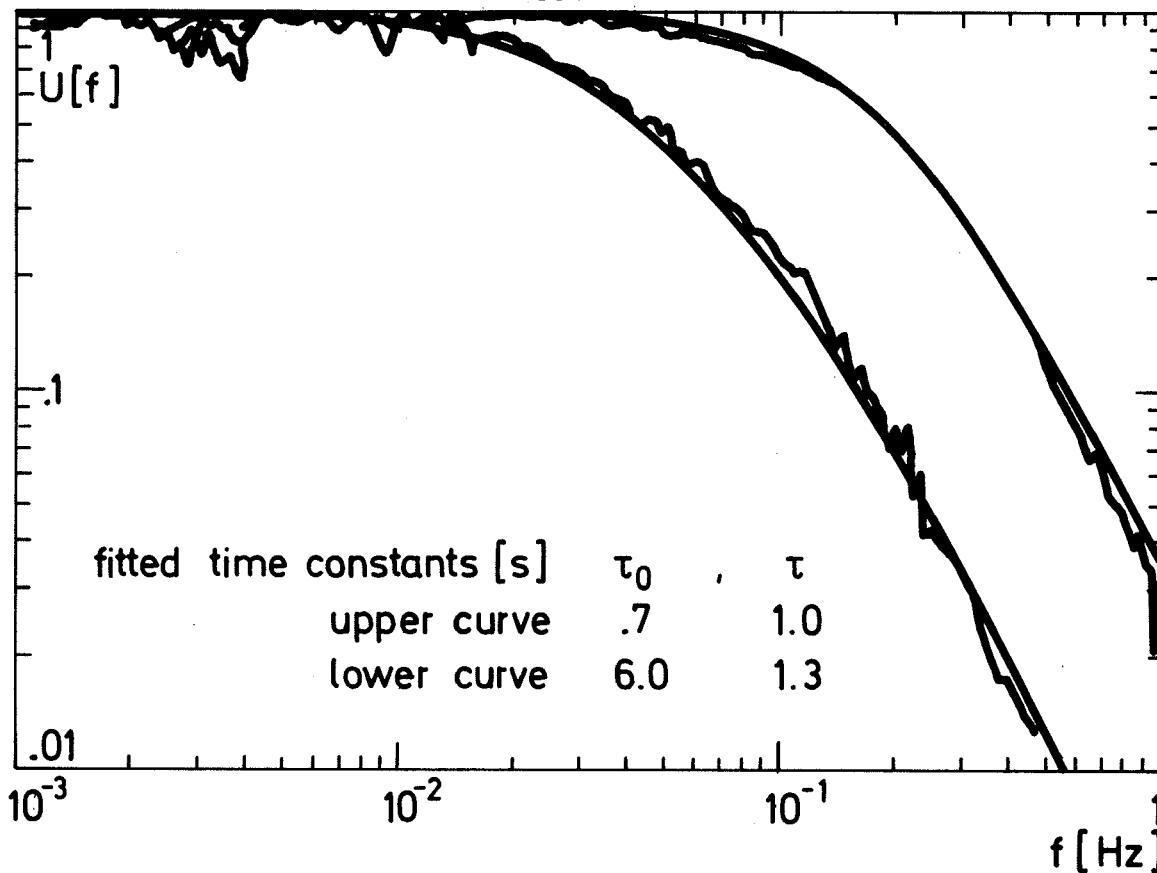


Fig.10 Measured and fitted theoretical transfer functions

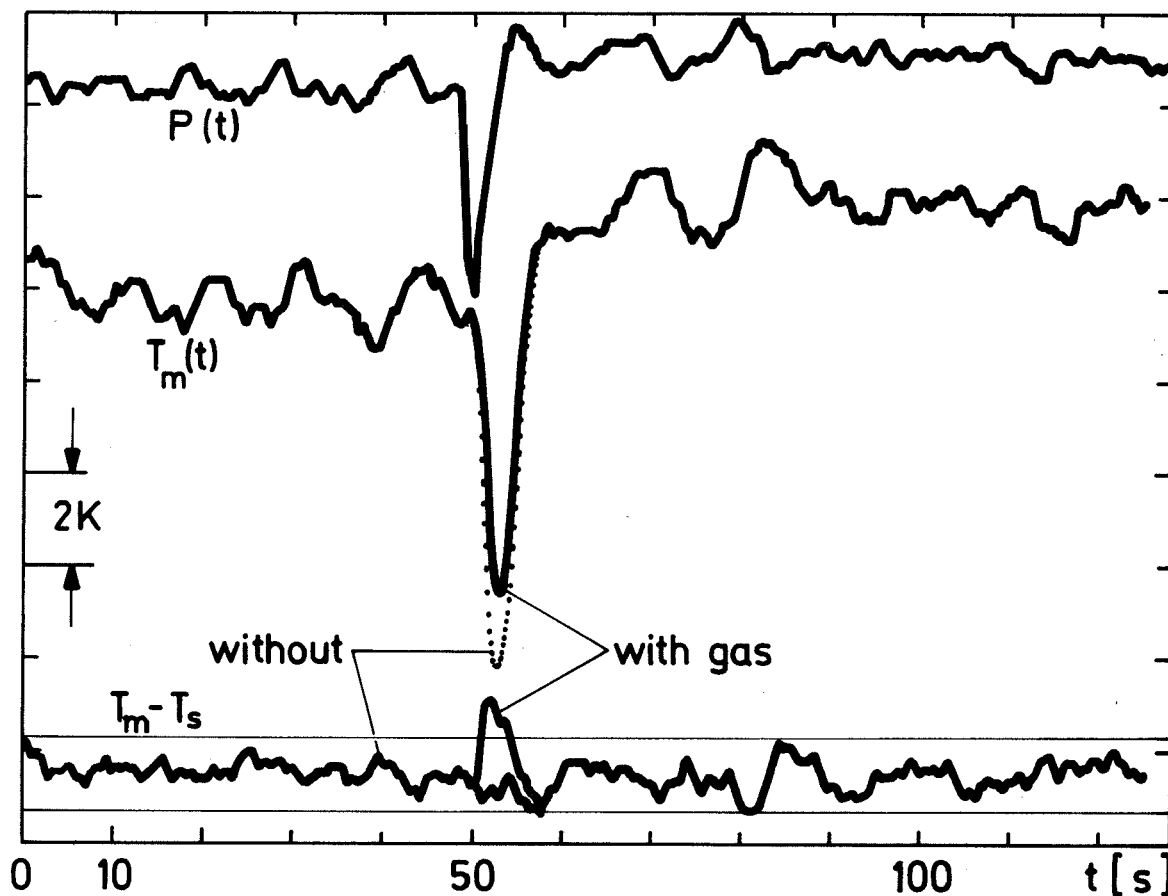


Fig.11 Normal and balanced outlet temperature signals with and without 1% simulated gas content

G. Weinkötz, H. Martin, L. Krebs

DETECTION OF COOLANT DISTURBANCES IN THE FUEL ELEMENTS OF AN
LMFBR BY TEMPERATURE FLUCTUATION ANALYSIS

International Atomic Energy Agency

International Working Group Nuclear Power Plant Control and Instrumentation Specialists' Meeting on "Procedures and Systems for Assisting an Operator during Normal and Anomalous Nuclear Power Plant Operation Situations", 5-7 Dec. 1979, Munich, F.R.G.

DETECTION OF COOLANT DISTURBANCES IN THE FUEL ELEMENTS OF AN LMFBR
BY TEMPERATURE FLUCTUATION ANALYSIS

G. Weinkötz, H. Martin, L. Krebs

Kernforschungszentrum Karlsruhe
Institut für Reaktorbauelemente
Postfach 3640, D-7500 Karlsruhe
Federal Republic of Germany

ABSTRACT

Sodium temperature noise measurements were performed at the coolant fluid outlets of an electrically heated 169-rod bundle and also a 28-rod bundle, with different partially blocked coolant sections. On both test assemblies, a flow mixer was installed downstream of the bundle fluid exit plane. For all tests, measuring planes with three-wire thermocouples containing both steel-sodium and chromel-alumel junctions were located on the upstream and downstream sides of the flow mixer. Statistical parameters such as the root mean square (RMS) and the power spectral density (PSD) of temperature fluctuations were investigated. The influences of flow velocity, heat flux, thermocouple cut-off frequency, and different blockage sizes on these statistical parameters were analysed. Moreover, an essential result of interpretation of the experiments is that a characteristic geometrical bundle coefficient was found which indicates coolant channel disturbances only, independent of the operational conditions of the bundles such as heat flux and flow velocity.

INTRODUCTION

During design and licensing procedure, the availability and performance of nuclear power plant safety instrumentation is always of importance. In addition, during operation and especially during emergencies the question arises, how can safety instrumentation be improved?

However, the impact of adding reactor instrumentation should be as small as possible. Therefore the measurement of the mean (time averaged) temperature is planned at every fuel element outlet of the SNR 300, the German prototype of an LMFBR, but not the measurement of mass flow.

Nevertheless, there is an urgency to detect cooling disturbances in the earliest stage. Moreover, it is of interest to identify the fuel element in

which such disturbances occur. Integral measurement devices are not suitable for local surveillance.

By analysing the mean temperature at every fuel element outlet, blockages involving more than 30% of the cooling cross-section can be detected. One possibility to improve the sensitivity is the compensation method /1/, proposed by Edelmann.

Another method is the analysis of temperature fluctuations superimposed on the mean temperature. In Ref. /2/, the connection between mean temperature and temperature fluctuation is investigated. It was demonstrated that the analysis of temperature fluctuations provides a higher sensitivity to detect cooling disturbances, than the analysis of mean temperature. One advantage of this method is the fact that no additional sensors are needed. Only the normally installed chromel-alumel thermocouples must be replaced by three-wire thermocouples of the same diameter. This provides the possibility of measuring the mean temperature and the temperature fluctuations, respectively, using the steel-sodium junction of the third wire /3/. The additional equipment requirements are restricted to the data acquisition system outside of the reactor core.

In the following experimental results of temperature fluctuation measurements are presented. In cooperation with the Institut für Reaktorentwicklung at the Nuclear Research Center Karlsruhe (KfK) and the Netherlands Energy Research Foundation (ECN) in Petten, the measurements were performed at the outlet of an electrically heated 169-rod bundle /4/ and a 28-rod bundle /5/. The influence of a flow mixer and the experimental parameters

- flow velocity
- cut-off frequency of the thermocouples
- rod power (heat flux)
- coolant blockage - sizes

on the intensity and frequency of the temperature fluctuation signals was investigated. Former results are published in Ref. /6/ and /7/.

STATISTICAL ANALYSIS

One of the mainly used characteristic values of a stochastic signal is the standard deviation or the Root Mean Square (RMS) value σ , defined by the relation

$$\sigma = \sqrt{\frac{1}{T} \cdot \int_0^T \delta^2(t) dt} \quad (1)$$

where t is the time, T the measuring time and $\delta(t)$ the fluctuating part of a temperature signal. In some cases it may be advantageous to use the square of the RMS value, the Mean Square (MS) value δ^2 . An important characteristic function is the Power Spectral Density (PSD) of a stochastic signal, the FOURIER-transforms of the Autocorrelation Function (ACF). The ACF is given by

$$\Phi_{\delta\delta}(\tau) = \frac{1}{2T} \cdot \int_{-T}^{+T} \delta(t) \cdot \delta(t-\tau) dt \quad (2)$$

and from this the PSD

$$S(f) = \int_{-\infty}^{+\infty} \Phi_{\delta\delta}(\tau) \cdot e^{-j2\pi f\tau} dt \quad (3)$$

τ means the correlation time and f the frequency.
The relation

$$\sigma^2 = \int_{-\infty}^{+\infty} S(f) df \quad (4)$$

shows additionally a relationship between the MS and the PSD.

Using the relations (1) to (4) the temperature fluctuation signals at the outlet of the electrically heated rod bundles were analysed.

DESCRIPTION OF THE TEST FACILITIES

Figure 1 illustrates the scheme of the two subassemblies. On the right-hand side the 169-rod subassembly (KNS) is sketched. On the left-hand side of the diagram is a sketch of the 28-rod subassembly of KfK-ECN. With respect to geometry, the 28-rod subassembly represents a 60° sectional subassembly of the 169-rod full subassembly. The rod diameter and the pitch correspond to the values of the SNR-300. On both test subassemblies a flow mixer was also installed downstream of the bundle outlet.

The first 169-rod subassembly had a central blockage of 49%. An edge blockage was introduced into the second 169-rod subassembly which blocked off 21% of the cross section of the coolant flow. The 28-rod subassembly had a cooling channel blockage of 68% in the first experiment and 34% in the second experiment. The blockages were located near the coolant flow inlet of the rod bundles. At the ECN experiment all of the 28-rods were electrically heated whereas at the KNS-experiment only 88 rods in the region of the blockage were heated.

In both subassemblies, temperature measurement lances were installed perpendicular to the flow direction at the subassembly outlet (measuring plane 1) and downstream of a flow mixing system (measuring plane 2). Each thermocouple measuring lance carried up to ten three-wire thermocouples of 0,5 mm diameter. Three-wire thermocouples consist of an insulated chromel-alumel measuring junction and a steel-sodium element. The cut-off frequency of the chromel-alumel thermocouples is around 12 Hz. The cut-off frequency of the steel-sodium thermocouples is greater than 100 Hz.

MEASUREMENTS AND RESULTS

Influence of Flow Mixer and Flow Velocity

Typical power spectral densities of the kind measured by means of steel-sodium thermocouples are shown in Figure 2. Signal parts up to 0.1 Hz were high pass filtered. The first analysed frequency point is 1.5 Hz. Immediately at the bundle outlet, measuring plane 1, the higher frequency signal parts of the temperature fluctuations are much more pronounced than downstream of the flow mixer. The frequency drop of the spectra corresponds roughly to a first order low pass approximately in the first two decades of the power spectral density. Therefore a cut-off frequency of the temperature fluctuation signals can be determined by the 3db decay of the PSD.

The influence of the flow velocity on these cut-off frequencies is shown in Figure 3. The dash-dotted line represents the curve of the cut-off frequencies at the bundle outlet, which shows an increase proportional to the flow velocity. At the maximum flow velocity of 4 m/s within the subchannels, corresponding

to a Reynolds number of about 80.000, the analysis of temperature fluctuations shows a cut-off frequency of 96 Hz.

The lower solid curve clearly demonstrates the influence of the flow mixer: Downstream of the flow mixer, the cut-off frequency is no longer proportional to the flow velocity.

Influence of the Cut-Off Frequency of Thermocouples

Another important experimental parameter is the cut-off frequency of the thermocouples. Now, the influence of this parameter will be considered. Two cases are distinguished:

1. The cut-off frequency of the thermocouple is higher than the cut-off frequency of the temperature fluctuations at maximum flow velocity v_{\max} , i.e. within the operational range ($1\text{m/s} < v < 4\text{m/s}$)

$$f_g(\text{T.C.}) > f_g(\delta_{v_{\max}})$$

2. The cut-off frequency of the thermocouple is lower than the cut-off frequency of the temperature fluctuations at minimum flow velocity v_{\min} , i.e. within the operational range ($1\text{ m/s} < v < 4\text{m/s}$)

$$f_g(\text{T.C.}) < f_g(\delta_{v_{\min}})$$

Within the two cases, the relationship between either the mean square value or the RMS value of temperature fluctuations with heat flux and flow velocity were investigated.

Considering the condition of case 1. the PSD dependence on the flow velocity at constant heat flux is plotted in the lower part of Figure 4. Two changes in the spectra can be observed dependent on flow velocity:

1. The cut-off frequency of the temperature fluctuations increases proportionally to the flow velocity.
2. The magnitude of the power density decreases with one over velocity squared.

As mentioned before, the surface area inside the power spectral density corresponds to the mean square. Therefore the RMS value σ is proportional one over the root of the velocity

$$\sigma \sim \frac{1}{\sqrt{v}} \quad \text{for case 1: } f_g(\text{T.C.}) > f_g(\delta_{v_{\max}}) \quad (5)$$

This result is shown in the upper part of the Figure 4.

For the instrumentation of a nuclear power plant, this case is significant because generally the temperature fluctuation frequencies do not increase proportionally to the flow velocity downstream of a flow mixer. This behaviour has no additional influence, if the cut-off frequency of the thermocouple is lower than the cut-off frequency of temperature fluctuations at minimum flow velocity as provided in case 2. This is shown in Figure 5. Again, the magnitude of the power density decreases with one over the velocity squared. But the frequency of the power spectral density is determined by the cut-off frequency of the thermocouple and therefore is

independent of the flow velocity. Corresponding to the RMS value we obtain the relation:

$$\sigma \sim \frac{1}{v} \text{ for case 2: } f_g(\text{T.C.}) < f_g(\delta_{v_{\min}}) \quad (6)$$

σ is proportional one over the velocity. However, if the cut-off frequency of the thermocouple is in the region of the cut-off frequency of the temperature signal occurring for various flow velocities, no steady relationship between the RMS-value of the temperature fluctuations and the velocity is obtained for the whole range of velocity investigated (1 to 4 m/s).

Influence of Heat Flux

The influence of the heat flux on the PSD of the temperature fluctuations at constant flow velocity is described in the lower part of Figure 6. The magnitude of the power increases proportionally to the square of the heat flux, whereas the cut-off frequency of the temperature fluctuations is not a function of heat flux. Therefore the RMS value is proportional to the heat flux at constant flow velocity at the two mentioned cases:

$$\sigma \sim N \text{ for case 1 and case 2} \quad (7)$$

This is shown in the upper part of Figure 6.

Connection between RMS Value and Coolant Temperature Rise

The heat flux and the flow velocity are connected with the temperature rise ΔT of the coolant between the bundle inlet and outlet by the relation:

$$\Delta T \sim \frac{N}{v} \quad (8)$$

Therefore a connection must also exist between the RMS value σ and the coolant temperature rise ΔT . Again the two cases are distinguished.

Case 1: $f_g(\text{T.C.}) > f_g(\delta_{v_{\max}})$

The connection of relation (8) with relations (5) and (7) leads to:

$$\sigma^2 \sim \Delta T \text{ for } N = \text{const.} \quad (9a)$$

$$\sigma \sim \Delta T \text{ for } v = \text{const.} \quad (10)$$

Case 2: $f_g(\text{T.C.}) < f_g(\delta_{v_{\min}})$

The connection of relation (8) with relations (6) and (7) leads to:

$$\sigma \sim \Delta T \text{ for } N = \text{const.} \quad (9b)$$

$$\sigma \sim \Delta T \text{ for } v = \text{const.} \quad (10)$$

These relations demonstrate that only in case 2

$$\sigma \sim \Delta T \tag{11}$$

is valid independent of the change of either heat flux or flow velocity. By contrast in case 1 the RMS value will be different according to the change of either heat flux or flow velocity. Therefore in this case no general valid relation can be found between the RMS value and the coolant temperature rise ΔT . The results of these considerations are summarized in Table 1.

	Case 1	Case 2
experimental conditions	$f_g(\text{TC}) > f_g(\delta_{v_{\max}})$	$f_g(\text{TC}) < f_g(\delta_{v_{\min}})$
heat flux $N = \text{const.}$	$\sigma^2 \sim 1/v$	$\sigma \sim 1/v$
flow velocity $v = \text{const.}$	$\sigma \sim N$	$\sigma \sim N$
coolant temp. rise $(N/v) \sim \Delta T = \text{const.}$	$\sigma = f(N, v)$	$\sigma = \text{const.}$

Table 1: Dependence of the RMS value σ on heat flux and flow velocity at different cut-off frequencies of thermocouples.

The Geometrical Bundle Coefficient k

On the basis of the relations (8) and (11) a proportionality coefficient k can be defined as follows for condition $f_g(\text{T.C.}) < f_g(\delta_{v_{\min}})$

$$k = \sigma \cdot \frac{v}{N} \tag{12}$$

In this equation, $k \text{ [K} \cdot \text{cm}^3/\text{Ws}]$ is a dimensional coefficient, which is independent of the variation of heat flux and flow velocity. If k does change, an essential reason would be a coolant channel disturbance. Therefore, k is defined as geometrical bundle coefficient. Since the bundle coefficient k is defined under the condition, that the cut-off-frequency of the thermocouple is restricted (case 2), it is not useful to analyse the entire frequency range of temperature fluctuations. A small frequency range of about 8 Hz is sufficient to detect coolant channel disturbances. This is an important result which allows one to develop a simple electronic signal processing device. In Figure 7 an on-line plot of the k value versus time is shown. The measurement was performed using 169-bundle test section. During the measuring time, the heat flux was increased in two steps at constant flow velocity. The RMS value increases with increasing heat flux, while the bundle coefficient k (lower curve) is constant during the measuring time. Corresponding to the condition of Case 2, $f_g(\text{T.C.}) < f_g(\delta_{v_{\min}})$ the temperature signals were low-pass filtered at 8 Hz.

Influence of Different Blockage Sizes

The influence of different blockage sizes on the RMS value and the bundle coefficient k , is now discussed. Figure 8 shows some results from the 28-rod test section with coolant blockage sizes of 34% and 68%. The temperature noise measurements were carried out downstream of the flow mixer. The temperature signals were low-pass filtered at 8 Hz corresponding to the condition of Case 2. On the left-hand side of the figure, the RMS value and the bundle coefficient k are shown as a function of heat flux at constant velocity. The lower solid curve demonstrates a proportional increase of the RMS value to the heat flux at blockage size of 34%. An extension of the blockage size to 68% caused an increase of the RMS value across the whole power range as shown by the dash-dotted line. On the right-hand side of the figure the RMS value is plotted versus flow velocity at constant heat flux. As analysed before in reference to Case 2, the RMS value of temperature fluctuations decreases inversely proportional to the flow velocity. Also, the influence of different blockage sizes on the RMS value is demonstrated in the lower two curves. The upper solid line and the dash-dotted line in both diagram parts present the bundle coefficient k . Independent of the flux and flow velocity, the bundle coefficient k indicates only the different blockage size.

Mean Temperature- and RMS- Profiles at the Bundle Outlet

28-Rod Bundle

The lateral temperature profile measured at the bundle outlet, measuring plane 1, and its associated RMS profile are plotted in Figure 9. The upper part of the figure shows the bundle cross section with the cooling channel blockage and the lateral thermocouple positions downstream of the fluid exit plane. The dotted curves in the diagram demonstrate the temperature and RMS profiles corresponding to a blockage size of 34%. The dash-dotted curves show the results at a blockage of 68%. An extension of the blockage size to 68% causes an increase in the RMS value by about a factor two at the most; however, the mean temperature rises only approximately 2%.

169-Rod Bundle

While in the 28-rod bundle all rods were heated electrically, only the rods in the region of the blockage were heated in the 169-rod bundle, i.e. a maximum of 88 rods. Transition from a central blockage (first bundle experiment) to an edge blockage also resulted in a different thermocouple configuration at the bundle outlet. The lateral temperature profiles measured at the bundle outlet and their associated RMS profiles of the temperature fluctuation are represented in Figures 10 and 11. Both for the central blockage and for the edge blockage the maximum RMS value measured of the temperature fluctuation lies in the transition zone between blocked and unblocked bundle cross-sections.

COMPARISON OF THE RESULTS

The results of measurements analysed at the two test facilities (28-rod bundle and 169-rod bundle) are summarized in Figures 12 and 13. For comparison the geometrical bundle coefficient k was used. The temperature signals investigated were low pass filtered at 8 Hz. Figure 12 is a plot of the maximum geometrical bundle coefficient k , determined at the bundle outlet, versus the size of the blockage. The maximum geometrical bundle coefficient k increases with increasing blockage. Since measurement results are not available for this bundle in the absence of blockage, the k -values determined were supposed to constitute a

0% blockage downstream of the unblocked bundle cross-section. These measured values agree well with measurements made on a 19-rod bundle without blockage. Figure 13 is a plot of the lateral k-values obtained downstream of the flow mixer as a function of the size of blockage. The lateral k-value downstream of the mixer is scattered by 20% at the maximum as compared to the averaged value. In case of the 28-rod bundle, a clear rise can be recognized of the lateral k-value when the blockage size increases from 34%. Much greater lateral k-values as compared to the central blockage of 49% are found for the 169-rod bundle with an edge blockage of 21%. The measured values for the 0% blockage were taken from Figure 12.

CONCLUSIONS

The results obtained up to now from temperature noise measurements downstream of the fluid exit plane of simulated LMFBR subassemblies allow the following preliminary statements to be made:

- The RMS value of the temperature fluctuations is a possible statistical parameter to be used for the detection of cooling channel blockage. The influence of heat flux and flow velocity can be described for a defined range of operation.
- When the cut-off frequency of the thermocouple is lower than the cut-off frequency of the temperature fluctuations at minimum flow velocity, a characteristic geometrical bundle coefficient k was found which indicates coolant channel disturbances only, independent of power and flow velocity.
- A coolant channel blockage can be detected by installing only one thermocouple downstream of a flow mixer. The uncertainty of the measurements is about 20%.

REFERENCES

- /1/ M. Edelmann: "Noise and D.C. Balanced Outlet Temperature Signals for Monitoring Coolant Flow in LMFBR Fuel Elements", Proc. SMORN II in Progr. Nucl. Eng., Vol. 1 No. 2-4 (1977), p. 543
- /2/ L. Krebs: "Ausbreitung von Temperaturstörungen in begrenzter Strömung hinter einen Düsenblock", KfK 2846, (Nov. 1979)
- /3/ J. Benkert: "Untersuchungen von Temperaturfluktuationen in flüssigem Natrium zur Ermittlung charakteristischer Strömungsparameter und Thermo-elementübertragungsfunktionen", Dissertation, TU Hannover (1977)
- /4/ A.J. Brock, F. Huber, W. Pepler: "Temperature Distribution and Local Boiling Behind a Central Blockage in a Simulated FBR Subassembly", International Meeting on Fast Reactor Safety and Related Physics, Chicago, Illinois (5-8 Oct. 1976)
- /5/ J.E. de Vries, J.C. Hoebe, B. Dorr: "Recent Results of a Local Blockage Experiment in a Sodium-Cooled Electrically Heated Bundle", International Meeting on Fast Reactor Safety and Related Physics, Chicago, Illinois (5-8 Oct. 1976)
- /6/ L. Krebs, G. Weinkötz: "Indication of a Coolant Blockage in a Fuel Element of a Sodium-Cooled Reactor by Temperature Fluctuation Measurements with Steel-Sodium Thermocouples", Proceedings of the International Meeting on Fast Reactor Safety and Related Physics, Chicago, Illinois (5-8 Oct. 1976)
- /7/ L. Krebs, G. Weinkötz: "Detection of Local Boiling in an LMFBR Subassembly by Temperature Fluctuations Analysis at the Outlet", Proc. SMORN II in Progr. Nucl. Eng., Vol. 1 No. 2-4 (1977), p. 507

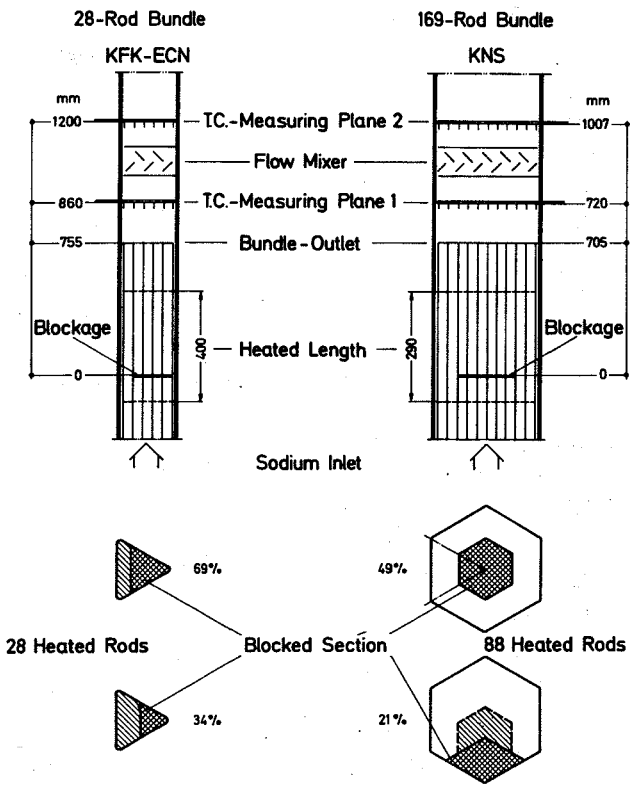


Fig. 1:
Sketch of the two Subassemblies,
Location of Blockages and Thermocouples

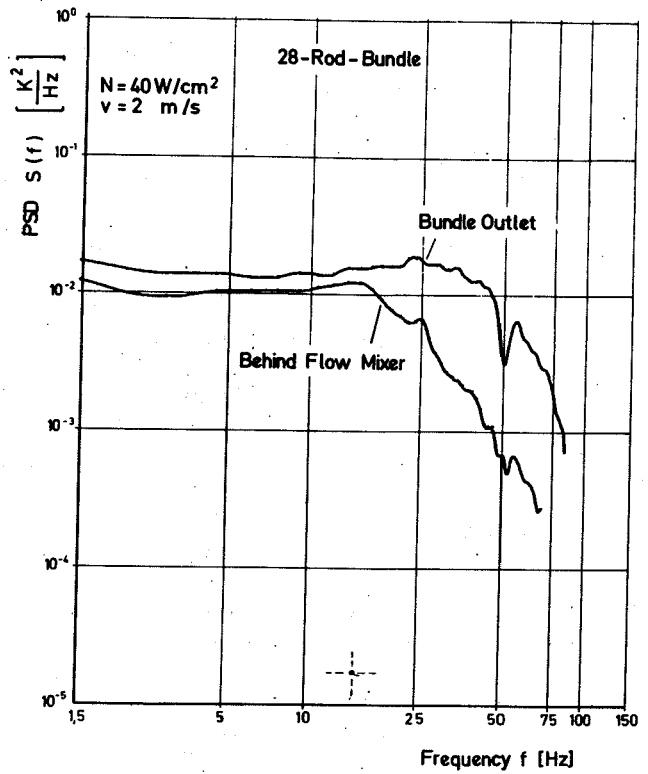


Fig. 2:
PSD of Temperature Fluctuations,
Measured by Steel-Sodium T.C.

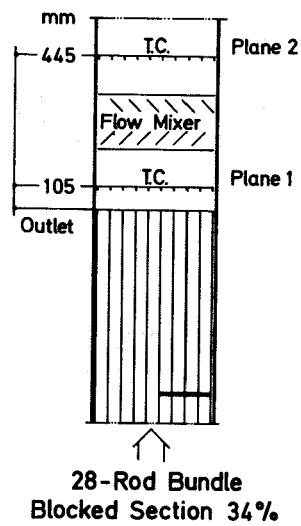
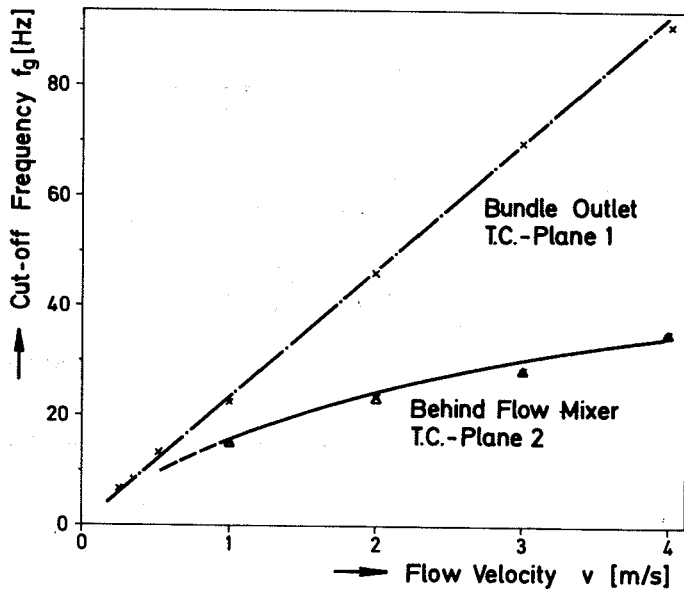


Fig. 3:
Cut-off Frequency of Temperature Fluctuations versus Flow Velocity,
Measured by Steel-Sodium T.C.

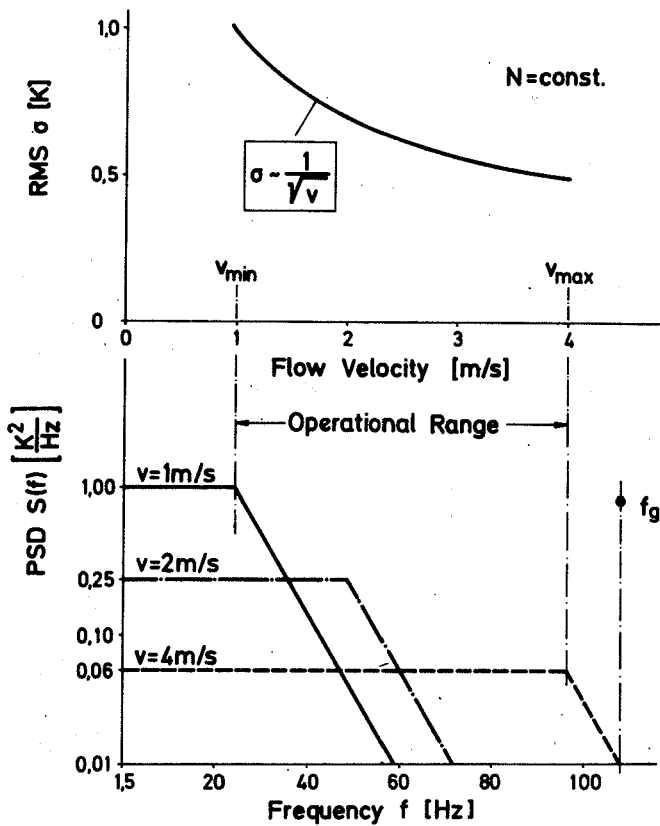


Fig. 4:

Influence of Flow Velocity on the PSD and RMS Value under the Condition

$$f_g(\text{T.C.}) > f_g(\delta_{v_{\max}})$$

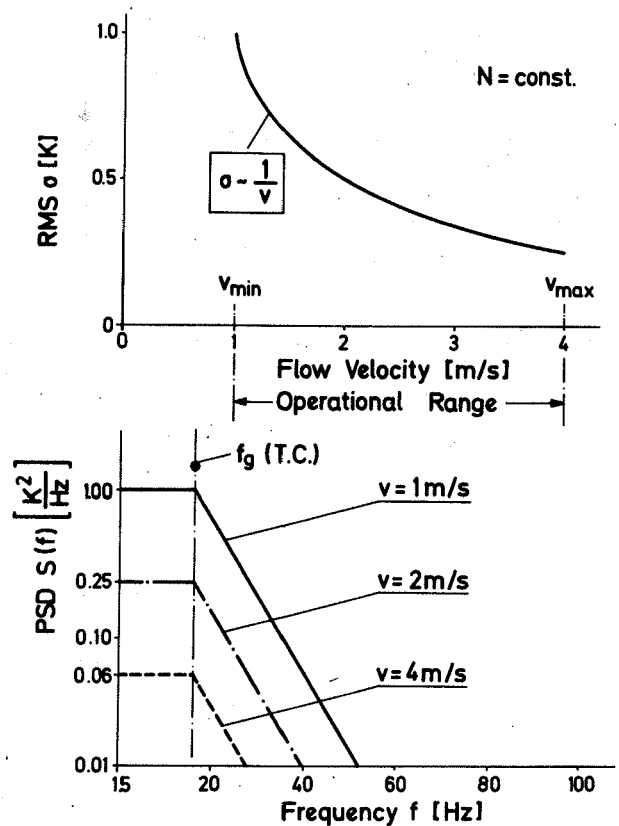


Fig. 5:

$$f_g(\text{T.C.}) < f_g(\delta_{v_{\min}})$$

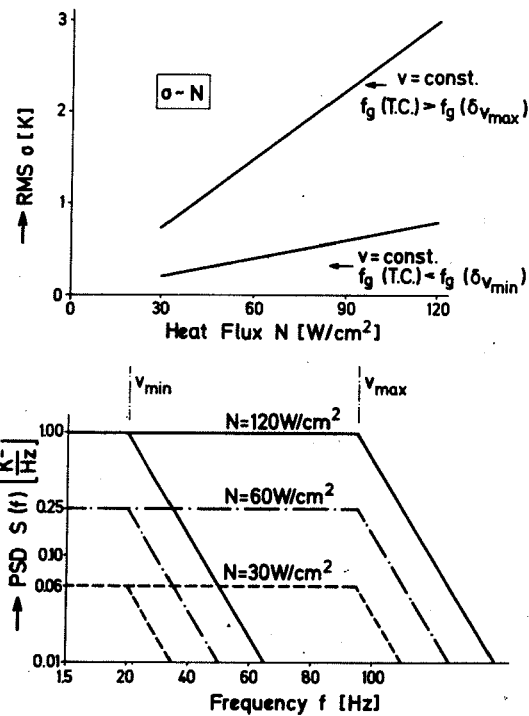


Fig. 6:

Influence of Heat Flux on the PSD and RMS Value.

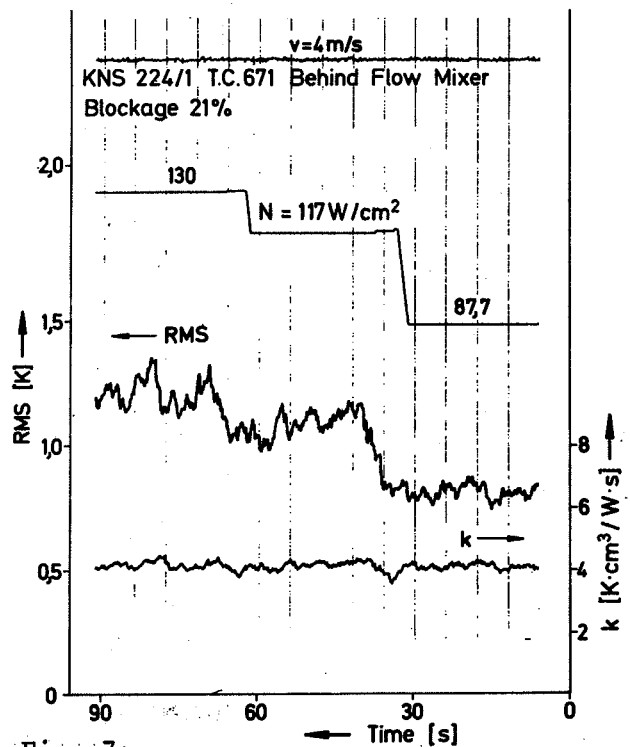


Fig. 7:

RMS of Temperature Fluctuations and Geometrical Bundle Coefficient versus Time at Different Heat Flux (169-Rod Bundle).

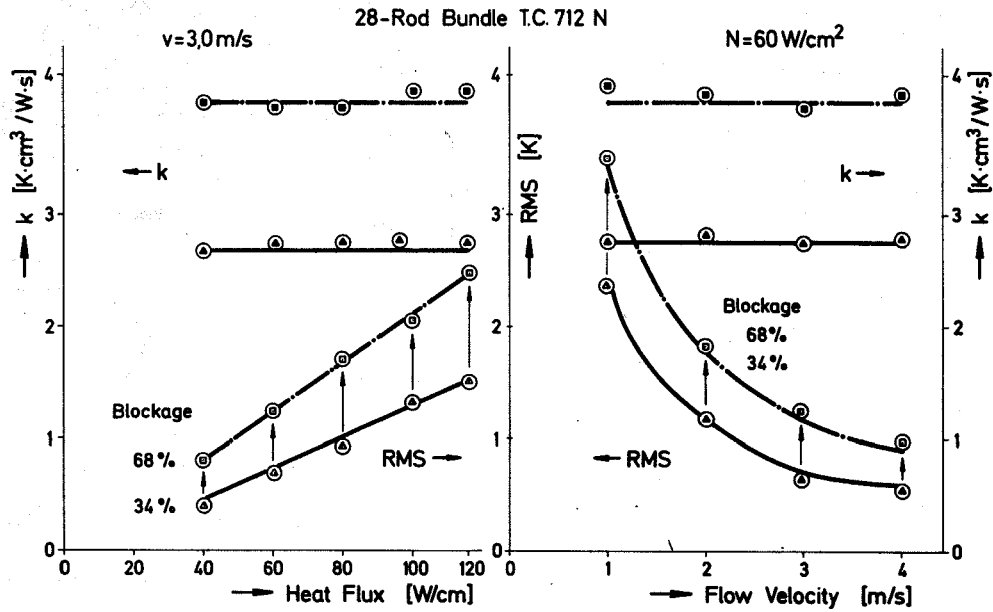


Fig. 8: Influence of Different Blockage Sizes on RMS Value and Geometrical Bundle Coefficient, Dependence on Heat Flux and Flow Velocity.

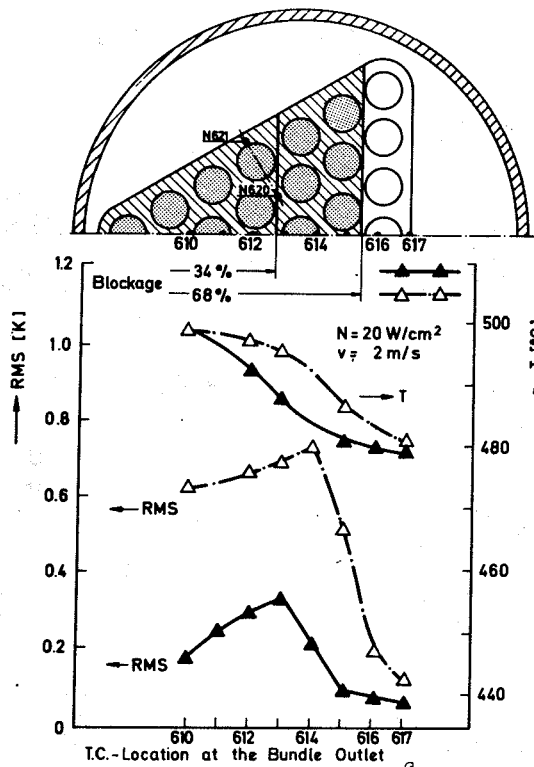


Fig. 9: Temperature- and RMS- Profile of the 28- Rod Bundle (Blockage Size 34% and 38%)

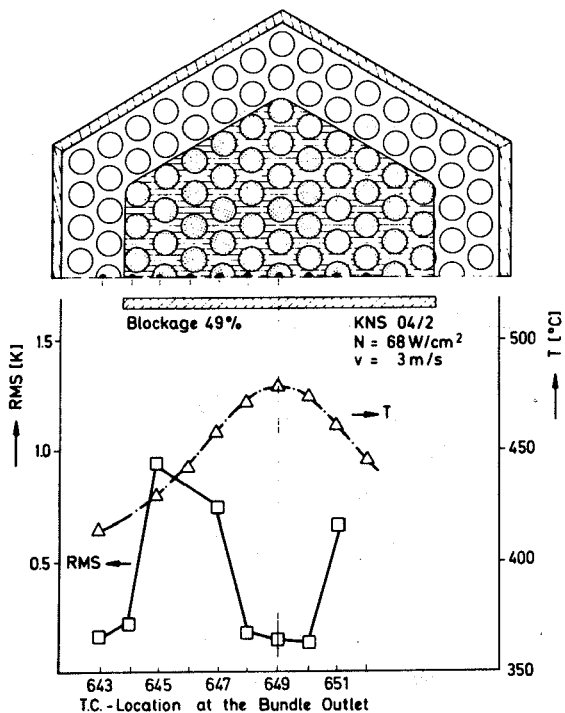


Fig. 10:
Temperature- and RMS-Profile of the 169-Rod Bundle
(Central Blockage)

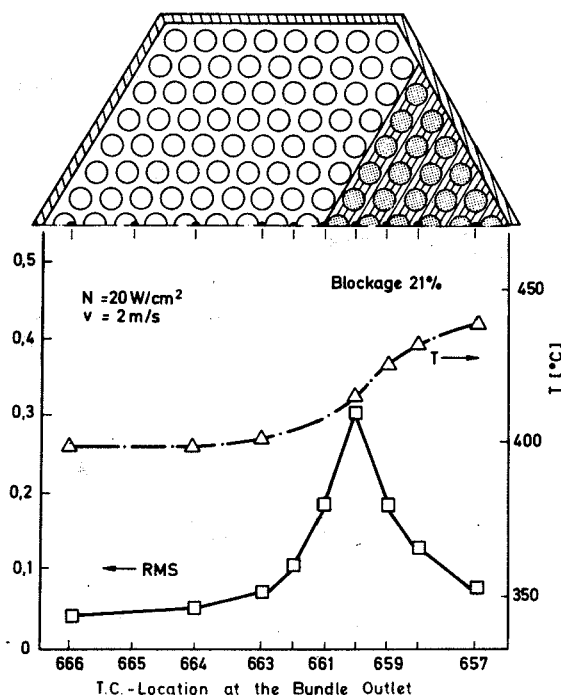


Fig. 11:
Temperature- and RMS-Profile of the 169-Rod Bundle
(Edge Blockage)

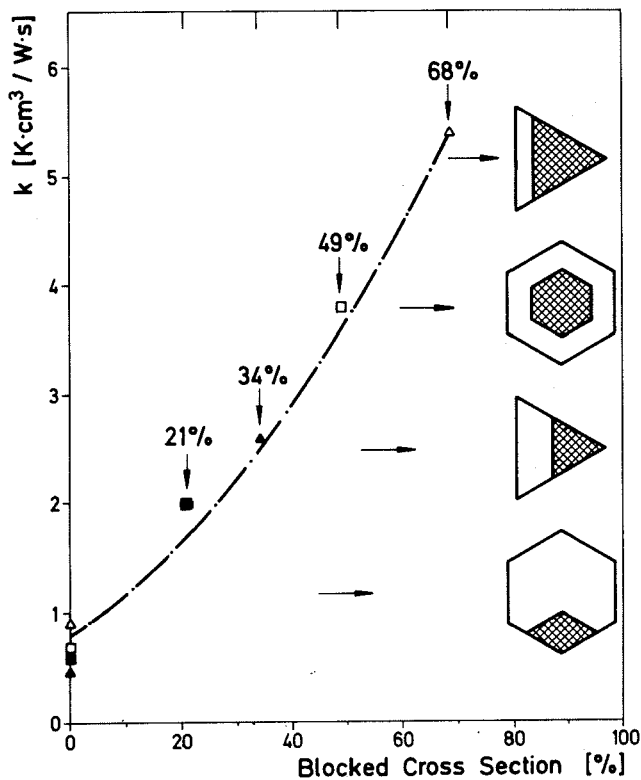


Fig. 12:
Max. Geometrical Bundle Coefficient k at the Bundle Outlet, Dependence on the Blockage Size.

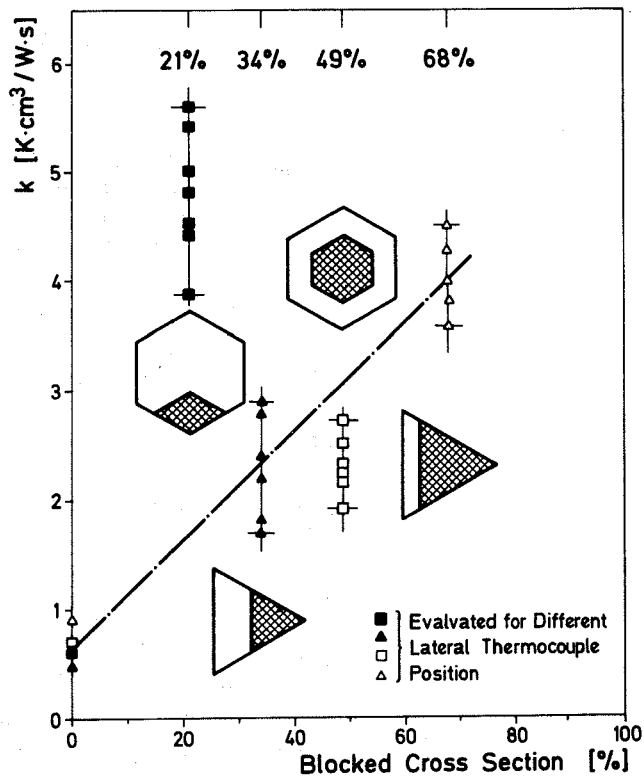


Fig. 13:
Geometrical Bundle Coefficient k downstream of the Flow Mixer, Dependence on the Blockage Size

P. Liewers, P. Schumann, F.P. Weiß

USE OF NOISE DIAGNOSIS FOR SURVEILLANCE OF PARTICULAR
DISTURBING PROCESSES IN A PRESSURIZED WATER REACTOR

INTERNATIONAL ATOMIC ENERGY AGENCY
INTERNATIONAL WORKING GROUP ON NUCLEAR POWER PLANT CONTROL
AND INSTRUMENTATION

SPECIALIST'S MEETING on
PROCEDURES AND SYSTEMS FOR ASSISTING AN OPERATOR DURING
NORMAL AND ANOMALOUS NUCLEAR POWER PLANT OPERATION SITUATIONS
5 - 7 December 1979, Munich, Federal Republic of Germany

Use of Noise Diagnosis for Surveillance of
Particular Disturbing Processes in a Pressurized Water
Reactor

P. Liewers, P. Schumann, F.-P. Weiß

Zentralinstitut für Kernforschung, Rossendorf, DDR

Use of Noise Diagnosis for Surveillance of
Particular Disturbing Processes in a Pressurized Water Reactor

P. Liewers, P. Schumann, F.-P. Weiß

Central Institute for Nuclear Research, Rossendorf, GDR

Abstract

Up to now the automatic application of noise diagnosis has been impossible because of the experimental character of noise methods and of the probabilistic character of their results. The importance of diagnostic results has induced the idea to implement a rough surveillance monitoring of known disturbing processes, which only gives the output information "normal" or "suspicious" to the operator. Indicated suspicious states must be investigated in more detail by noise specialists. A few such monitors are being tested now. Their results stored in a data record office also serve as recommendations for the next revision period.

1. Introduction

Noise diagnosis has become well-known in the field of nuclear energy. Everybody knows the convincing results of the investigations concerning the measurement and the identification of core barrel movements (Fry [1], Bastl [2]), the successful application of loose parts monitoring (Wach [3], Zigler [4]) and the promising efforts which are undertaken for leak detection (Dio [3]).

In spite of this noise techniques are only rarely used in nuclear power plants. This fact may be caused by the necessity of additional equipment as well as noise specialists who are able to interpret the information content of the noise signals. Although both are expensive the results have a probabilistic character only. That means up to now the integration of noise methods into normal control and instrumentation has seemed to be questionable.

In our opinion today noise diagnosis is in the state of an experimental method, which is very useful in the hand of a specialist and which can give helpful informations additionally to those of conventional methods. Undoubtedly the high expenses of noise techniques can be accepted in the case of a damage as demonstrated in Harrisburg (Majo [5]) or during commissioning [3] when a precise investigation of initial disturbing processes is necessary, but for general application the expense is too high. Therefore efforts have been made to find a possibility for a continuous application of noise methods to some general important disturbing processes using only a few special noise techniques and partly renouncing noise specialists. A satisfying solution has not yet been found.

Some aspects of monitoring will be discussed in the following by representing a hypothesis for our work in this field.

2. The basic idea of a limited monitoring

The situation at a nuclear power plant is the following (fig. 1). The reactor is equipped with an instrumentation which signals are the input information of the automatic control and safety system. The operator observes the whole process and controls it taking into account a lot of boundary conditions.

To apply noise methods an additional equipment must be installed, consisting of a noise instrumentation and more or less electronics for data processing. The noise specialist is a part of the noise diagnosis system, he extracts the informations from the noise signals by means of analysing and identifying procedures and gives his conclusions to the operators. These informations are precise in the sense of mathematical statistics and can be of sufficient confidence only for an already well-known disturbing process.

This situation is especially interesting for the above mentioned method of loose parts detection [3]. The detection principle is well-known: Impacts of loose parts produce sound waves picked up by an acceleration detector. Sound waves with an amplitude greater than an adjustable threshold will be registered automatically using a transient recorder of a similar equipment whereby an alarm signal is given to the operator. During a long time interval without alarms the operator can be sure within certain probability limits that big loose parts don't exist. However, after an alarm signal has occurred the noise specialist must be called to interpret the stored bursts, to check their confidence and to calculate parameters as the most probable location and the order of magnitude of the loose part. Conclusions concerning the further operation can only be drawn in an agreement between the operating staff and the noise specialist.

In our opinion the basic idea of this method can be generalized to obtain a monitor conception. Instead of the complete noise diagnostic system including the noise specialist relatively simple monitors supervise the most essential disturbing pro-

cesses during normal operation. The purpose of these monitors is twofold:

- (1) indication of a normal or suspicious state of the disturbing process for operating purposes
- (2) storage of noise signals from suspicious situations for a further precise analysis by the noise specialists.

The advantage of this monitor conception is the use of only simple electronics and the partly renunciation of noise specialist. The disadvantage is his limitation. At present only the decision "normal" or "suspicious" can be given by a rough monitoring. A reference to the human reaction upon suspicious noise is very instructive in this context. After having heard suspicious noise we try to investigate the reason more precisely by means of more precise instruments - e.g. by means of our eyes. To do this we have to wait for a repetition of suspicious noise, if there is no repetition we have to recapitulate the impression from our mind. Obviously our intelligence distrusts the significance of noise.

The distrust seems also to be evoked even in the case of rough monitoring because particular attributes of the disturbing process cannot be predicted in general. In general, according to the experimental character of noise methods a systematical improvement of monitors is only possible by calibration and adjustment during operation of the reactor. Only after having found the optimum for the adjustment the monitor output information can be given directly to the operator. As long as there is no alarm signal it is not necessary to consult a noise specialist. But if alarm signal have occurred the noise specialist has to explain the reasons by special investigations using the stored signals. These stored signals are also used to derive recommendations for the next revision period.

On the other hand the results of the inspection are well suited for the adjustment of the monitor. The loads and perils being induced by the disturbing processes are unknown in many cases.

But in the course of years this disturbances may become more and more important. Such disturbing processes have to be supervised in their trends to extract some signs for the revision. Some investigations concerning the supervision of trends performed at a FWR will be reported on in the following.

3. Monitors for partial disturbing processes at a FWR

Noise analysis system for pressurized water reactors of the WWER-440 type have been working in the GDR for some years [6]. The most progressive version RAS-2 is a prototype for research and routine investigations which is now being completed by monitors.

The instrumentation includes about 120 noise signals per reactor from the whole primary circuit. Half of them are neutron flux signals at incore and excore positions. They are thought to detect disturbing processes inside the pressure vessel. Acceleration detectors at the surfaces of the pressure vessel, of pipes, pumps and of the steam generators are installed for vibration and loose parts detection. For the investigation of control element movements there are acceleration detectors at the guide tubes of the elements too, and there are piezoelectric pressure fluctuation detectors for the diagnosis of pumps and for the aim of noise source separation.

After preamplification noise signals are conditioned, tested and programmed to several outputs in the central measurement unit. A data processor capable of programming, identifying and scaling the signals automatically is coupled with the measurement system. A software package including all modern signal analysis methods is available to the processor and can be used as identification subroutines for particular disturbing processes if required. According to the above mentioned monitor conception the main task of the processor is to check and to control the monitors, to store their output informations in a data record office

and occasionally to perform special investigations for monitor calibration. So the processor is ready for special investigations if the monitor detects a suspicious situation.

The whole equipment including mathematical models of disturbing processes represents the noise diagnosis system shown in fig. 1. On the one hand it must be completed by the experiences and the intelligence of the noise specialist and by monitors on the other hand.

Monitors should be as simple as possible electronic devices with a high efficiency in respect of the supervised disturbing processes. They must work as continuously as necessary. For this a monitor can be implemented in different manners. At our PWR e.g. the supervision of pressure vessel oscillations seems only to be necessary periodically in time intervals of a few weeks, because the average oscillation amplitude of some micrometers produce a maximum tension which is more than one order of magnitude smaller than allowed. Therefore it seems to be sufficient monthly to perform a spectral density analysis for all of the thirteen acceleration signals at the surface of the pressure vessel and to store the results. This discontinuous software monitoring is an additional function of the data processor. It might be useful to make a scaled display of the passband limited signals at the main frequencies of the oscillation e.g. when pumps are put into or out of operation.

Systematic investigations of control element movements have shown an experimental possibility of separating a fluctuation component produced by only one special control element from a complex neutron noise signal with the help of the information of the sound level signal from that special guide tube [7]. This separation is possible though all other control elements are moving in a similar manner. These experiments give a lot of informations [8], but they are too complicated for a simple monitoring. Sound events from the guide tubes produced by an impact between the element and the channel wall are better suited for monitoring, because they are generated during the

potential load process. At present a monitor is being tested which supervises the intensity and the repetition frequency of sound events in several frequency ranges. This monitor is capable of processing 30 sound signals, it is a multiplexing device of hybrid type. The results accumulated in the data record office can be used for a classification into several suspicious groups. The quality of classification can be improved by the results of the next control element inspection. Provided that the calibration was right the monitor will give actual informations about unwanted strong impacts. So the operator can avoid a critical rod position.

There is a second hybrid type monitor in the testing state too. It is devoted to the detection and registering of loose parts in the lower water volume of the reactor pressure vessel. High sensetivety in combination with a low false alarm rate shall be achieved by detecting sound waves at five different positions during an adjustable time interval. It is advantegous to indicate a suspicious situation only if sound waves greater than a certain threshold appear in delayed coincidence in four of five acceleration signals. Preliminary tests at the reactor vessel with artificial impacts in the presence of normal operational noise have demonstrated the reliability of the detection even if the impacts cannot be heard clearly.

The experiencies obtained up to now are very promising. The monitor conception seems to be a realistic way to get diagnostic informations using noise techniques.

4. References

- [1] Fry, D. N., R. C. Kryter, J. C. Robinson
Analysis of Neutron-Density Oscillations Resulting from
Core Barrel Motion in the Palisades Nuclear Power Plant,
ORNL-TM-4570, May 1974
- [2] Bastl, W., V. Bauernfeind
The estimation of Vibration of Reactor Internals by
Noise Analysis of Non-Nuclear Parameters, EACRP Specialist
Meeting on Reactor Noise - SMORN-1, Rome, October 1974
- [3] Dio, W. H., H. Stoelben, W. Bastl, D. Wach, B. Raible
On-line Surveillance of LWR Primary Systems; State of the
Art and Development Trends of Vibration-, Loose Parts-
and Leakage Monitoring Systems in the Federal Republic
of Germany, Progress in Nuclear Energy Vol. 1 (2-4), 1977,
p. 747
- [4] Zigler, G. I., D. M. Stevens
Experience in Loose Parts Monitoring of Operating Nuclear
Power Plants, Progress in Nuclear Energy Vol. 1 (2-4),
1977, p. 663
- [5] Mayo, C. W.
Post Accident Reactor Diagnostics at TMI-2, 12th Informal
Meeting on Reactor Noise Analysis, Studsvik, Sweden,
May 16-18, 1979 (Technical Paper)
- [6] Buttler, E. et al.
Ein Rauschanalysesystem zur Schadensfrüherkennung an Kern-
kraftwerken mit Druckwasserreaktor, Kernenergie 20 (1977),
389
- [7] Grabner, A., P. Liewers, P. Schumann, F.-P. Weiß
Decomposition of Noise Signals composed of Many Similar
Components. Progress in Nuclear Energy Vol. 1 (2-4), 1977,
615
- [8] Grunwald, G., P. Liewers, P. Schumann, F.-P. Weiß
Experimental Investigation of Flow-Induced Control-Element
Movements by Noise Analysis, Nuclear Power Plant Control
and Instrumentation, Vol. 1, 1978, 291

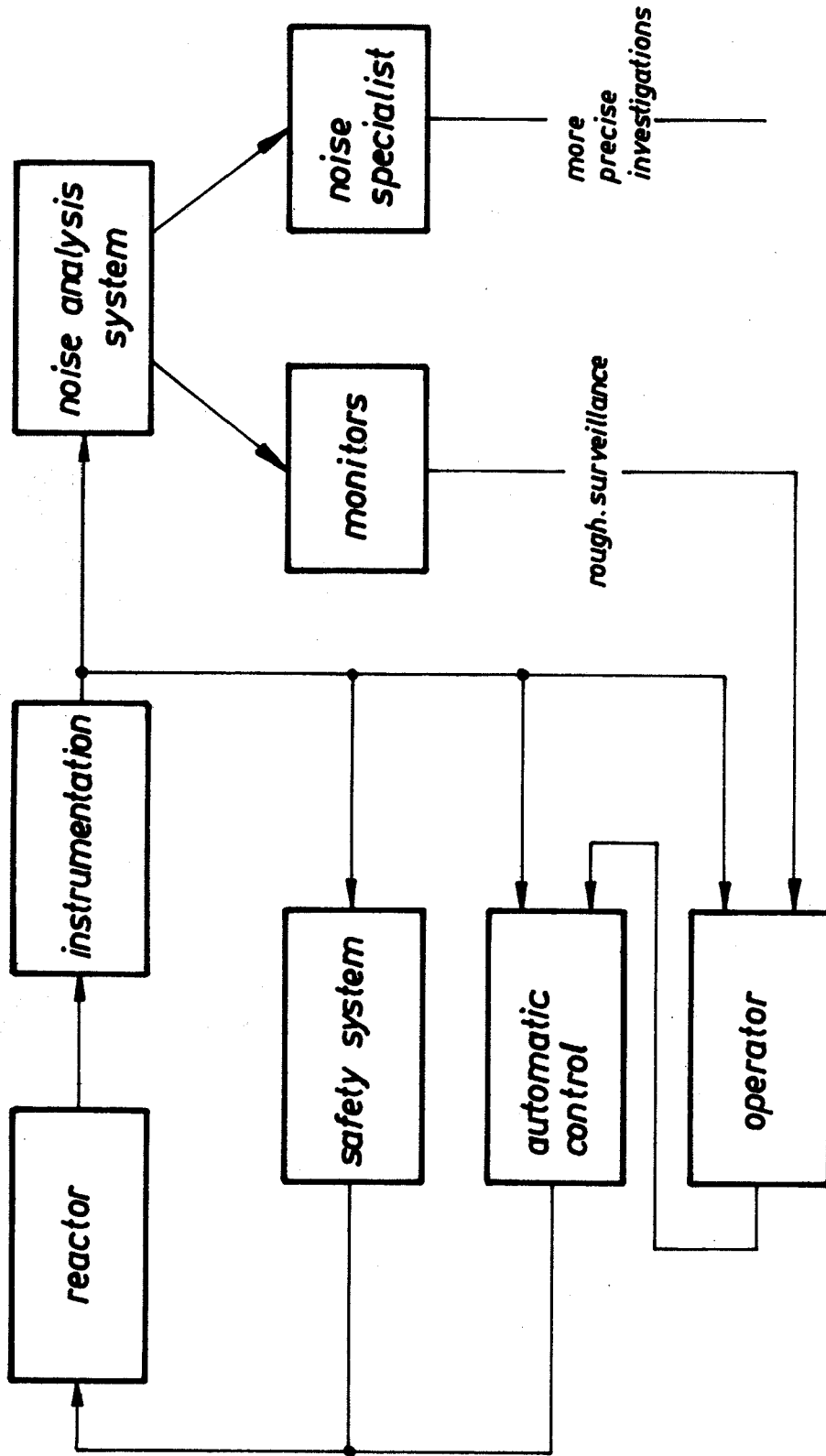


Fig. 1 Block diagram of the reactor control and safety system completed by noise methods

M. Sato, T. Sato, A. Kameda, Y. Yoneda

OPERATIONAL GUIDANCE EQUIPMENT FOR FUEL HANDLING SYSTEM

IAEA/NPPCI Specialists' Meeting on Procedures and Systems for
Assisting an Operator During Normal and Anomalous Nuclear Plant
Operation Situations, Munich, Federal Republic of Germany, 5-7
December 1979

Operational guidance equipment
for fuel handling system *

- M. SATO, Advanced Reactor Engineering Department, Toshiba Corp.
- T. SATO, Fuchu Works, Toshiba Corp.
- A. KAMEDA, Advanced Reactor Engineering Department, Toshiba Corp.
- Y. YONEDA, Power Reactor and Nuclear Fuel Development Corp.

* This work was performed under contracts between Power
Reactor and Nuclear Fuel Development Corporation and
Toshiba Corporation.

Abstract

At the Experimental Fast Breeder Reactor "Joyo", fuel handling operation, which includes spent fuel transfer from the core to the in-vessel storage rack and storage rack to the transfer rotor, and new fuel transfer to the opposite direction, are performed almost every two months.

No erroneous fuel handling of the operator, such as misaddressing or double-addressing are allocated in these processes. For this purpose, this equipment has been introduced to the fuel handling system.

This equipment provides the following functions.

- 1) Monitoring of the operation of charging between of fuels in the core and in the storage rack in the reactor vessel.
- 2) Monitoring of the operation of fuel transportation between the storage rack in the reactor vessel and the transfer rotor.
- 3) Operation guidance for each fuel handling procedure.
- 4) Confirmation of fuel appropriate grappling by weight detection.
- 5) Memorizing the fuel addressing status in the core and the storage racks, and updating these status according to the process.

These functions are realized by a process computer composed by a CPU (central processing unit), process input/output modules, input/output typewriter, output typewriter, paper tape reader and a color CRT display, etc..

Operation guidance and plant status information are displayed and/or printed by the color CRT display and the typewriter respectively, and the operator proceeds his operation by confirming these messages.

1. Introduction

The fuel handling facility handles new core fuels, blanket fuels, control rods, reflectors and special test assemblies. Spent fuels and other assemblies are removed from the reactor, cleaned, canned and stored in a water pool.

The refueling of an LMFBR has special features compared to that of light water reactors owing to the sodium coolant. The high chemical activity, melting point over 98°C and opacity of sodium makes the handling machines quite complicated.

In the case of "Joyo" the In-Core Charge Machine is used for the transfer of assemblies in the reactor vessel and the Ex-Vessel Transfer Machine addresses and removes the assemblies from the reactor vessel.

In the refueling process, such serious troubles as double loading, erroneous loading and collision and dropping of fuels must definitely be avoided.

To improve the operationability and to maintain the reliability of the refueling system, operational guidance equipment by a process computer was introduced.

2. The Objectives

The refueling of an LMFBR has some specific problems compared to that of light water reactors. For the case of Joyo, followings were experienced.

- (1) The refueling is done under shielded plugs and the handling quite complicated.
- (2) In the case of "Joyo", the refueling was done by the In-Core Charge Machine for the transfer of assemblies in the reactor vessel and by the Ex-Vessel Transfer Machine for insertion and removal of assemblies to and from the reactor vessel, for this reason the refueling procedure could not be done fully sequentially with only one machine.
- (3) The spacing between fuel in the reactor vessel was tight.
- (4) The addressing of each fuel was done by two rotating plugs which being used as a lid of the reactor vessel, so it made the handling quite complicated.

When "Joyo" start her normal irradiation service operation, re-fueling will be done every two months four or five times a year. To assist this operation this equipment was required to provide the following functions.

- 1) Monitoring of the operation of charging between of fuels in the core and in the storage rack in the reactor vessel.
- 2) Monitoring of the operation of fuel transportation between the storage rack in the reactor vessel and transfer rotor.
- 3) Operation guidance for each fuel handling procedure.
- 4) Confirmation of fuel appropriate grappling by weight detection.
- 5) Memorizing the fuel addressing status in the core and the storage racks, and updating these status according to the process.

These functions are realized by a process computer composed by a CPU (central processing unit), process input/output modules, input/output typewriter, output typewriter, paper tape reader and a color CRT display, etc..

Operation guidance and plant status information are displayed and/or printed by the color CRT display and the typewriter respectively, and the operator proceeds his operation by confirming these messages.

3. Plant Description

The fuel handling facility of "Joyo" consists of the In-Core Charge Machine, Ex-Vessel Transfer Machine and Rotating Plug inside the containment vessel, and the New Fuel Storage Facility, Cask Car, Fuel Cleaning Facility, Fuel Canning Machine and Spent Fuel Storage Facility at the outside. Arrangement of the fuel handling facility is shown in Fig. 1. There is also the transfer Rotor at the wall of the containment vessel which transfers the assemblies in to and out of the containment.

The operational guidance equipment covers the In-Core Charge Machine, Ex-Vessel Transfer Machine and Rotating Plug inside the containment vessel and also the Transfer Rotor at the wall of the containment vessel as shown in Fig. 3.

The vertical layout of the fuel transportation equipment in the containment vessel is shown in Fig. 2 and the function of each equipment is described as follows.

The In-Core Charge Machine is placed on the floor door valve of the Small Rotating Plug and is able to handle core fuels, blanket fuels and special test assemblies. Using the two rotating plugs, any positions can be addressed. To this machine, the operational guidance equipment monitors the operation of fuel exchange between of fuels in the core and in the storage rack in the reactor vessel and gives guidance of each fuel transportation procedure and also gives confirmation of fuel appropriate grappling by weight detection and memorizes the fuel addressing status in the core.

The fuel storage rack is used as a relay station for the addressing of new fuels into the core and as a cooling station for spent fuels before removal from the reactor vessel. The rack has a maximum capacity of twenty.

The Ex-Vessel Transfer Machine is installed on a travelling car which is placed on a movable bridge, and this enables the machine to run along and across the travelling floor. The machine carries the fuels from the Transfer Rotor to the fuel storage racks surrounding the core. To this machine, the operational guidance equipment monitors the operation of fuel transportation between storage rack in the reactor vessel and transfer rotor and gives guidance of each fuel transportation procedure and also gives confirmation of fuel appropriate grappling by weight detection and judges the pot type for transfer.

The Transfer Rotor is installed at the walls of the containment vessel and works at the entrance and exit of fuels going into the reactor. Since the fuel is transported in argon gas outside of the containment vessel and in sodium inside of the containment vessel, the Transfer Rotor acts as a sodium boundary for fuels. To the transfer rotor, the operational guidance equipment monitors incomings and outgoings of fuels.

The transportation of assemblies from the New Fuel Storage to the Transfer Rotor and from the Transfer Rotor to the Fuel Cleaning Facility is done by a fuel handling Cask Car. During refueling the car will run back and forth on two parallel rails.

When refueling is done, new fuels will be taken out of the New Fuel Storage Facility, preheated in the Cask Car and then addressed to the sodium filled pots in the Transfer Rotor. Spent fuels taken out of the Transfer Rotor will be addressed into the cleaning pot of the Fuel Cleaning Facility. After sodium cleaning is done, it will be canned in water and be sent to the Spent Fuel Storage Facility to be cooled and stored for shipment.

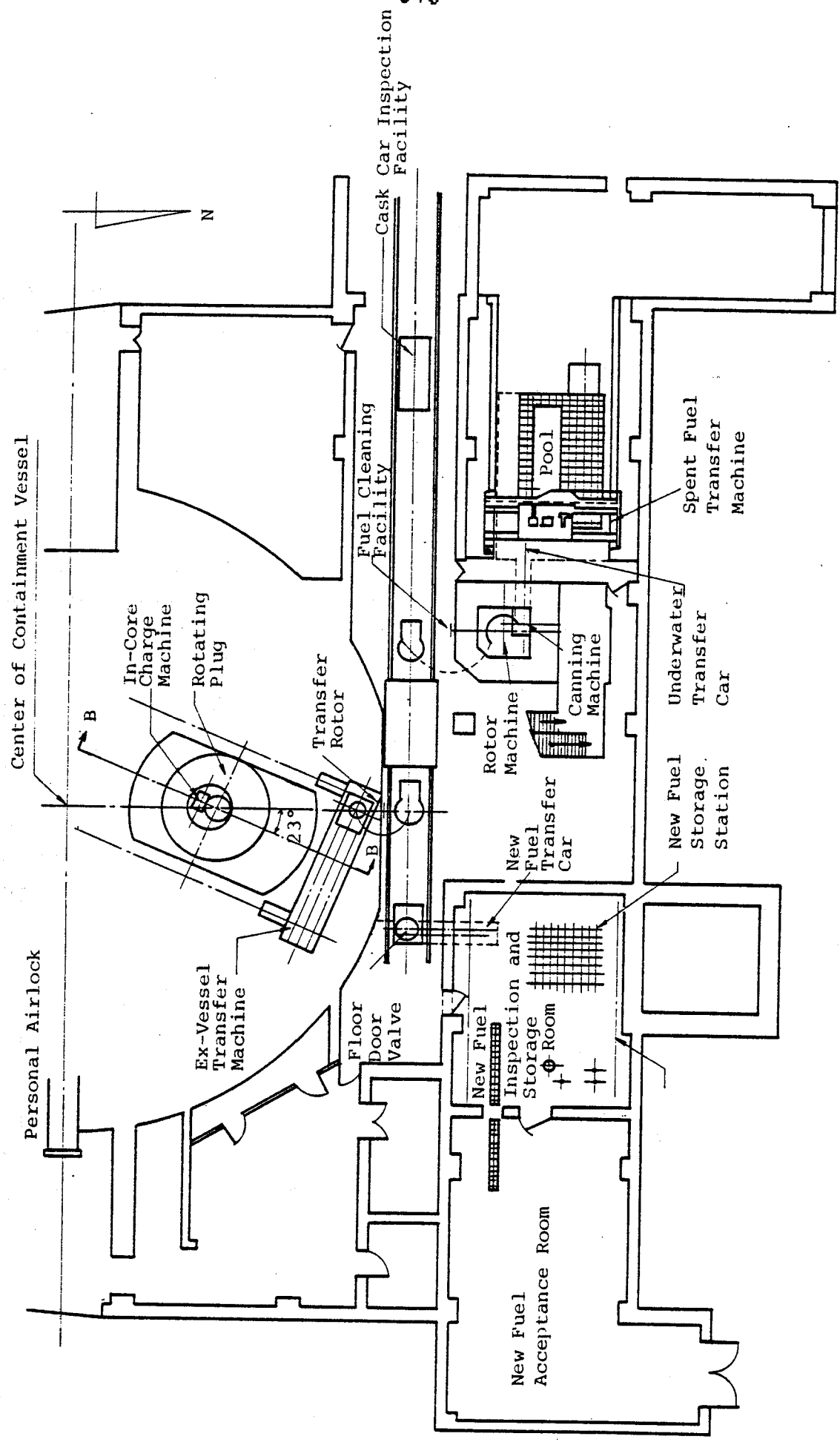


Fig. 1 Arrangement of the Fuel Handling Facility

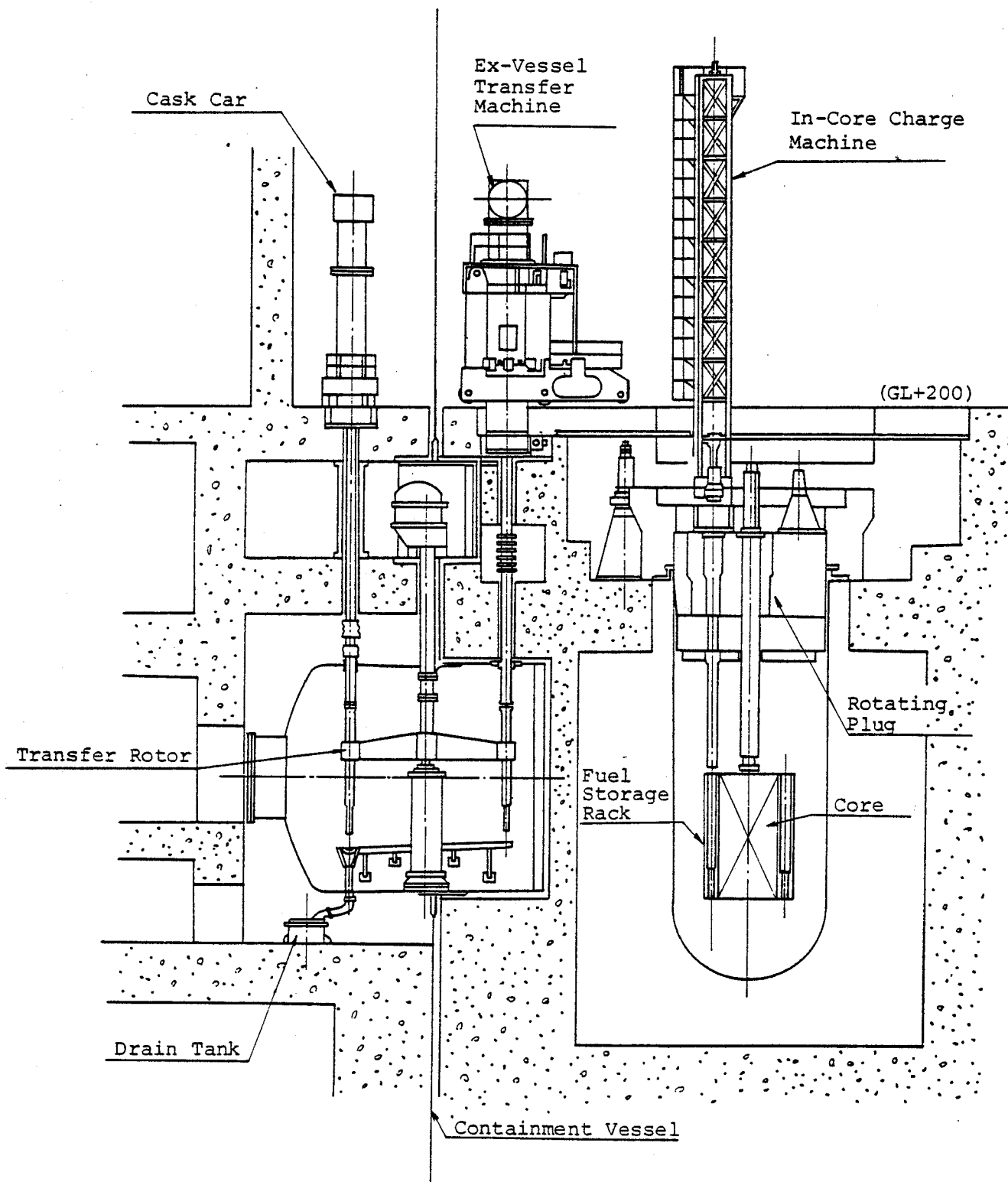


Fig. 2 Vertical layout of the fuel transportation equipment in the containment vessel

4. System Description

This operational guidance equipment is designed to assist the operation of the In-Core Charge Machine, Ex-Vessel Transfer Machine and Rotating Plug inside the containment vessel and also the Transfer Rotor at the wall of the containment vessel shown in Fig. 3.

Fig. 4 presents the operation sequence thus developed for operational guidance.

4.1 Hardware Composition

The main part of this operational guidance system consists of the TOSBAC-40C system. The Fuel Handling Operational Guidance System Configuration and the Computer Hardware System Configuration are presented in Fig. 5 and 6.

The hardware composition are listed as follows.

Central Processing Unit (TOSBAC-40C) 1 Unit

Core memory: 48KB

Process input/output unit

Analog inputs: 32 points

In-Core Charge Machine load-cell

In-Core Charge Machine gripper position

Ex-Vessel Transfer Machine coffin pressure

Ex-Vessel Transfer Machine blow-down gas flow rate

Ex-Vessel Transfer Machine load-cell

Transfer Rotor rack position

etc.

Digital inputs (contact): 192 points

Ex-Vessel Transfer Machine gripper position

Ex-Vessel Transfer Machine gripper finger position

Large and small rotating plugs' angle

In-Core Charge Machine gripper position

In-Core Charge Machine gripper finger position

etc.

Relay output: 16 points

Fuel-loading status

Timer hold

etc.

Interrupt inputs: 16 points

4.2 Software Composition

The Fuel Handling Operational Guidance software system consists of three main functions, such as Internal Processing function, Demand function and Refueling monitoring function. These functions are executed under the control of the Operating system (POPS-C).

(1) Internal Processing Function

This function includes the analog scanning, digital inputs (contact) scanning, message outputs and trend display etc..

(2) Demand Function

This function is to take suitable steps or printing owing to the request of the operator such as information inputs or information print out.

(3) Refueling Monitoring Function

This function is to monitor the fuel operational sequence set by the operator, and if troubles happened, it gives message by printing or displaying to the operator.

The Computer Software System Configuration is presented in Fig. 7.

Still more, plant tables' method, which is performed by a "Fill-in-the-Blanks" method, are introduced. So, there is no need to draw conventional block charts. System designing is based upon the plant tables, and the program can be obtained as a result; thus, plant control design and software design becomes unified.

5. System Testing and Test Operation

Before the computer system was connected to the actual plant, its principal functions were verified and adjusted by means of a function simulator.

The computer system was then connected to the actual plant, and the test was repeated on the actual installation. The plant operation table system greatly simplified the work of correcting deviations from the design data.

6. Conclusion

The possibility of improving the operability and of maintaining the reliability of the fuel handling facility was demonstrated with a TOSBAC-40C computer system.

The test showed that the interactive computerized operator console with cathode ray tube fully answered the purpose of integrating the operation and supervisory functions.

In this system, only the operation monitoring and operation guidance are realized by the computer, but it is expected that with the experience of this system the blocking signal to the misoperation will be taken from this system in the near future.

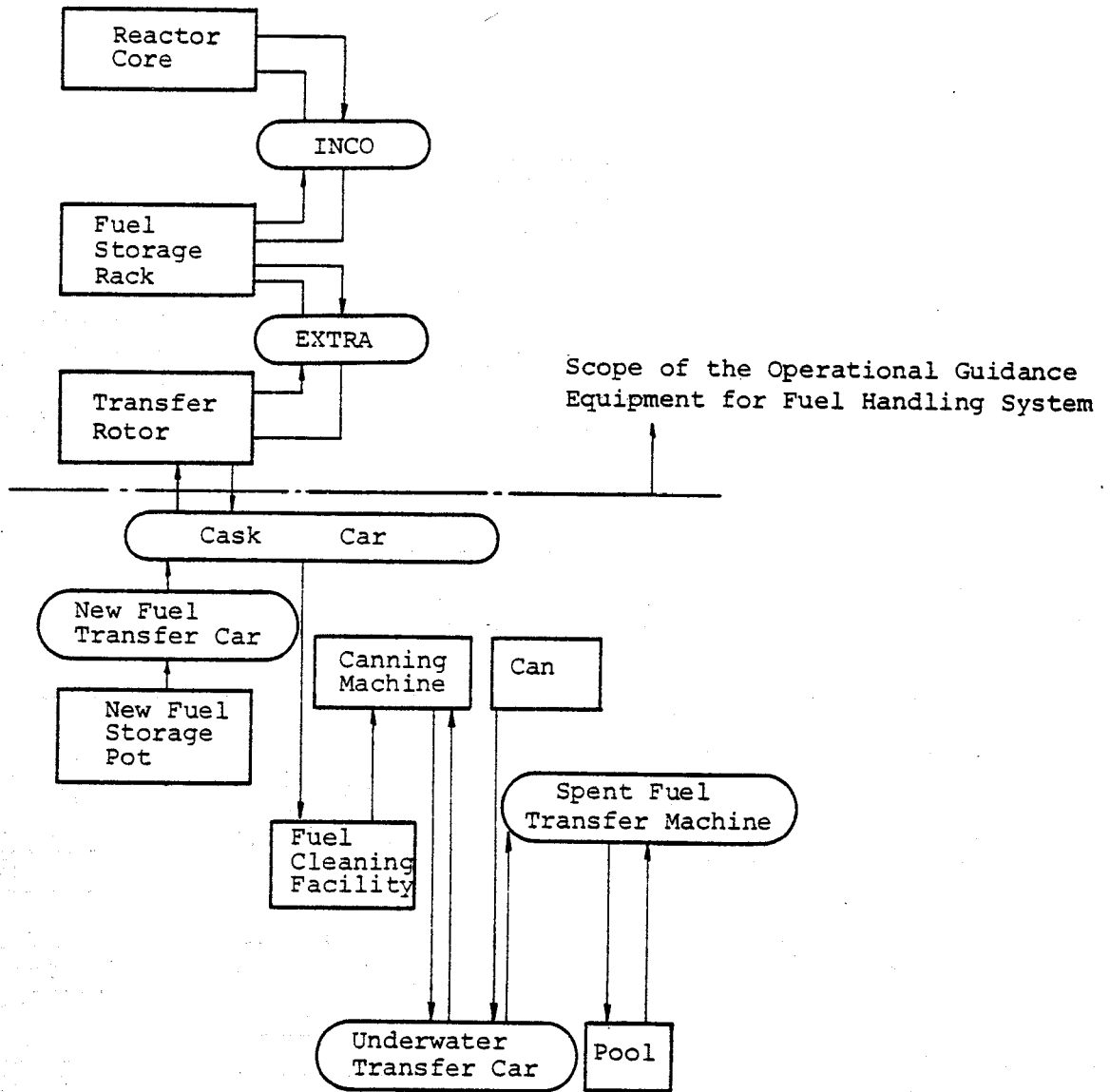
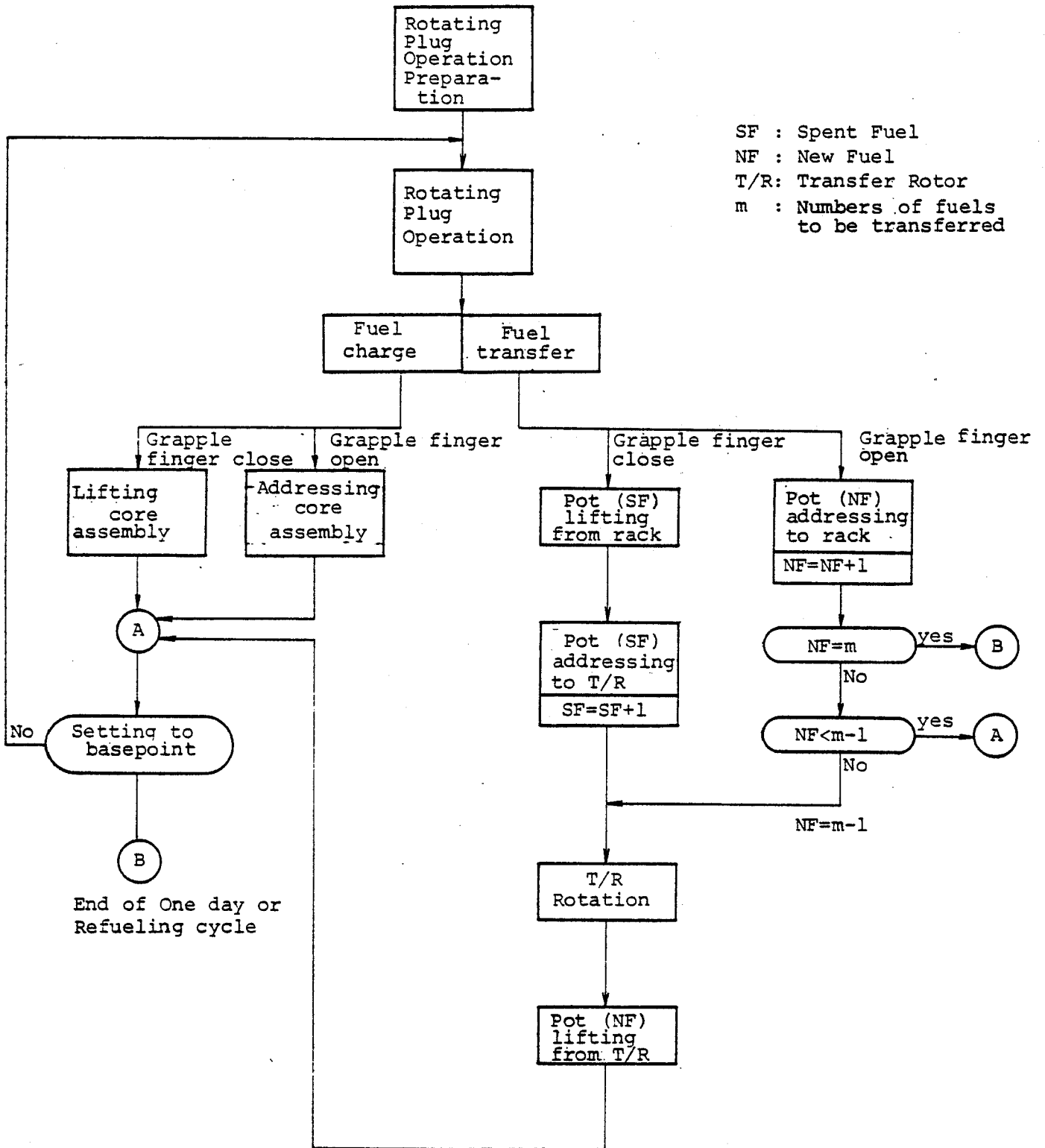


Fig. 3 Fuel Transportation Flow



SF : Spent Fuel
 NF : New Fuel
 T/R: Transfer Rotor
 m : Numbers of fuels to be transferred

Fig. 4 Fuel Operational Sequence

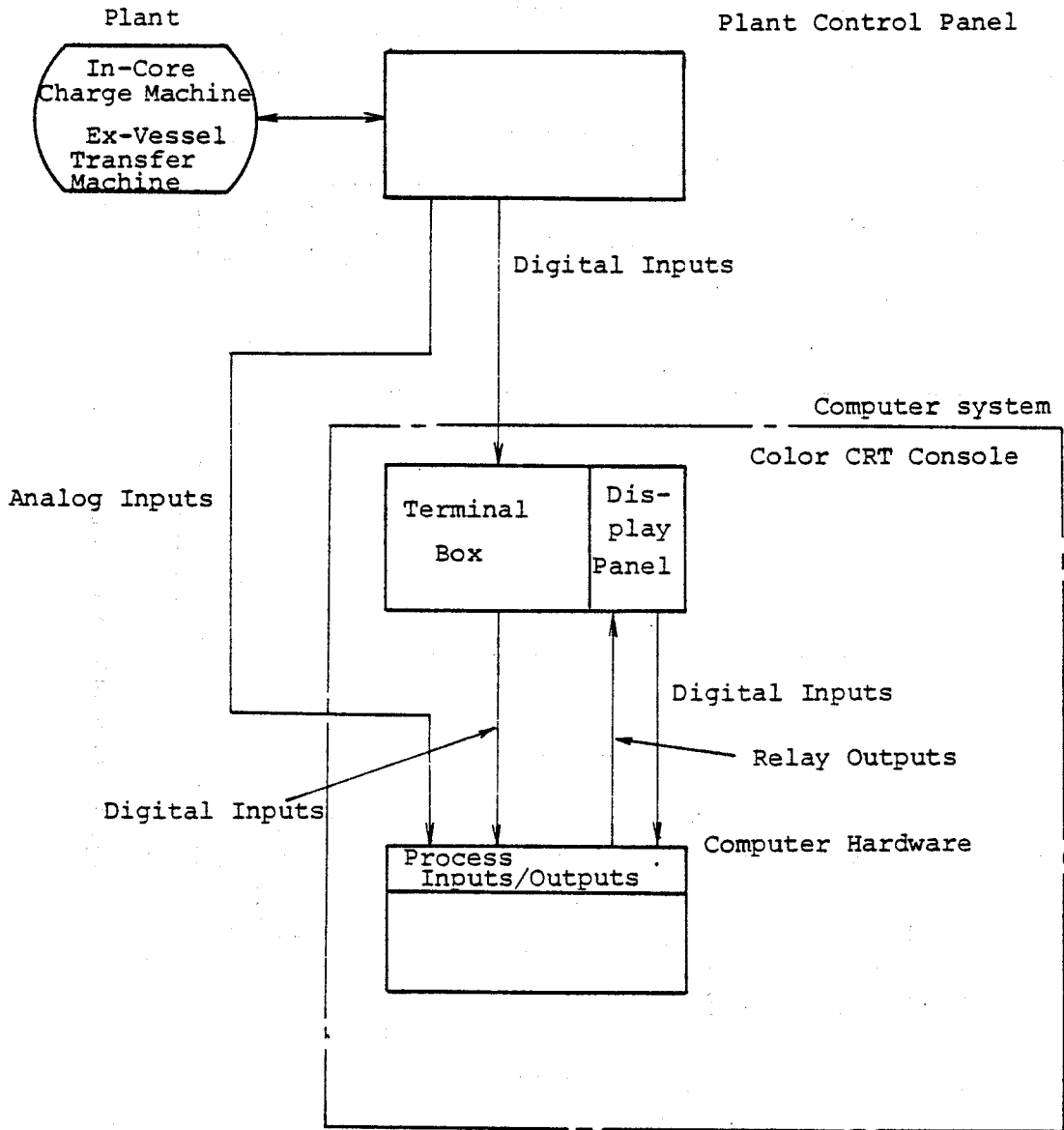


Fig. 5 Fuel handling operational guidance system configuration

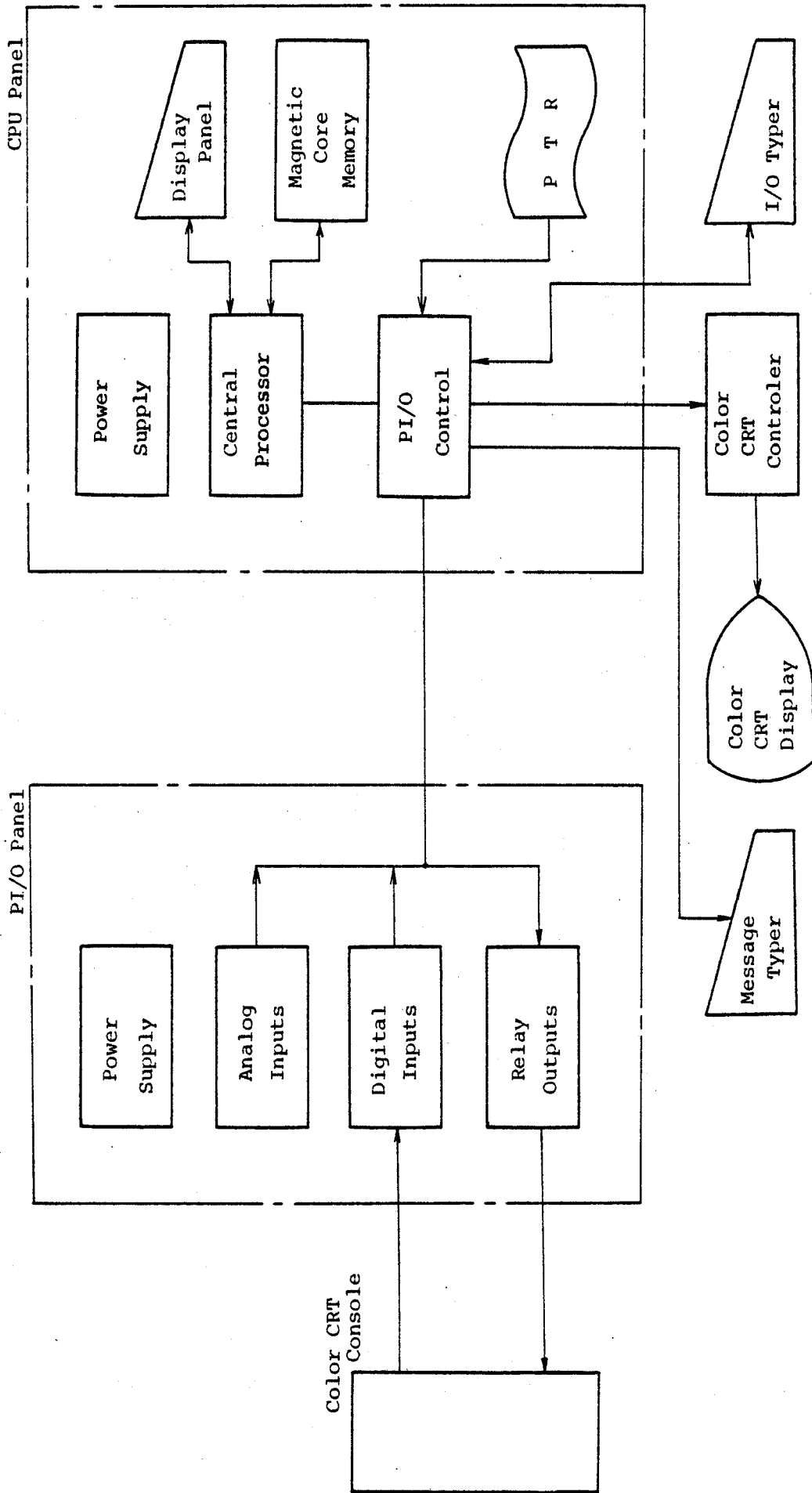


Fig. 6 Computer hardware system

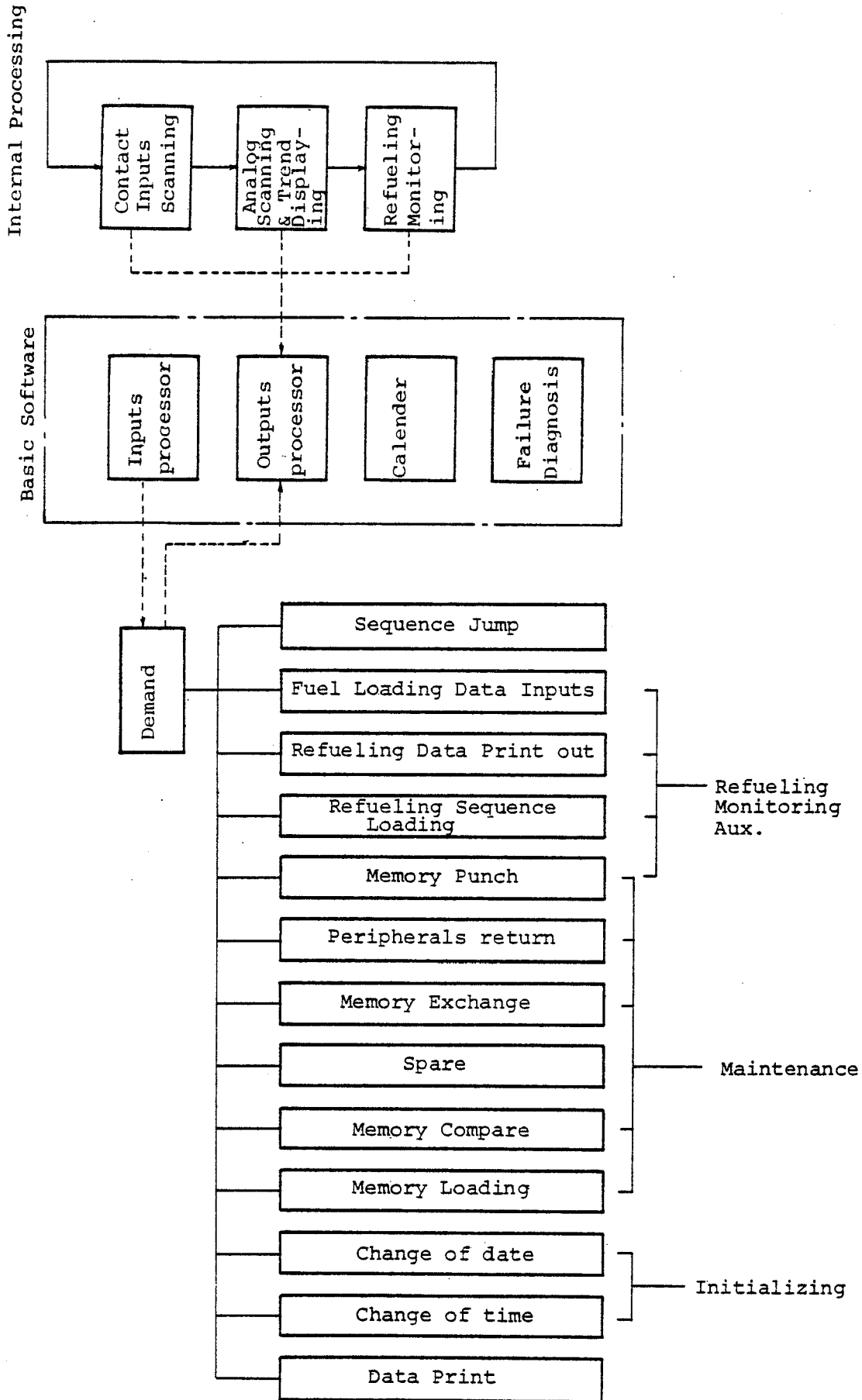


Fig. 7 Computer Software System

CONTENTS

Session V

BASIC INVESTIGATIONS OF SURVEILLANCE

Chairperson: J. Wakabayashi

Secretary: L. Felkel

J. Wakabayashi	
SUMMARY OF SESSION V	555
J. Wakabayashi, A. Fukumoto	
SIMULATION STUDY ON THE DIAGNOSIS SYSTEM OF NUCLEAR POWER PLANT OPERATION	561
R. Černý	
THE DYNAMIC CLASSIFICATION AND REDUCTION OF ALARMS IN COMPUTER BASED INFORMATION SYSTEMS	575
M. Lind	
THE USE OF FLOW MODELS FOR DESIGN OF PLANT OPERATING PROCEDURES	583
T. Tamaoki, N. Naito, T. Tsunoda, M. Sato, A. Kameda	
VERIFICATION TEST FOR ON-LINE DIAGNOSIS ALGORITHM BASED ON NOISE ANALYSIS	605
R. Avenhaus, G. Spannagel	
ANALYSIS OF PROCESS SIGNALS IN NUCLEAR INSTALLATIONS	629
W. Ehrenberger	
SOFTWARE VERIFICATION IN ON-LINE SYSTEMS	645

Written Contribution

E. Holló

OPERATOR-INTERACTIVE SURVEILLANCE METHOD OF PERIODIC
INSPECTION OF ACTIVE ENGINEERED SAFETY SYSTEM OF
WWER 440 TYPE REACTORS

667

G.P. Beraud, A. Bonnemay, A. Le Dieu de Ville, J.C. Nimal
ESTIMATION OF LOCAL POWER IN A PWR CORE FROM GAMMA RAYS
MEASUREMENTS

ESTIMATION OF LOCAL POWER IN A PWR CORE
FROM GAMMA RAYS MEASUREMENTS

G.P. BERAUD* - A. BONNEMAY** -
A. LE DIEU DE VILLE** - J.C. NIMAL** -

MUNICH 5 - 7 DECEMBRE 1979

* EDF/SEPTEN/FRANCE

** CEA/SACLAY/FRANCE

1 - INTRODUCTION

1.1. Power distribution monitoring on EDF PWR plant

The present status of power distribution monitoring on EDF PWR plant uses mainly two systems :

- an out of core neutron flux measurement. The detectors are ionisation chamber without compensation at power. These measurements lead to monitor by following the axial offset parameter. Utilisation is permanent and includes protective functions.

- an incore system composed by : the fixed thermocouples, located over the core, which provide continuous measurements of enthalpy rise in the channel, however corresponding values are associated with large incertainties due to cross flow.

: a set of movable miniature fission chambers acquiring an axial profile flux for about a third of the assemblies.

Measurements are carried on each time is necessary. This instrumentation is time consuming and inaccurate during transients, but furnishes the fine structure power sharing.

In order to improve power distribution determination several methods and instrumentations are under development, particular attention is given to fixed incore using gamma thermometer.

The following parts review a brief description of gamma thermometer principle and advantages, give some comments about data treatment and more details about gamma signal interpretation.

1.2. Gamma thermometer description

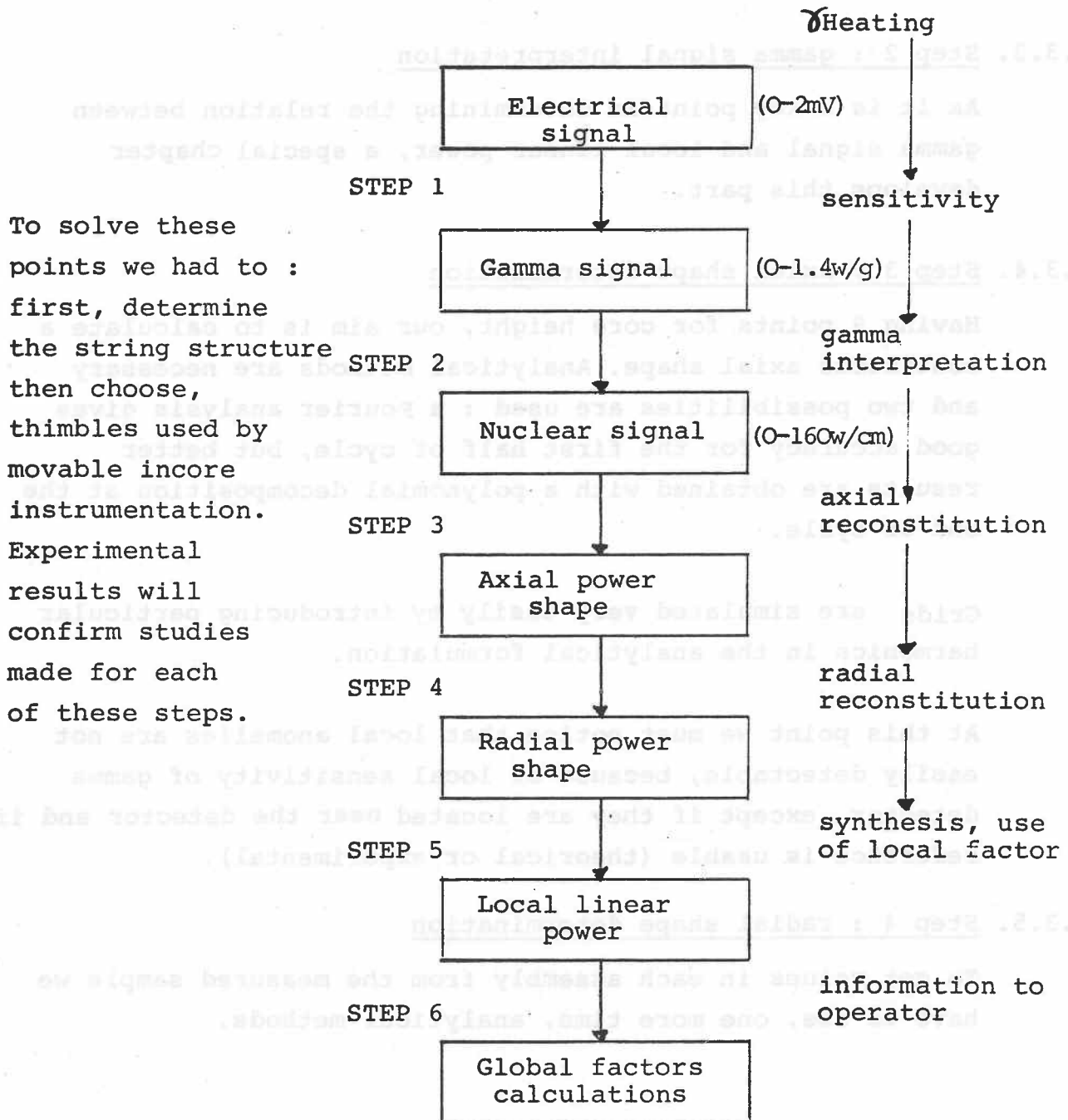
The sensitive part is a stainless steel rod isolated from thimble by a chamber filled with gaz. On the axial axis a variation of temperature between the level of the chamber and the thimble is obtained due to heating caused by gamma radiations.

Preliminary studies have led to define a string with nine regularly spaced detectors, the sensitivity of which are about 40°C for 1.4 watt per gram in gamma rays, in those conditions the signal level is about 2 millivolts. At the present time we use these strings in movable incore thimbles to verify the performances of this type of detector.

1.3. Signal treatment

1.3.1. Principle of treatment

The following chart describes the principle of treatment :



1.3.2. Step 1 : Determination of sensitivity

This is made, to day, by an excore calibration which uses an electrical power generation. The factor measured relates the sensitivity in w/g to the signal in mV.

On line incore methods are also investigated using transfert function determination (response to step function or white noise). Relation between this function and sensitivity is expected.

1.3.3. Step 2 : gamma signal interpretation

As it is a key point in determining the relation between gamma signal and local linear power, a special chapter develops this part.

1.3.4. Step 3 : axial shape determination

Having 9 points for core height, our aim is to calculate a continuous axial shape. Analytical methods are necessary and two possibilities are used : a Fourier analysis gives good accuracy for the first half of cycle, but better results are obtained with a polynomial decomposition at the end of cycle.

Grids are simulated very easily by introducing particular harmonics in the analytical formulation.

At this point we must notice that local anomalies are not easily detectable, because of local sensitivity of gamma detector, except if they are located near the detector and if some reference is usable (theoretical or experimental).

1.3.5. Step 4 : radial shape determination

To get values in each assembly from the measured sample we have to use, one more time, analytical methods.

Two possibilities are investigated :

- without theoretical references ; this method needs : an instrumentation of all assemblies after having taken into account all symetries (for instance : 26 assemblies for a 1/8 core symetry in a 157 assemblies Westinghouse PWR).
: some redundancy to determine a gross radial tilt. First studies for a first cycle are very encouraging.
- with analytical references. To avoid loss of time in an on-line processing we have to give analytical correlations or tables established for values of influent parameters (power level, rod position, burnup).

This second method has the disadvantage to use parameters values we suppose to be good but not necessary real values, nethertheless the problem is the same for movable core map and accuracy is the same.

1.3.6. Step 5 : determination of fine power distribution

From the preceding steps local power is obtained for each point surrounding the central part of each assembly, to use linear power everywhere in the core user must determine a set of coefficients reflecting, for each part of the core, the relation between local power in a rod and power near the instrumentation thimble. The result is a 3 D distribution of local nuclear power. This step is the same for movable incore.

1.3.7. Step 6 : calculations for operator

Now as all what is needed to inform the operator has been obtained, several possibilities are offered :

- select what parameters must be calculated, if they must be scoped or tabulated, on demand or continuously monitored
- choose the frequency of refreshment, the accuracy of calculations (coarse of fine). All this part need more development and is the object of other articles.

2 - DETERMINATION OF THE GAMMA THERMOMETER RESPONSE FROM THE REACTOR POWER

2.1. Sources taken into account

The gamma sources taken into account are the following for the standard assembly.

- gamma rays coming directly from fission
- gamma rays emitted by fission products
- gamma rays from captures in U^{238}
- gamma rays from captures in U^{235}
- gamma rays from neutron captures in fuel cladding
- gamma rays emitted by neutrons captures in borated water
- gamma rays emitted by the gamma thermometer itself and its associated water.

For an assembly containing control rods, we have also taken into account the gamma emitted by silver, indium, cadmium rods and by the steel rods. We have also considered elements with poisons.

It is planned to take into account the neutron heating by means of ANISN calculation and the gamma heating due to inelastic reactions in fuel.

2.2. Calculation tools

2.2.1. Gamma sources from fission products

The gamma issued from fission products are evaluated using the PICFEE code (1). Let $f_j(t)$ be the number of gamma emitted per unit of time in the energy group j , where t is the cooling time after the elementary fission. Let $W(t)$ be the power variation versus time t in fission rate per unit of time. The PICFEE code calculates the convolution product (1) for several cooling time t .

The result of the integration is the gamma spectrum emitted by the fission products.

$$(1) \quad S_j(t) = \int_0^t W(\tau) f_j(t-\tau) d\tau$$

The functions $f_j(t)$ are obtained by the following way.

For short cooling times, $f_j(t)$ is given by Maienschein (2) measurements for t between 0 and 1500 seconds. After 1500 seconds, the kernels $f_j(t)$ are computed by the code PEPIN (3) which solves the differential equations satisfied by the fission product concentrations during the cooling time after the elementary fission (PEPIN treats also any power diagram). A PEPIN calculation involves 635 fission products. For each fission product the library of PEPIN contains capture cross section, half time, branching ratio, gamma and β spectrum emitted by radioactive decay.

The PICFEE calculations don't take into account the neutron capture on fission products. To evaluate this approximation we have made a PEPIN calculation which take into account the neutron captures and a PICFEE calculation. The two calculations are made with the same power diagram. The difference between the two calculations is lower than 1 % during the power operation and for short cooling times (1000 seconds).

2.2.2. Other gamma sources

The determination of the gamma sources from captures and fissions supposes the knowledge of several reaction rates in all parts of the cell: captures in water, in boron, in fuel cladding, in U^{235} and U^{238} , fission density, captures in poisons and control rods and so on. For this purpose, we have used the cell code APOLLO (4) which solves the Boltzmann equation by the collision probability method.

2.2.3. Gamma transport calculations

Two different gamma transport calculations were made to obtain the gamma thermometer heating :

- a) line of sight point attenuation kernel method
- b) Monte Carlo method.

a) The line of sight point attenuation kernel method was used for all gamma contributions except for gamma coming from captures in the gamma thermometer itself and its associated water. MERCURE-IV (5) performs this calculation. MERCURE IV treats a three dimensional geometrical configuration. The geometry is composed of homogeneous volumes limited by plane or quadratic surfaces. The source distribution is also three dimensional. The linear attenuation coefficients are used in the multigroup structure defined in table 1.

TABLE 1

Number of group j	Upper energy (MeV)	Lower energy (MeV)
1	8.5	7.5
2	7.5	6.5
3	6.5	5.5
4	5.5	4.5
5	4.5	3.5
6	3.5	2.75
7	2.75	2.25
8	2.25	1.75
9	1.75	1.25
10	1.25	0.75
11	0.75	0.50

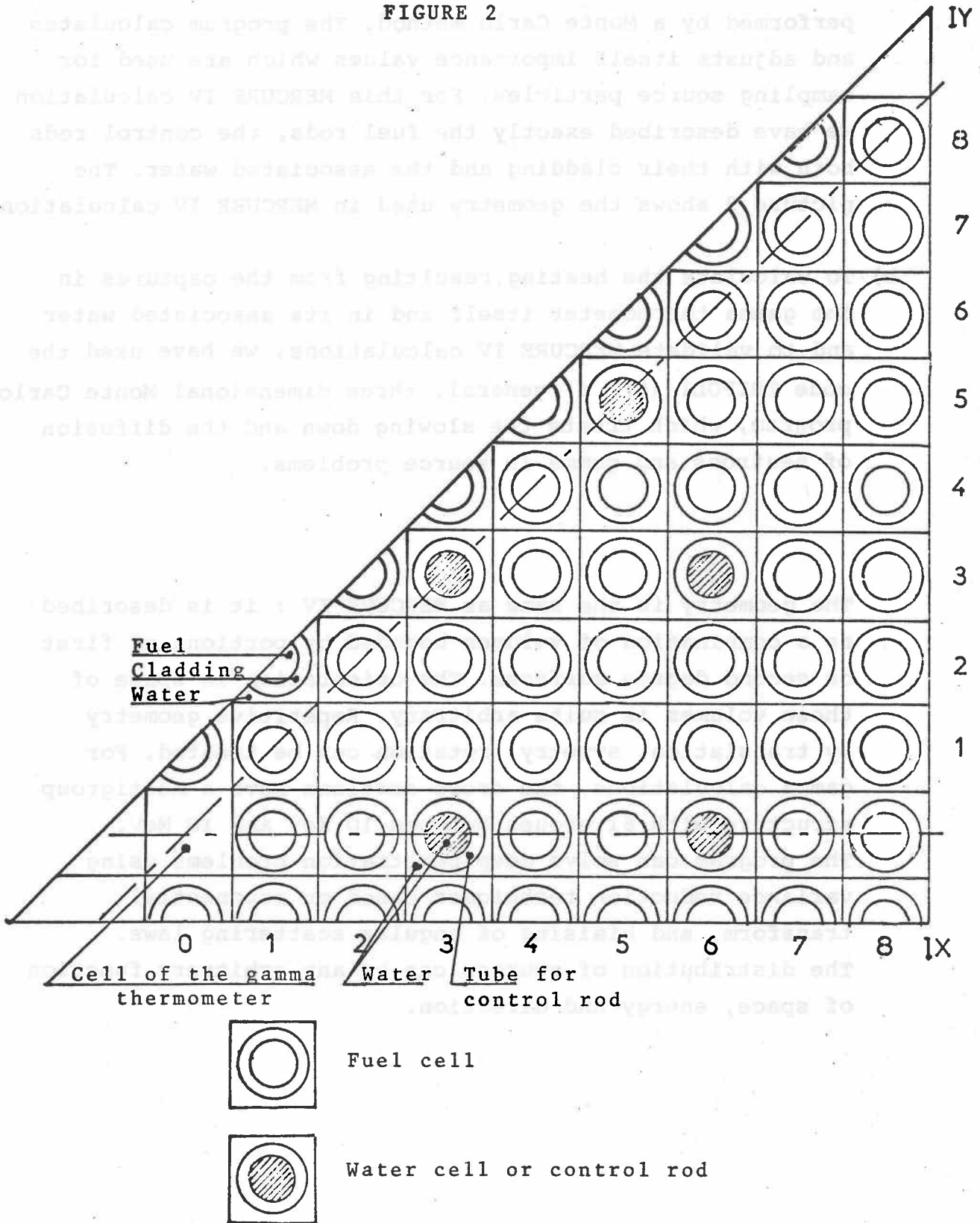
The gamma spectra were defined in these 11 groups. The group number 11 contains also gamma rays of energy lower than 500 KeV with conservation of the total energy emitted.

The build up factors use the KITAZUM formula, which takes into account the sequence of materials along the gamma path. The integration of the attenuation kernel is performed by a Monte Carlo method. The program calculates and adjusts itself importance values which are used for sampling source particles. For this MERCURE IV calculation we have described exactly the fuel rods, the control rods both with their cladding and the associated water. The picture 2 shows the geometry used in MERCURE IV calculations.

- b) To calculate the heating resulting from the captures in the gamma thermometer itself and in its associated water and to validate MERCURE IV calculations, we have used the code TRIPOLI (6), a general, three dimensional Monte Carlo program, which treats the slowing down and the diffusion of neutrons and gamma in source problems.

The geometry is the same as MERCURE IV : it is described as a combination of volumes bounded by portions of first or second degree surfaces. The orientation in space of these volumes is quite arbitrary. Repetitive geometry by translation, symmetry, rotation can be treated. For gamma calculations, the cross sections have a multigroup structure with 61 groups between 10 KeV and 10 MeV. The program can solve deep penetration problems using variance reduction techniques based on exponential transform, and biasing of angular scattering laws. The distribution of sources can be any arbitrary function of space, energy and direction.

FIGURE 2



2.3. Validation of MERCURE IV calculations

2.3.1. Comparison between MERCURE IV and TRIPOLI calculations

We have made TRIPOLI and MERCURE IV calculations with the same conditions for two fuel rods. The first fuel rod was very far (IX=8, IY=7) from the gamma thermometer and the second was near (IX=4, IY=2). For each rod, we calculated the contribution of the 11 energy groups defined in table 1.

The agreement is good above 2.5 MeV (see results on table 3) for both fuel rods. MERCURE IV over estimates the heating below 2.5 MeV essentially at 1 MeV. The total heating is over estimated of 15 % for the distant fuel rod and of 11 % for the nearest fuel rod. In view of the standard deviation, about 5 %, the overevaluation is about the same for any rod.

The table 4 gives a comparison between the different contributions to the heating coming from several sources in the fuel rod. The agreement between MERCURE IV and TRIPOLI is very good and this fact is more important than the disagreement in absolute value.

2.3.2. Influence of gamma rays of lower energy than 500 KeV

Two calculations were made. In these two calculations, the 10 energy groups above 0.75 MeV are the same. In one calculation we have taken into account the exact gamma spectrum up to 100 KeV. In the other calculation, we have only one group between 0.75 MeV and 0.5 MeV with conservation of the energy emitted below 0.75 MeV

The table 5 gives the comparison between the two calculations for the fission product component and 8 fuel rods. The calculations with 11 groups over estimates the response of 0.43 %.

TABLE 3 - FUEL ROD 4.2 HEATING DUE TO GAMMA PROMPT OF FISSION

Energy group	Group	TRIPOLI	MERCURE IV	Ratio <u>TRIPOLI</u> MERCURE IV
		Heating $\pm 2 \sigma$ w/g	Heating $\pm 2 \sigma$ w/g	
8.5	1	3.535E-20 \pm 13%	3.597E-20 \pm 3.5%	0.983
7.5	2	1.041E-19 \pm 10%	9.565E-20 \pm 1.6%	1.088
6.5	3	3.360E-19 \pm 9%	2.869E-19 \pm 0.7%	1.171
5.5	4	6.294E-19 \pm 8%	5.783E-19 \pm 4.3%	1.088
4.5	5	1.767E-18 \pm 9%	1.572E-18 \pm 1.9%	1.124
3.5	6	2.663E-18 \pm 9%	2.413E-18 \pm 1.7%	1.104
2.75	7	2.638E-18 \pm 10%	2.667E-18 \pm 1.8%	0.989
2.25	8	3.311E-18 \pm 8%	3.649E-18 \pm 1.6%	0.907
1.75	9	4.299E-18 \pm 9%	5.047E-18 \pm 1.1%	0.852
1.25	10	4.334E-18 \pm 8%	5.797E-18 \pm 0.9%	0.748
0.75	11	2.748E-18 \pm 12%	3.307E-18 \pm 1.7%	0.831
0.50				
TOTAL w/g		2.287E-17 \pm 3.4%	2.545E-17 \pm 0.5%	<u>0.898</u>

Normalization : 1 gamma from fission per cm³.s

σ : standard deviation due to Monte Carlo method

TABLE 4

1°) Nearest fuel rod

	TRIPOLI	MERCURE IV	RATIO <u>MERCURE IV</u> TRIPOLI
γ directly from fission	40.75 %	40.70 %	0.9988
γ from fission products	37.91 %	37.74 %	0.9955
γ captures on U ²³⁵	5.69 %	5.68 %	0.9982
γ captures en U ²³⁸	15.65 %	15.88 %	1.0147

2°) Distant fuel rod

	TRIPOLI	MERCURE IV	RATIO <u>MERCURE IV</u> TRIPOLI
γ directly from fission	40.31 %	40.09 %	0.9945
γ from fission products	38.84 %	38.91 %	1.0018
γ captures on U ²³⁵	5.62 %	5.59 %	0.9947
γ captures on U ²³⁸	15.23 %	15.41 %	1.0118

2.4. Most important results with fission products at equilibrium

The most important results are given in the tables 6 and 6 bis. The table 6 gives the percentage of heating in the gamma thermometer from several cell rows. About 91 % of the heating comes from the instrumented fuel element and 9 % from the 8 surrounding elements. The table 6 bis gives the decomposition of the gamma thermometer heating. 65 % of the heating is directly proportionnal to power density or thermal flux 35 % comes from the fission products.

The heating due to the gamma issued from neutron captures in the gamma thermometer itself and its associated water amounts up to 7.4 % additional.

TABLE 5 - FISSION PRODUCTS BELOW 500 KeV

Cell rod number	Row number	MERCURE IV (w/g) with 11 energy groups (conser- vation of total energy)	MERCURE IV (w/g) with 13 energy groups	RATIO <u>MERCURE IV 11 groups</u> <u>MERCURE IV 13 groups</u>
1-1	1	3.7960 E-15	3.7944 E-15	1.00042
2-1	2	1.8556 E-15	1.8496 E-15	1.00032
3-1	3	6.9808 E-16	6.9045 E-16	1.011
4-1	4	3.8760 E-16	3.8409 E-16	1.0091
5-1	5	2.3518 E-16	2.3355 E-16	1.0070
6-1	6	1.5021 E-16	1.4946 E-16	1.0050
7-1	7	1.0170 E-16	1.0132 E-16	1.0038
8-1	8	7.3009 E-17	7.2780 E-17	1.0031

Normalization : 1 fission per cm³

Approximate influence on the gamma thermometer heating

with 11 groups ----- 1.0787 E-13 w/g

13 groups ----- 1.0741 E-13 w/g

Difference ----- 0.43 %

TABLE 6

Row number from which the gamma are issued	Number of fuel rods	Number of water cells	Heating amount percent
1	8	0	29.90
2	16	0	22.24
3	16	8	11.36
4	32	0	10.82
5	36	4	6.57
6	36	12	4.04
7	56	0	3.75
8	64	0	2.83
9	72	0	2.47
10	80	0	1.80
11	76	12	1.28
12	84	12	0.84
13	104	0	0.73
14	80	32	0.42
15	120	0	0.45
16	128	0	0.33
17	104	32	0.17

The gamma from neutronic captures in gamma thermometer add 7.4 % to this value.

TABLE 6 bis

Gamma from fission -----	38 %
Gamma from fission products -----	35 %
Gamma from capture in U ²³⁸ -----	17 %
Gamma from capture in U ²³⁵ -----	6 %
Gamma from capture in fuel cladding ----	2 %
Gamma from capture in borated water ----	2 %

Gamma from neutron captures in gamma thermometer itself
7.4 % additional.

2.5. Response due to several power transients

Several power transients have been studied.

The first power diagram is shown on the figure 7. The diagram is periodical and the period is exactly one day. The power decreases or increases by a factor 3 during half an hour. The ratio between the gamma thermometer heating normalized to unity and the nuclear power is between 1.25 and 0.93. The picture 8 shows another type of power diagram and the corresponding heating.

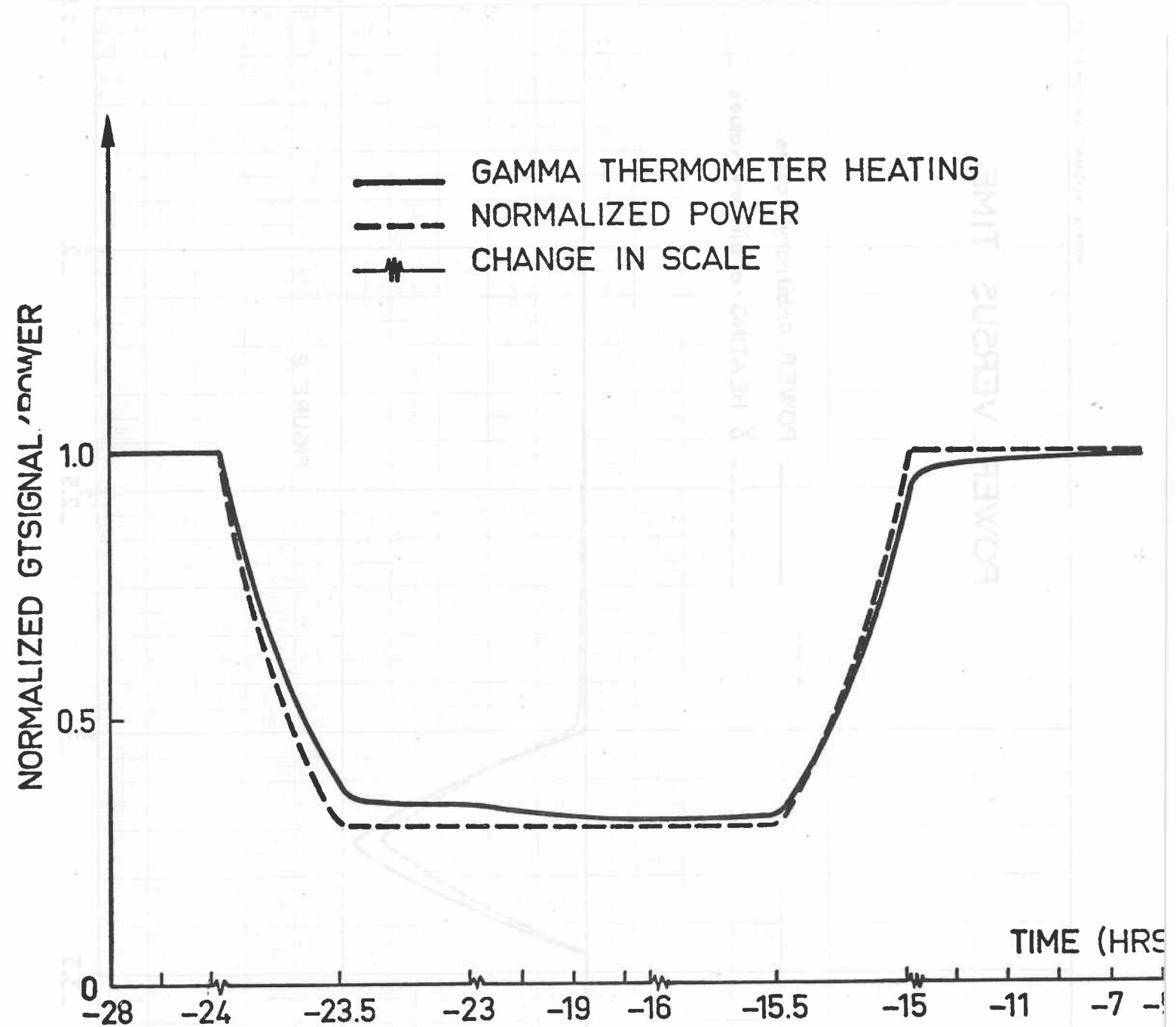
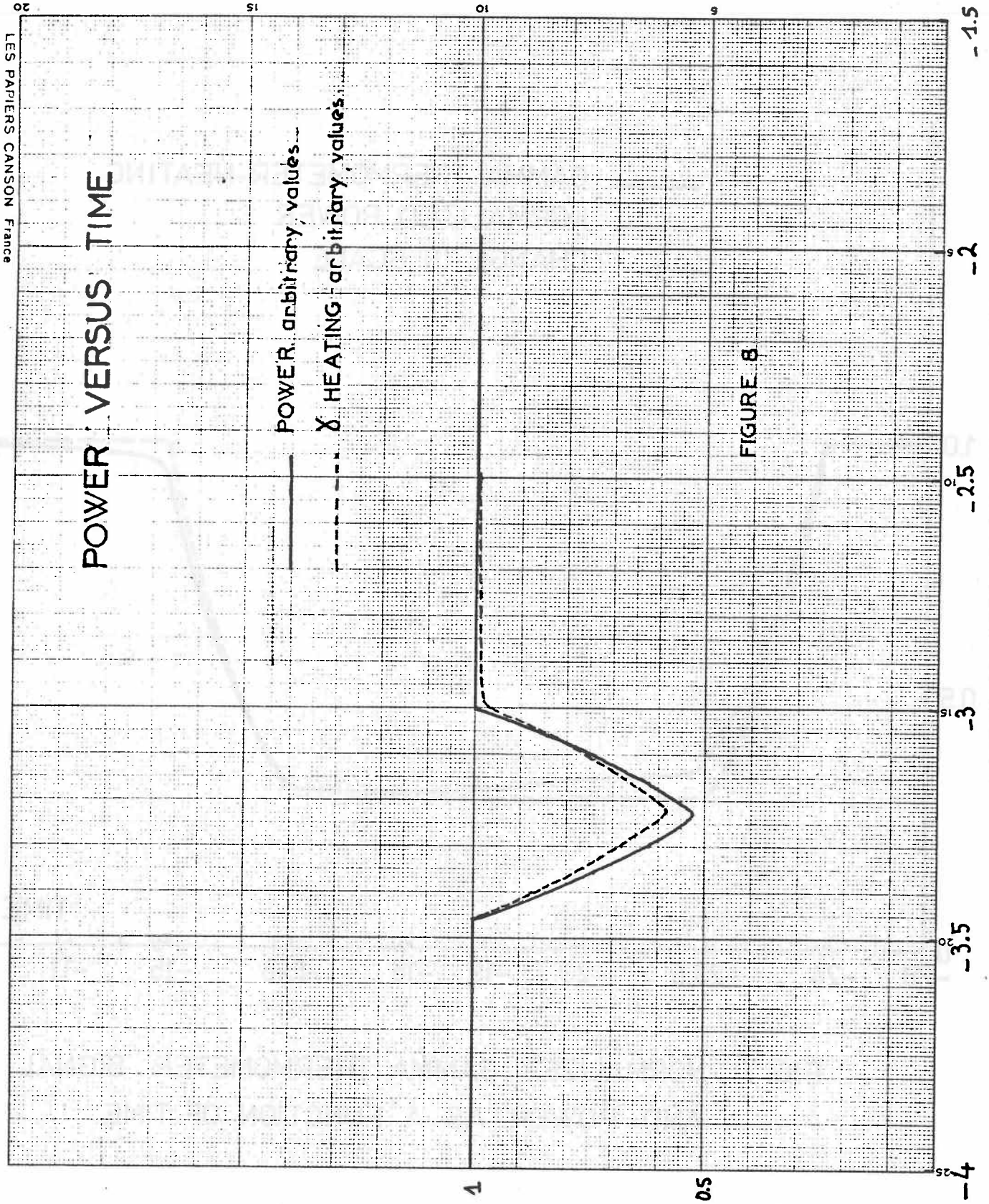


FIG. 7 - NORMALIZED GAMMA THERMOMETER SIGNAL AND POWER AS A FUNCTION OF TIME



3 - PROCESSING OF THE GAMMA THERMOMETER SIGNAL

3.1. Statement of the problem

It can be shown that the heating power in the gamma thermometer is related to the local nuclear power by a relation :

$$e_{\gamma} = \alpha w(t) + \int_0^t H(t-\tau)w(\tau)d\tau$$

and so, the output current i_{γ} , which is proportional to

$$i_{\gamma} = \delta \cdot e_{\gamma}$$

is related to local nuclear power by :

$$i_{\gamma} = \delta \left(\alpha w(t) + \int_0^t H(t-\tau)w(\tau)d\tau \right)$$

It appears that we have to process conveniently the output signal i_{γ} in such a way that we obtain a signal proportional to the local nuclear power. This signal might be :

- as accurate as possible
- obtained by an on line processing.

3.2. Choice of a method

Up to now, no definitive choice was taken on the method. As a matter of fact, it depends upon different actually unknown options as :

- technology of the processing (analoga , digital hardware, software...)
- the use of the signal (automatic control, open loop surveillance, operator's read out etc...)
- the expected validity area (is the signal of a gamma thermometer processed if the bottom of control rod is in its neighbourhood.

Nevertheless, a study was made using a "reasonable" choice, which is the digital filtering.

This method as the advantage to be easily adaptable to one or the other of the preceedingly mentionned options.

The following study was made by means of a dynamical simulation, and no experimental result is obtained for now.

3.3. Approximation of the decay function of fission products

Equation (1) is a convolution equation which kernel $H(t)$ summarizes the contribution of eleven energy groups of fission products to the global phenomenon of decay of fission products.

So it is the sum of a very high number (several hundred) of exponential functions. It has the noteworthy property of being very satisfactorily fitted by a sum of a limited number of exponential functions. (about 5, as shown in further computations).

Fig 9 gives the function $H(t)$ and the fitted five exponential function. Those functions can be interpreted as period groups.

The accuracy of the fitting as well as this of the estimated local nuclear power increases slowly from a 5 period groups approximation to a 11 period groups approximation. For more than 11 no advantage can be taken of the improvement of the number of groups, because of :

- the presence of noise
- the dynamic behaviour of the gamma thermometer itself.

Parameters of the exponentials were obtained by a classical least square method, for instance, the five period groups approximation is :

$$\begin{aligned}
 H(t) \approx & 0.8210^{-3} e^{-0.48 \cdot 10^{-3} t} + 0.410^{-2} e^{-0.3 \cdot 10^{-1} t} \\
 & + 0.3 \cdot 10^{-1} e^{-0.2 \cdot 10^{-2} t} + 0.35 e^{-0.23 t} \\
 & + 0.3 e^{-2 t}
 \end{aligned}$$

3.4. Synthesis of the filter

Let us denote $H^*(t)$ some n-period-group approximation of H , and let us consider the modified equation :

$$i\gamma = \delta \left(\alpha w(t) + \int_0^t H^*(t-\tau) w(\tau) d\tau \right)$$

Its Laplace transform is :

$$\frac{1}{\delta} \mathcal{L}[i\gamma] = \alpha \mathcal{L}[w] + \mathcal{L}[H^*] \cdot \mathcal{L}[w]$$

So, we get :

$$\mathcal{L}[w] = \frac{1}{\delta} \frac{1}{\alpha + \mathcal{L}[H^*]} \mathcal{L}[i\gamma]$$

(where $\mathcal{L}[\cdot]$ denotes the Laplace transform operator)

From this expression, we can derive the equation of a filter :

$$\frac{dw_i}{dt} - \frac{1}{b_i} (w - w_i) = 0 \quad i = 1 \dots \nu$$

$$Bw + C \sum_{i=1}^{\nu} \frac{a_i}{b_i} w_i - i\gamma = 0$$

where

$$B = \alpha \delta = \frac{i\gamma(0)}{w(0)} = 0,6009$$

$$C = \lim_{t \rightarrow \infty} \frac{i\gamma - \alpha \delta w}{\delta \int_0^+ H(t-\tau) w(\tau) d\tau} = 0,0543$$

For sake of stability, a complementary term was computed

(7) and added in the algebraic equation of the filter.

3.5. Preliminary results

The accuracy of the filter was tested for 5 and 11 period-groups, corresponding to $\gamma = 5$ and $\gamma = 11$ in the above equations, on two transients.

A "U transient" see fig 10

A "V transient" see fig 11

It can be shown that :

- a) error never exceeds 6 %
- b) this maximum value is reached only in a little time interval
- c) average value of error is about 1.5 %
- d) permanent error is zero

Those results were obtained by use of the simulation

language NEPTUNIX (8) (9).

4 - CONCLUSION

The fixed incore instrumentation using gamma thermometer offering possibilities of continuous and accurate incore measurement will be a precious aid for operator, making his work easier especially in fuel management, load follow and frequency adjustment domains. It may also improve the use of the margins power capabilities. Investigations for some specific protectives functions are under way.

FIGURE 10

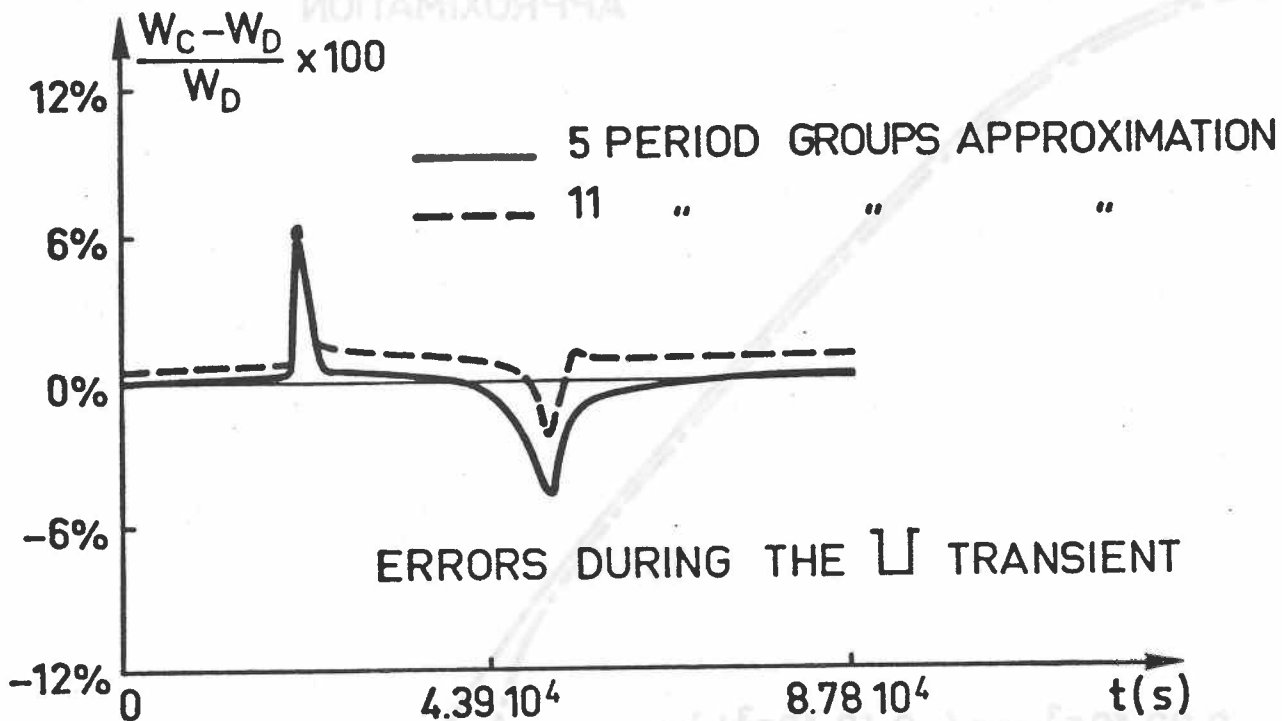
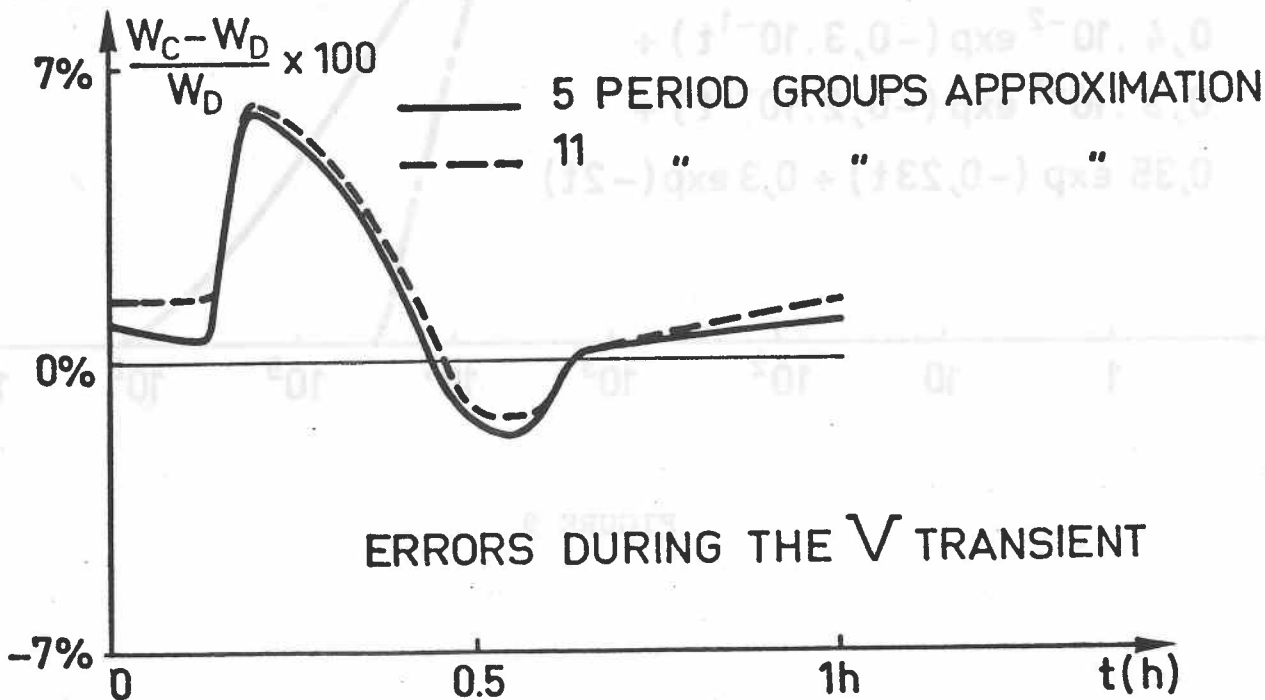


FIGURE 11



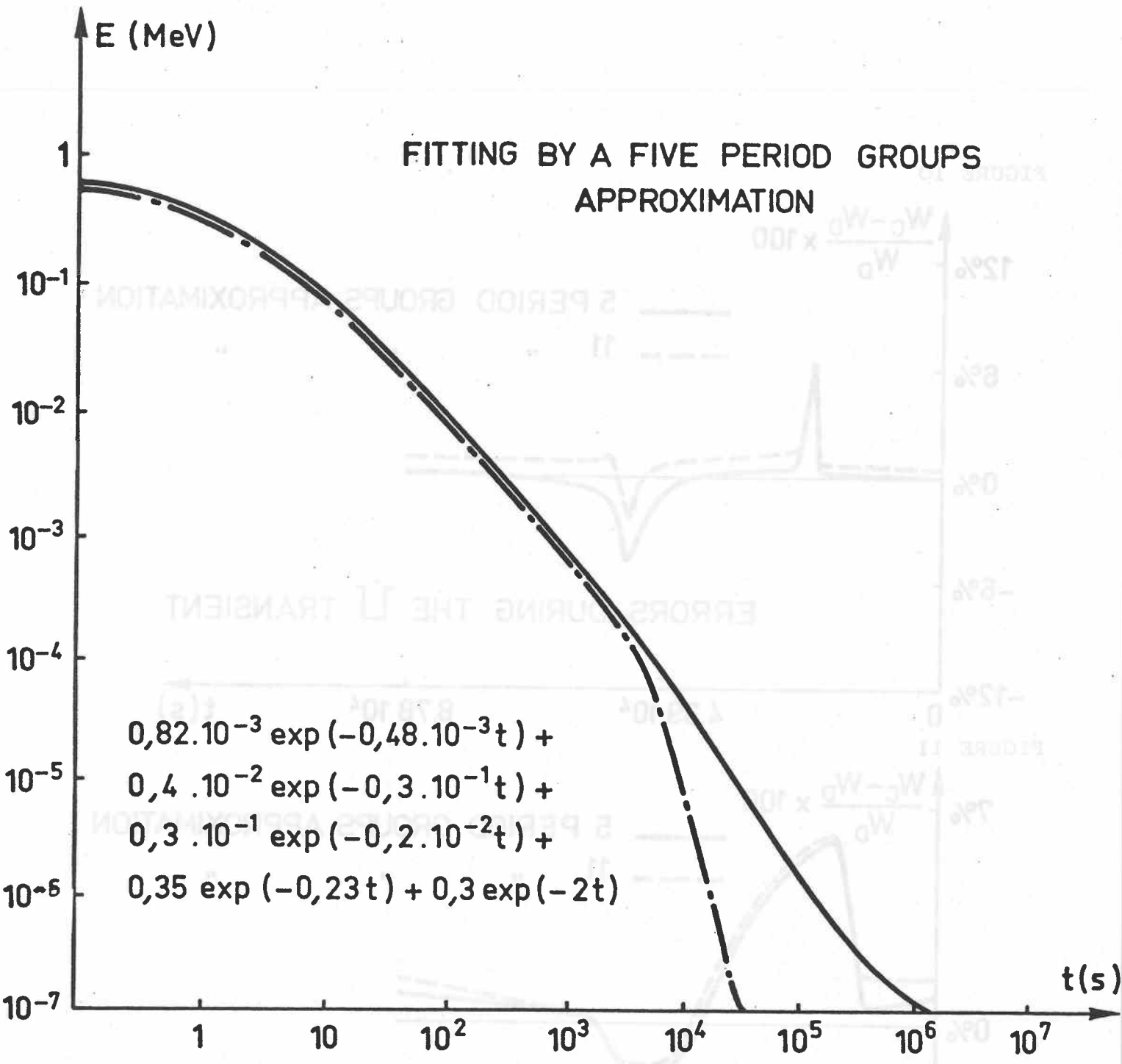


FIGURE 9

- 551 -
BIBLIOGRAPHY

- 1 Internal report
- 2 F.C. MAIENSCHHEIN - R.W. PEELE - W. ZOBEL - T.A. LOVE -
Gamma rays associated with fission
A/Conf. 15/P/670 1958
- 3 To be published
- 4 A. HOFFMANN and al.
Rapport SERMA/1193/S 1972
APOLLO - Code multigroupe de résolution de l'équation
du transport pour les neutrons thermiques et rapides
- 5 C. DEVILLERS - C. DUPONT -
Note CEA N 1726 1974
MERCURE 4 - Un programme de Monte Carlo à trois dimensions
pour l'intégration de noyaux ponctuels d'atténuation en ligne
droite.
- 6 J.C. NIMAL and al.
Note CEA.N.1919 (7 tomes) 1976
Programme de Monte Carlo polycinétique à trois dimensions
TRIPOLI 01
- 7 BONNEMAY - FONTANA -
Rapport SERMA/T/390
- 8 BONNEMAY et al
NEPTUNIX,
2nd Int. Symposium on large engineering systems
Univ. of Waterloo, Canada, 1978
- 9 ROUX et al.
Large system real time -----
IMACS symposium, Sonento, 1979

CONTENTS

Session V

BASIC INVESTIGATIONS OF SURVEILLANCE

Chairperson: J. Wakabayashi

Secretary: L. Felkel

J. Wakabayashi	
SUMMARY OF SESSION V	555
J. Wakabayashi, A. Fukumoto	
SIMULATION STUDY ON THE DIAGNOSIS SYSTEM OF NUCLEAR POWER PLANT OPERATION	561
R. Černý	
THE DYNAMIC CLASSIFICATION AND REDUCTION OF ALARMS IN COMPUTER BASED INFORMATION SYSTEMS	575
M. Lind	
THE USE OF FLOW MODELS FOR DESIGN OF PLANT OPERATING PROCEDURES	583
T. Tamaoki, N. Naito, T. Tsunoda, M. Sato, A. Kameda	
VERIFICATION TEST FOR ON-LINE DIAGNOSIS ALGORITHM BASED ON NOISE ANALYSIS	605
R. Avenhaus, G. Spannagel	
ANALYSIS OF PROCESS SIGNALS IN NUCLEAR INSTALLATIONS	629
W. Ehrenberger	
SOFTWARE VERIFICATION IN ON-LINE SYSTEMS	645

Written Contribution

E. Holló

OPERATOR-INTERACTIVE SURVEILLANCE METHOD OF PERIODIC
INSPECTION OF ACTIVE ENGINEERED SAFETY SYSTEM OF
WWER 440 TYPE REACTORS

667

J. Wakabayashi

SUMMARY OF SESSION V

J. Wakabayashi

SUMMARY OF SESSION V

The subject of session V was "Basic Investigation of Surveillance". Six papers were presented in this session. Most of the papers proposed the new methods or new techniques for the increase of safety and reliability of nuclear power plants operation.

Some of them, presented by Mr.R.Černý, Power Research Institute, Czechoslovakia, and Mr.G.Spannagel, Karlsruhe, Germany, were concerned with the application technique of new methods which were developed in the other field, not the field of a nuclear power plant. The alarm messages will be reduced by utilizing the dynamic classification of alarms. This method will aid the understanding of plant situation for the operators, but future studies on the reliability of this method will be necessary before the actual application. The data processing technique utilizing the statistical analysis will be successfully applied in the field of nuclear power plant operation.

The papers presented by Mr.T.Tsunoda, NAIG Nuclear Research laboratory, Japan, and myself were concerned with the diagnosis method which was studied by off-line experiment and computer experiment. The application of noise analysis is one of the promising techniques for the diagnosis of local anomaly. The pattern recognition technique and the estimation technique of state variables will be successfully applied in the diagnosis of plant operation.

The paper presented by Mr.M.Lind, Risø National Laboratory, Denmark, proposed the operating flow model for assisting the understanding of operating situation. The paper presented by Mr.W.

Ehrenberger, GRS, Germany, was concerned with the reliability of computer software. These two papers were also interesting works for us.

Many of the valuable discussions were provided on the presentations of this session. Some discussions were concerned with the applicability and some were concerned with the reliability. All the works in this session were the basic studies and they do not apply to the actual plant at present time, but I hope that these methods or techniques will be applied in the actual nuclear power plants in a short time.

Now, I shall express my own opinion concerning the basic investigation.

1) The small trouble which occurs in the nuclear power plant causes the loss of a lot of money, because it takes a long time to repair the equipment due to the radiation. Therefore, the development of more reliable equipments and the development of more reliable protection techniques are the most important tasks for the nuclear power plants. The good equipment, i.e. the development of hardware, and the good protection technique, i.e. the development of software, are inseparable just like the right and left wheels of the car.

2) The increase of the reliability of the protection system which includes the human operation is quite important. I think, this fact was proved by the TMI accident. The development of the operator aid system, just the subject of this meeting, is very important. The new methods or the new techniques must be investigated at the various organizations, and I hope that these new methods or new techniques are speedily applied in the actual plants and that the comparative studies of them are made internationally. Of course, each technique will be utilized as the supplement system at the first time, but in the future, it may be utilized as one of the safety equipments.

3) Many of the discussions concerning the reliability of the protection system were made in this meeting. I think, most of them were concerned with the reliability of the computer system. I think, many of the people are considering that a computer is a rather expensive equipment, but as you know, the technique of L.S.I. is progressing rapidly, the cost of microprocessors is decreasing day by day. Therefore, the exclusive computer (not multipurpose computer) for the diagnosis system or the protection system can be provided at low cost. The double or triple system may be provided at low cost in few years. Thus, it can be considered that the reliability problem of the computer has been already solved.

4) As the future problems, I want to point out that,

A) as mentioned before, the investigation of the protection system including the human operation is one of the important problems.

B) After the accident or the reactor shut-down, it is very important to estimate the state variables inside the reactor vessel. In this case, only the usually provided detector signals (some of them may be wrong due to accident) must be utilized.

J. Wakabayashi, A. Fukumoto

SIMULATION STUDY ON THE DIAGNOSIS SYSTEM OF NUCLEAR POWER
PLANT OPERATION

Simulation Study on the Diagnosis System of Nuclear Power Plant Operation

Jiro WAKABAYASHI and Akira FUKUMOTO

Institute of Atomic Energy, Kyoto University

1. INTRODUCTION

In order to prevent the accidents and to diminish the unnecessary outage, the development of a diagnosis system of nuclear power plants is one of the most important tasks. The diagnosis technique may be composed of following four stages, i.e.

1. Early detection of the anomalous state.
2. Estimation of primary causes of the anomaly source (disturbance).
3. Prediction of the future trend of anomaly.
4. Selection of the best remedy to rectify the anomalous state.

The techniques of noise analysis and pattern recognition are successfully utilized in stage 1. The noise analysis is one of the most promising technique for obtaining the useful informations relate to the anomaly from limited number of the detected signals. On the other hand, the statistical analysis to the obtained informations will improve the reliability of the identification of anomaly.

Since the estimation of the anomaly source is made using a simplified system model, the model identification is a major problem of stage 2. If the model is identified by the regression equations, the anomaly source may be estimated by the regression analysis. On the other hand, if the model is identified by the ordinary differential equations, the filter technique may be utilized in the estimation of anomaly source.

Stage 3 is closely connected with dynamic analysis of the system, and Stage 4 is related to the evaluation of its safety operation. Therefore, stages 1 and 2 may be considered as the peculiar problems in the diagnosis system.

The diagnosis technique may also be classified into following two major purposes,

- A) Early detection of the local failure which could not be detected directly. -local blockage of fuel assembly, failure of fuel rod, loose parts, etc.
- B) Early detection of the insignificant anomaly and estimation of the anomaly source during the operation. -deviation of the characteristics of the control system, deviation of the pump speed, etc.

The methods applied in the diagnosis system for above two major purposes will be slightly differed.

The present study is concerned with the latter problem. From our previous studies, we considered that the practical diagnosis system would be consisted of three blocks, i.e. 1) detection and classification of the anomalous state, 2) estimation of the primary cause of detected anomaly and 3) storage of past detected signals. The linear discriminant function technique is applied in block 1 and the Kalman-filter technique is applied in block 2. The Kalman-filter corresponding to the individual anomalous state (category) classified by block 1 is derived from the simplified dynamic model which identified beforehand for each category using a set of training data generated by the plant simulator.

The applicability of this diagnosis system in an actual plants is examined using a hybrid computer, where a 450MWe PWR plant simulator was composed by the analogue computer and a diagnosis system was composed by a digital computer. The computer experiments were made for several presumed anomalous states, i.e. 1) reactivity change, 2) decreases of the primary coolant flow, 3) change of the feed water flow and 4) change of the demand power generation.

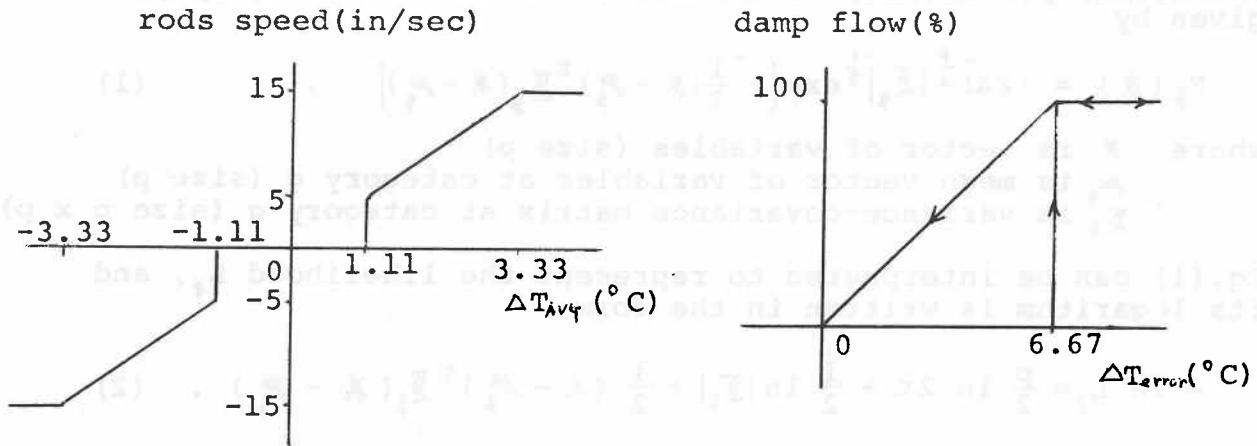
The results show that the detection and the classification of the anomalous state are possible within the reasonable time and the anomaly source (disturbance) is estimated with reasonable accuracy. However, the development of future techniques for blocks 1 and 2 will be important problems to improve the reliability of the diagnosis system.

2. 450MWe PWR PLANT SIMULATOR

A 450MWe PWR plant simulator was composed by an analogue computer, where the following assumptions and approximations are adopted due to the capacity of our computer.

- 1) Neutron kinetics of the reactor core can be expressed by the one point kinetic equations and three groups of delayed neutrons ($\lambda_i > 0.3$) can be treated similar as prompt neutrons.
- 2) Reactivity coefficients of the fuel and coolant temperatures are given by $2 \times 10^{-5} \Delta K/K/^\circ C$ and $1 \times 10^{-4} \Delta K/K/^\circ C$, respectively.
- 3) Complete mixing are accomplished in the upper and lower plenums.
- 4) The transfer lags of the hot leg and cold leg primary coolant flow between the pressure vessel and the steam generator are expressed by the first order lags.
- 5) Typical one steam generator is taken into consideration (unbalance of steam generators is ignored)
- 6) One point approximations are applied to the thermo-hydraulic equations of the reactor core and the steam generator.
- 7) Electric power generation is proportional with the first order lag of turbine inlet steam pressure at close on the operating point.
- 8) Primary loop pressure is kept to constant. (the trouble of pressurizer is ignored)

- 9) The speed of control rods is controlled by the combined signal, ΔT_{AVT} , as shown in Fig.1 a) and the reactivity worth of control rods is $1.5 \times 10^{-4} \Delta K/K/in$.
- 10) P-I controller is provided on the throttle valve control, where the difference between the demand power and the generated power is utilized as an error signal.
- 11) Steam damp valve is controlled by the combined signal, ΔT_{error} , as shown in Fig.1 b).



a) Control rods speed

b) Steam damp flow

$$\Delta T_{AVT} = \frac{1 + 30s}{1 + 3s} t_{AVT} - \frac{0.059}{1 + 3s} P_e + \frac{4}{9} \left(1 - \frac{1}{1 + 50s} \right) n$$

$$\Delta T_{error} = \frac{1 + 10s}{1 + 3s} t_{AVT} - \frac{0.059}{1 + 3s} P_e$$

- t_{AVT} ; deviation of average coolant temperature ($^{\circ}C$)
- P_e ; deviation of electric power generation (MWe)
- n ; deviation of average neutron flux (%)

Fig.1 Control characteristics of control rods speed and steam damp flow

We assumed that the following signals may be utilized in the diagnosis system, i.e. 1) average neutron flux N , 2) primary coolant temperatures measured at the inlet and outlet of steam generator T_{Si} , T_{So} , 3) primary coolant flow G , 4) main steam temperature T_{stm} , 5) steam pressure measured at turbin inlet P_i , 6) feed water flow G_w , 7) steam generator level L_s , 8) out-put electric power P_e and 9) combined signals ΔT_{AVT} and ΔT_{error} . The average coolant temperature is obtained as the average value of T_{Si} and T_{So} , and main steam pressure is obtained from the main steam temperature.

3. LINEAR DISCRIMINANT FUNCTION (BLOCK 1)

The detection and classification of the anomalous state are accomplished by pattern recognition technique utilizing the signals

obtained from the multitude of detectors in the plant. A set of detected signals is identified with one of the patterns (categories) prescribed to present the normal and several anomalous states in multi-dimensional space, by applying a linear discriminant function. The discriminant function is learned by the computer beforehand from a set of training data generated by a plant simulator.

The normal probability distribution function of category g is given by

$$F_g(\mathbb{X}) = (2\pi)^{-\frac{p}{2}} |\Sigma_g|^{-\frac{1}{2}} \exp\left[-\frac{1}{2}(\mathbb{X} - \mu_g)^t \Sigma_g^{-1} (\mathbb{X} - \mu_g)\right] \quad (1)$$

where \mathbb{X} is vector of variables (size p)
 μ_g is mean vector of variables at category g (size p)
 Σ_g is variance-covariance matrix at category g (size $p \times p$).

Eq.(1) can be interpreted to represent the likelihood L_g , and its logarithm is written in the form

$$-\ln L_g = \frac{p}{2} \ln 2\pi + \frac{1}{2} \ln |\Sigma_g| + \frac{1}{2} (\mathbb{X} - \mu_g)^t \Sigma_g^{-1} (\mathbb{X} - \mu_g) \quad (2)$$

Then the logarithm of likelihood ratio between categories 1 and 2 is given by

$$z = \ln \frac{L_2}{L_1} = (\mu_2 - \mu_1)^t W^{-1} \mathbb{X} + \frac{1}{2} (\mu_1^t W^{-1} \mu_1 - \mu_2^t W^{-1} \mu_2) \quad (3)$$

where W is the variance-covariance matrix assumed to be common to the categories 1 and 2.

Since the mean vectors μ_1 , μ_2 and variance-covariance matrix W are estimated from the set of training data, Eq.(3) is rewritten by

$$z = b^t \mathbb{X} + c \quad (4)$$

and the linear discriminant function is defined by

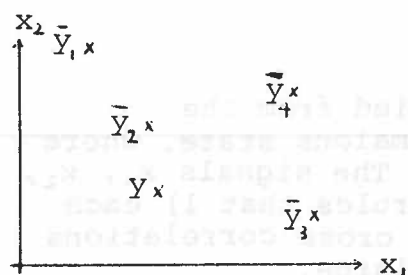
$$y = b^t \mathbb{X} \quad (5)$$

The sampled (or observed) data \mathbb{X} is identified with one of the two predetermined categories by the following rule,

$$\begin{aligned} |y - \bar{y}_1| < |y - \bar{y}_2| & \quad \text{category 1,} \\ |y - \bar{y}_1| > |y - \bar{y}_2| & \quad \text{category 2,} \end{aligned}$$

where y is calculated by Eq.(5), and \bar{y}_1 and \bar{y}_2 are given by $b^t \mu_1$ and $b^t \mu_2$, respectively.

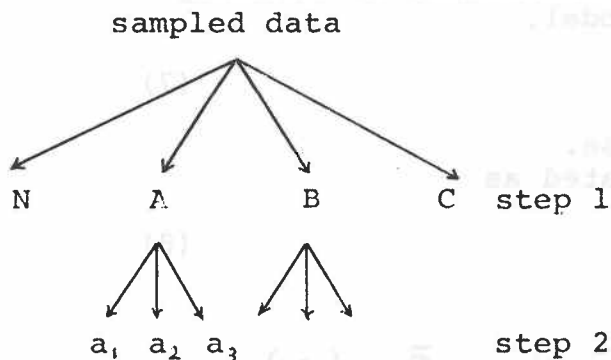
Above procedure is repeated for all possible pairs of predetermined



Pair	Desig.	Ident.
1,2	2	2
1,3	3	
1,4	4	
2,3	2	
2,4	2	
3,4	3	

categories, and the sampled data X is identified to belong in a category designated the greatest number. Two dimensional example is shown in Fig.2, where the sampled data is identified to belong in a category 2.

Fig.2 Procedure of identification



If it is necessary, the stepwise identification technique as shown in Fig.3 can be applied on the sampled data. In step 1, a set of sampled data is classified into large categories N (normal), A, B, C, then, for example, category A is further identified into small categories a_1 , a_2 and a_3 in step 2.

Fig.3 Stepwise discrimination

4. SIMPLIFIED DYNAMIC MODEL AND KALMAN-FILTER (BLOCK 2)

When a set of sampled data is identified into one of the predetermined categories by block 1, one of the Kalman-filters corresponding to the identified category is selected from block 2, and the anomaly source (disturbance) is estimated from a set of sampled data corresponding to the selected Kalman-filter. The Kalman-filters provided in block 2 are made beforehand from the simplified dynamic models corresponding to the predetermined categories.

A simplified dynamic model corresponding to the individual category is identified by the first order simultaneous ordinary differential equations using the training data, where the signals obtained from several selected detectors are treated as the state variables, i.e. a simplified dynamic model corresponding to the category 1 is identified as follows.

A dynamic model is given as

$$\frac{dX}{dt} = AX' + Bu \quad (6)$$

where

$$X' = \begin{pmatrix} x_1 \\ \vdots \\ x_k \end{pmatrix}, \quad A = \begin{pmatrix} a_{11} & \dots & a_{1k} \\ \vdots & \ddots & \vdots \\ a_{k1} & \dots & a_{kk} \end{pmatrix}, \quad B = \begin{pmatrix} b_1 \\ \vdots \\ b_k \end{pmatrix},$$

x_1, x_2, \dots, x_k ; signals obtained from selected detectors,
 u ; disturbance.

The coefficient matrices A and B are identified from the training data obtained for the categorized anomalous state, where the method of the least squares is applied. The signals x_1, x_2, \dots, x_k are selected empirically under the two rules that 1) each signal shows the typical time behavior, 2) the cross correlations between the signal and disturbance are rather large.

In order to get the estimation of disturbance u , following assumption is made in the filter model,

$$\frac{du}{dt} = v \quad (7)$$

where v is assumed to be white noise.

Thus, the system equation is formulated as

$$\frac{dX}{dt} = \bar{A}X + \bar{B}v \quad (8)$$

where

$$X = \begin{bmatrix} u \\ x_1 \\ \vdots \\ x_k \end{bmatrix}, \quad \bar{A} = \begin{bmatrix} 0 & 0 & \dots & 0 \\ B & A & & \end{bmatrix}, \quad \bar{B} = \begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix}.$$

Since there are two cases that the disturbance u is detected directly and not, the observed vector Y is given by

$$Y = HX + w \quad (9)$$

where

$$H = \begin{bmatrix} 1 \text{ or } 0 & & & \\ & 1 & & 0 \\ & & \ddots & \\ 0 & & & 1 \end{bmatrix}, \quad w = \begin{bmatrix} w_0 \text{ or } 0 \\ w_1 \\ \vdots \\ w_k \end{bmatrix},$$

w_0, w_1, \dots, w_k ; equivalent observation noises which simulate the system noises and observation noises of the actual plant.

The filter equation and the covariance equation for Eq.s (8) and (9) are given by

$$\frac{d\hat{X}}{dt} = \bar{A}\hat{X} + P H^t R^{-1} (Y - H\hat{X}) \quad (10)$$

$$\frac{dP}{dt} = \bar{A}P + P\bar{A}^t + \bar{B}Q\bar{B}^t - P H^t R^{-1} H P \quad (11)$$

where \hat{X} is the estimation of X , Q is the covariance matrix of v , R is the covariance matrix of w and P is the covariance matrix of $(\hat{X} - X)$.

The estimation \hat{x} is obtained by solving the Eq.s (10) and (11) where the variance of v is treated as parameters and the reasonable value of variance is obtained from computer experiments.

5. COMPUTER EXPERIMENTS

The system noises and observation noises are included in the detector signals obtained from the actual plant. In computer simulation, these noises are simulated by the equivalent observation noises which superposed on the sampled data at the digital computer side. On the other hand, the noises terms of the training data may be ignored because the training data are obtained from the plant simulator or the many times repetition of training in the actual plant.

As mentioned before, following four sorts of anomalous states are taken into consideration, i.e.

- 1) Change of the reactivity ρ , (two kinds of ramp change)

$$\begin{aligned} \rho &= (\rho_m/T)t & \text{at } t \leq T, & \quad \rho_m = \pm 0.0125\% \sim \pm 0.1\% \\ \rho &= \rho_m & \text{at } t > T, & \quad T = 20 \text{ sec or } 100 \text{ sec} \end{aligned}$$

- 2) Decreases of the primary coolant flow G , (exponential change)

$$\begin{aligned} G &= G_0 - g_m \{1 - \exp(-t/T_0)\}, & \quad g_m &= 0.05G \sim 0.2G_0 \\ & & \quad T_0 &= 20 \text{ sec} \end{aligned}$$

- 3) Change of the feed water flow G_w , (exponential change)

$$\begin{aligned} G_w &= G_{w0} - g_{wm} \{1 - \exp(-t/T_1)\}, & \quad g_{wm} &= \pm 0.025G_{w0} \sim \pm 0.15G_{w0} \\ & & \quad T_1 &= 20 \text{ sec} \end{aligned}$$

- 4) Change of the demand power P_e , (step and ramp change)

$$\begin{aligned} P_0 &= P_{00} - p_m, & \quad p_m &= \pm 0.025P_{00} \sim \pm 0.2P_{00} \\ P_0 &= P_{00} - (p_m/T_2)t & \text{at } t \leq T_2, & \quad T_2 = 100 \text{ sec} \\ P_0 &= P_{00} - p_m & \text{at } t > T_2. & \end{aligned}$$

In our computer experiments, the sampling time of data is fixed to 0.5 sec and the equivalent observation noises are assumed to be white noises with the cut-off frequency of 2 Hz. The standard deviations of the equivalent observation noises of detected signals are shown in Table 1.

The linear discriminant functions of block 1 are composed using the observed data as shown in Table 1. The present operating state is identified with one of the categories prescribed to represent the normal and 28 of anomalous categories. The identification was made every 12.5 sec using the average data of past 25 sec (past 50 samples).

As an example, the dynamic behavior of eight detected signals and the time transition of the identification result due to the reactivity disturbance of $\rho_m = 0.05\%$, $T = 100$ sec are shown in Fig.4. The similar results for all prepared anomalous states are summarized as shown in Table 2, where the anomalous states belong to the same sort are classified into the several categories separated

Table 1. Detected signals utilized in the diagnosis system

Detected signal	Noise level (standard deviation)	Block 1	Utilization		
			Dynamic model ξ	G	G_w
Average neutron flux	$\approx 0.4\%$ (5MWt)	o			
Temp. of S.G. inlet	0.5 °C	o		o	
Temp. of S.G. outlet	0.5 °C			o	
Average coolant temp.	0.5 °C		o		
Main steam temp.	0.5 °C	o	o		o
Press. of turbin inlet	0.5kg/cm ²	o			
S.G. level	2.5%	o			o
Electric power	0	o			
Control signal ΔT_{Avq}	0.5 °C	o			
Movement of control rods (Primary coolant flow)	5%	o		u	
(Feed water flow)	5%				u

by the dotted lines. The training data for each category is indicated by the mark T. The results show that the correct classification was accomplished within the reasonable time.

Since the estimation of the demand power change will not be necessary, the simplified dynamic models were identified for other three sorts of anomalous states. The state variables (detected signals) utilized in the dynamic models are shown in Table 1, where the same state variables are utilized in the all categories belong to the same sort of anomalous state.

The typical results of the disturbance estimation and the evaluations of estimation error are shown in Fig.5, where the estimation error E_e is defined as,

$$E_e = \frac{\int_0^{T_e} |u - \hat{u}| dt}{\int_0^{T_e} u dt}, \quad T_e = 300 \text{ sec}$$

The results show that the disturbances can be estimated with the accuracy of about 20%~30%, even if they are not detected directly.

6. CONCLUSION

A diagnosis system proposed in this paper is relating to the early detection of the anomalous state and the estimation of the anomaly source, where the linear discriminant function technique and Kalman-filter technique were utilized. The applicability of this diagnosis system in the actual power plants was examined using a PWR plant simulator.

The results of computer experiments showed that 1) the detection and the classification of the anomalous state were accomplished within the reasonable time by block 1, 2) the estimation of the anomaly source (disturbance) was performed with reasonable accuracy by block 2, and 3) the computation time was short enough for the real time diagnosis. Thus, we conclude that this diagnosis system will be successfully applied in the actual plants.

In order to improve the ability and reliability of this diagnosis system, future studies on the following items will be necessary;

- 1) Improvement of the plant simulator.
- 2) Increase of the presumed anomalous states.
- 3) Optimization of the number and size of categories.
- 4) Study on the multiplex anomaly sources.
- 5) Study on the selection method of detected signals which are utilized in block 1 or block 2.
- 6) Study on the applicability of non-linear equations and non-linear filters in block 2. (In our previous study, the utilization of non-linear filter took much computation time and did not remarkably improve the estimation results.)
- 7) Development of the more reliable methods.

Acknowledgment

The authors gratefully acknowledge the valuable discussion offered by Dr. T. Hoshino, Associate professor, Institute of Atomic Energy, Kyoto University. Acknowledgment is also to Mr. K. Tokura, who have cooperated with us in the course of his work for the Bachelors' thesis.

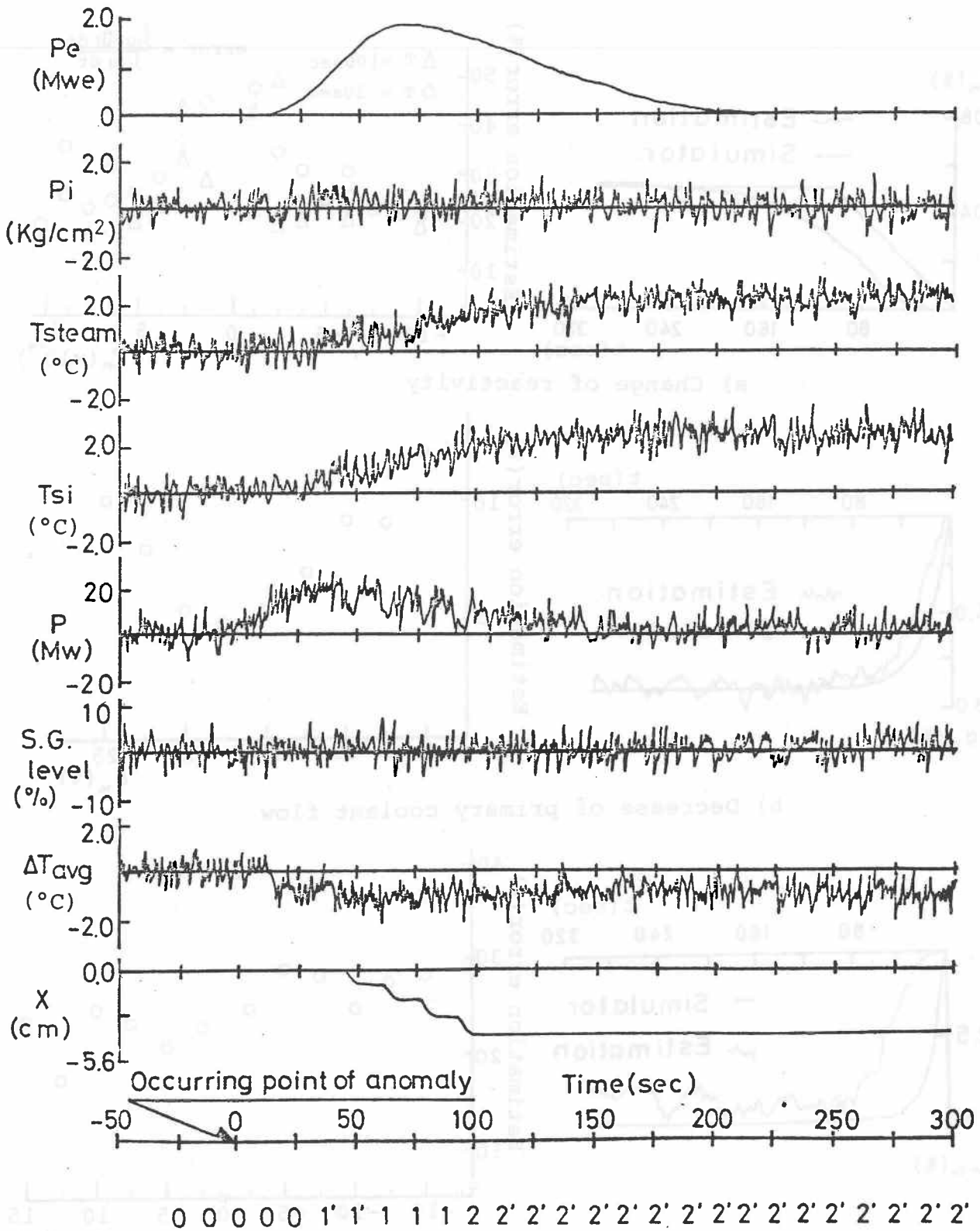
references

1. S. Ina, H. Yoshikawa and J. Wakabayashi; Proc. Power Plant Dynamics, Control and Testing. 21 (1973)
2. S. Ina, H. Yoshikawa and J. Wakabayashi; J. Nucl. Sci. Tech. Vol. 11, p 275-283 (1974)
3. J. Wakabayashi, K. Yamaguchi, S. Ina and J. Kondo; Proc. 2nd Power Plant Dynamics, Control and Testing. 12 (1975)
4. Y. Shinohara and R. Oguma; Nucl. Sci. Eng. Vol. 52 p 76-83 (1973)
5. S. Arimoto; Kalman Filter (Japanese), Sangyo-Tosyo Inc. (1977)
6. A. Fukumoto and J. Wakabayashi; Preprint, 1978 Fall Meeting, At. Energy Soc. Japan C-38 (Japanese) (1978)
7. A. Fukumoto and J. Wakabayashi; Preprint, 1979 Fall Meeting, At. Energy Soc. Japan A-51 (Japanese) (1979)

Table 2 Results of the classification of disturbance (Block 1)

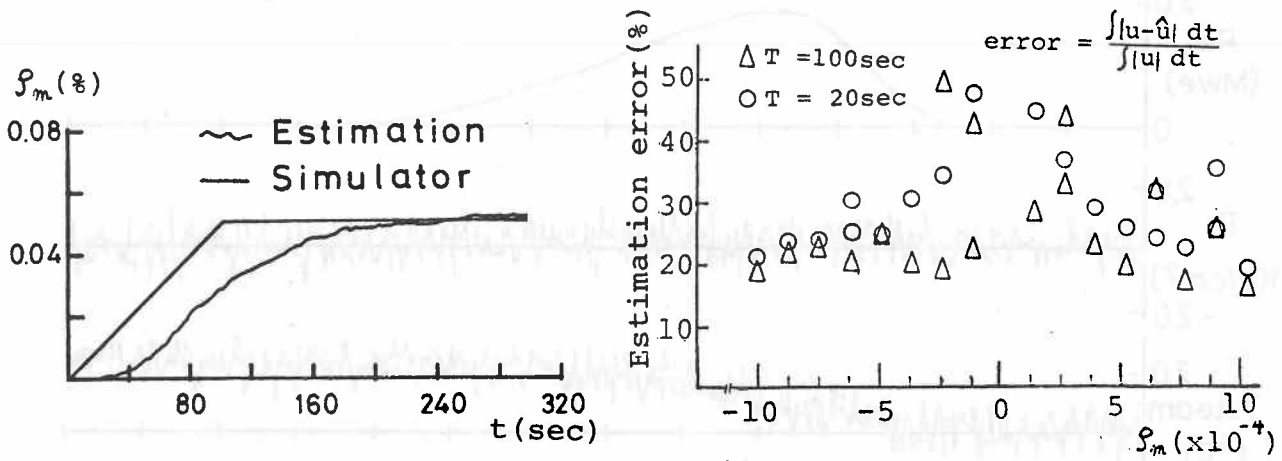
Disturbance u	No.	Time (x12.5 sec)																				
		0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
20 sec ramp	T-.0125	1	0	0	1'	1'	1'	1'	1	1	1
	-.025	1	0	0	1'	-8	1'	1'	1'	1	1	1
	-.0375	1	0	0	1'	2	2	2
	T-.05	2	0	0	1'	2	2	2
100 sec ramp	-.0625	2	0	0	1'	2	2	2	3	3	2	3	3	3	3	2	2	2	3	3	3	3
	T-.075	3	0	1'	-9	3	3	3
	-.0875	3	0	1'	2	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3
	T-.1	4	0	1'	2	3	4	4	4
20 sec ramp	T-.0125	1'	0	0	0	0	0	0	1'	1'	1'
	-.025	1'	0	0	0	0	-8	1'	1'	1'	1	1	1	1	1	1	1	1	1	1	1	1
	-.0375	1'	0	0	0	1'	1'	1'	1'	1	1	1	2'	2'	2'
	T-.05	2'	0	0	0	1'	1'	1	1	1	2	2'	2'	2'
100 sec ramp	-.0625	2'	0	0	0	1'	1'	1	1	2	3	3'	3'	2'	2'	3'	2'	2'	2'	.	.	.
	T-.075	3'	0	0	1'	1'	1'	1	2	3	3'	3'	3'
	-.0875	3'	0	0	1'	1	1	2	3	3	3'	3'	3'
	T-.1	4'	0	0	1'	-8	1	2	2	3	3'	3'	4	4	4	4	4	4	4	4	4	4
20 sec ramp	T-.0125	-1	0	0	0	7	7	-1	-1	-1	-1	-1	-1	-1	-1
	-.025	-1	0	0	10	10	7	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1
	-.0375	-1	0	0	10	-2	-1	-1	-1	-2	-2	-2
	T-.05	-2	0	0	7	-2	-2	-2
100 sec ramp	-.0625	-3	0	-7	7	-2	-2	-2	-2	-2	-2	-2	-3	-3	-2	-2	-3	-3	-3	-2	-2	-3
	T-.075	-3	0	-7	10	-2	-3	-3
	-.0875	-4	0	7	-1	-3	-4	-4	-4
	T-.1	-4	0	7	-2	-3	-4	-4	-4
coolant g _m (%)	T-5	-5	0	0	0	-5	0	-5	-5	-5
	-7.5	-5	0	0	0	-5	0	-5	-5	-5
	-10	-5	0	0	0	-5	-5	-5	-5	-5
	-12.5	-5	0	0	-5	-5	-5	-5	-5	-5	-5	-6	-6	-6
feed water g _w (%)	-15	-6	0	0	-5	-5	-5	-6	-6	-6
	-17.5	-6	0	0	-5	-6	-6	-6
	T-20	-6	0	0	-5	-6	-6	-6
	demand power p(%)	T2.5	7	0	0	0	0	0	9	9	9	9	9	9	9	7	7	7
-5		7	0	0	0	0	0	9	9	9	9	9	9	9	8	8	8
T7.5		8	0	0	0	7	9	9	9	9	9	9	9	9	8	8	8
-10		8	0	0	0	7	7	9	9	9	9	9	9	9	8	8	8
demand power ramp	T12.5	9	0	0	0	7	7	9	9	9
	-15	9	0	0	0	7	7	9	9	9
	T-2.5	-7	0	0	0	0	-7	-7	-7	-7
	-5	-7	0	0	0	0	-7	-7	-8	-8	-7	-7	-8	-8	-8	-8	-8	-7	-7	-7	-8	-8
demand power ramp	T-7.5	-8	0	0	0	-7	-7	-8	-8	-8
	-10	-8	0	0	-7	-8	-8	-8
	T-12.5	-9	0	0	-8	-8	-8	-8	2'	2'	2'	2'	2'	2'	2'	2'	2'	2'	2'	2'	2'	2'
	-15	-9	0	0	-8	-8	1	2	2'	2'	2'	2'	2'	2'	2'	2'	2'	2'	2'	2'	2'	2'
demand power ramp	T2.5	10	0	0	0	0	0	0	10	10	10
	-5	10	0	0	0	0	0	0	10	10	10
	T7.5	11	0	0	0	0	0	0	10	10	10	11	11	11
	-10	11	0	0	0	0	10	10	10	10	10	11	11	11
demand power ramp	12.5&15	11	0	0	0	0	10	10	10	10	11	11	11
	17.5&20	11	0	0	0	0	10	10	10	10	11	11	11
	T-2.5	-10	0	0	0	0	-7	0	-10	-10	-10
	-5	-10	0	0	0	0	-10	-10	-10	-10	-10	-10	-10	-10	-10	-10	-10	-10	-10	-10	-10	-10
demand power ramp	T-7.5	-11	0	0	0	0	-10	-10	-10	-10	-10	-10	-11	-11	-11
	-10	-11	0	0	0	0	-10	-10	-10	-10	-10	-11	-11	-11
	-12.5&-15	-11	0	0	0	-10	-10	-10	-10	-10	-11	-11	-11
	-17.5&-20	-11	0	0	0	-10	-10	-10	-10	-10	-11	-11	-11

Step change of the demand power were classified more quickly,
No. and T; Number of category and training data utilized for each category.

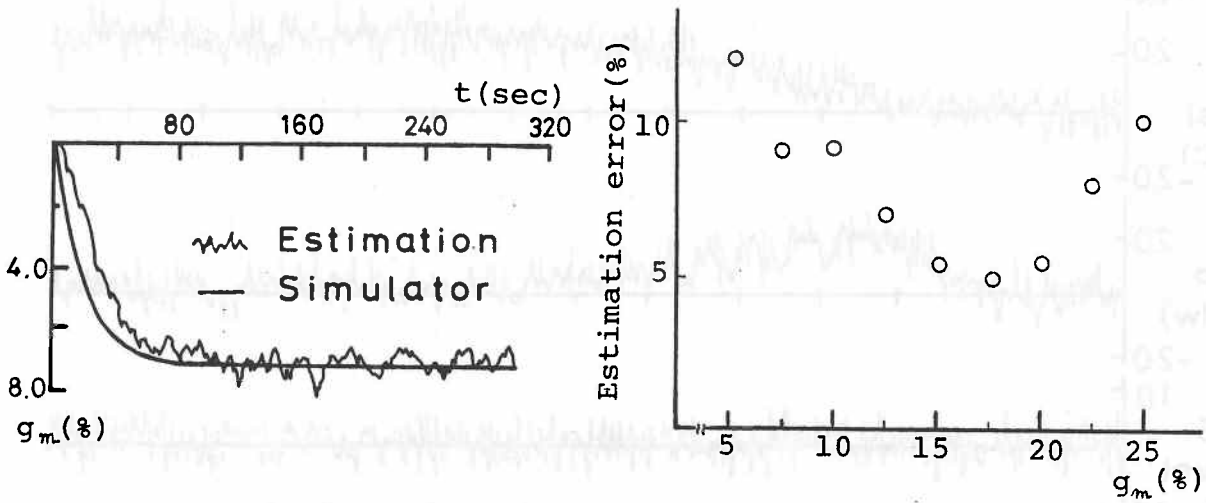


Time transition of the identification

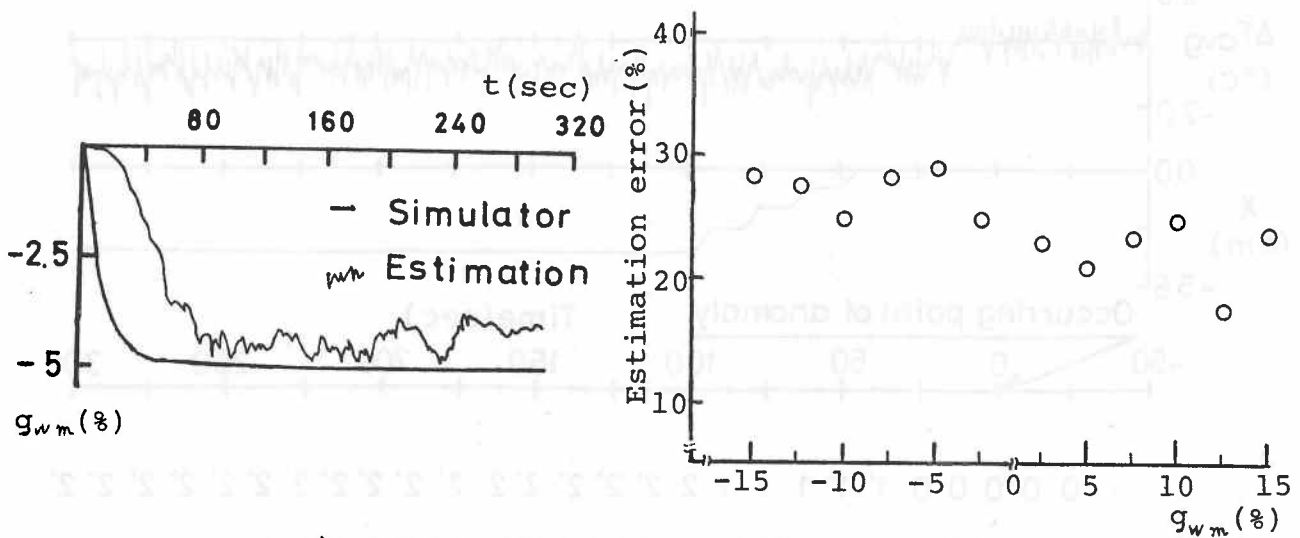
Fig.4 Dynamic behavior of the detected signals and time transition of the identification



a) Change of reactivity



b) Decrease of primary coolant flow



c) Change of feed water flow

Fig.5 Typical results of the disturbance estimation and the evaluation of estimation error

R. Černý

THE DYNAMIC CLASSIFICATION AND REDUCTION OF ALARMS IN
COMPUTER-BASED INFORMATION SYSTEMS

Robert Černý

Power Research Institute

Prague

THE DYNAMIC CLASSIFICATION AND REDUCTION OF ALARMS IN COMPUTER-BASED INFORMATION SYSTEMS

1. Introduction

Computer-based information systems for power plant operators have become a regular part of power unit control systems. In a variety of system functions the commonly accepted alarm function is of the most important. The system checks periodically whether the value of any variable, both analog and binary, is within the normal region. If the value of a variable gets out of this region, the system recognizes the variable to be in an alarm state. The information of such alarm is then presented in a form of an alarm message to the operator, and is registered as individual item in an alarm log of the power unit.

The alarm function of this kind appears to be useful and convenient in common cases of operation disturbances, when the number of alarm messages is small. However, when more extensive disturbances occur the number of alarm messages can exceed reasonable limits, so that the operator is no more capable to process all the information presented.

This experience, gained in operation of conventional power unit has led us to devise dynamic classification of alarms as computer function which reduces the number of alarm messages presented to the operator without loss of meaningful information. The conditions for realization were:

- i: minimal alteration of existing programming system
- ii: simple algorithmic solution so that adoption of the function for all input variables would not adversely affect the throughput of the computer system
- iii: the suppressed data must be available to the operator on demand.

In accordance with this the alarms are classified in hierarchical priority order and alarm messages are derived only from alarms of highest significance. The suppressed data and other related information form predefined groups of variables, which may be presented to the operator on demand.

2. Classification and reduction of alarm messages

The task of this system function is to reduce the number of alarm messages which appear on alarm display. The entries of alarm messages in power units alarm log are not affected.

All input variables, from which an alarm can be derived are of three types:

- a) an alarm is displayed on alarm display whenever it appears
- b) an alarm is never displayed (and enters only an alarm log)
- c) an alarm is displayed conditionally, in dependence on the state of other variables.

The variables of the type c) are divided into group corresponding to individual parts of technology, so that variables in a group are to some extent mutually dependent. Variables within a group are classified into four priority levels (0+3), which express the significance of alarm related to each variable. The system operates as follows:

At appearance of an alarm with the priority level i ($i=0,1,2,3$)

- an alarm message is typed in the alarm log
- an alarm message is displayed on alarm CRT unless other alarm from the same group and of the same or higher priority has been already displayed. The alarm messages of the highest priority (3) are displayed in all cases
- an alarm message of lower priority (if it exists) is withdrawn from the alarm display.

If an alarm on the level i ceases to exist,

- the event is recorded in an alarm log
- the alarm message is withdrawn from the alarm display
- other alarm message from the same group and of the same (or lower) priority is displayed.

In consequence of this processing of alarms only the alarms of momentarily highest significance from each group are presented on alarm display.

In addition to this standard procedure a provision has been made for individual, non-standard processing of alarms by special subroutine. By this any logic function for presenting new alarm messages and for withdrawal of earlier ones can be realized.

3. Acknowledging of alarms with additional information

The function of classification of alarms has been extended by the possibility to acquire additional data related to individual alarms on demand of the operator.

In existing system the newly appeared alarms have to be acknowledged by the operator. The acknowledgment is meant to assure that an alarm had been noticed and would be taken care of. In the proposed extension of this function the operator has the possibility of choice to acknowledge new alarm as before or - by pressing different key on the operator's console - to acknowledge it and obtain additional information related to the alarm.

In accordance with this any variable can have a group of related variables that render additional information on the immediate state of the process. Such group of variables is available to the operator on a monitor display immediately after acknowledging the latest alarm message, or - if he requires a group belonging to other than latest alarm variable - after typing the variable name on operator's keyboard.

By acknowledging the alarm with demand of additional data the monitor CRT clears and the group of data appear in the following format:

first line - the variable, to which the following group is related

second line - blank

third to twentieth line - up to 18 variables and their updated values together with a note whether the variable is in an alarm state.

As the groups of additional data usually contain variables of a corresponding group of classification, the operator thus has at his disposal an information of all variables of the classification group, though some of alarm messages derived from the classification group might be suppressed.

4. Function verification

The described algorithm has been devised with the intention to introduce the function in a nuclear power plant with PWR. As up to present there has not been the possibility to verify it on an existing plant, it has been introduced in operation of a 200 MW coal-fired power unit, which is equipped with similar computer information system as planned for the said nuclear plant.

The algorithm has been programmed as an extension to the existing data acquisition program system. For introducing the programs and data into the system a special program has been used, which enables easy data entry and modification even during the operation.

The power unit information system has approximately 1500 input variables (600 analog, 900 binary), from all of which some 930 are alarm variables. The whole set of input variables has been divided into 28 subsets, each describing individual part of the power unit. The set of alarm variables has been divided into 138 classification groups and the number of related groups of additional information data amounts to 81.

The division and allocation of individual variables has been the main task in introducing the proposed system function. In approximately half of cases the priority allocation could be easily derived from the hierarchical order of analog and binary variables measured on identical spots (the threshold devices are set to superimpose the limits on corresponding analog values), so that binary alarm variables are usually on higher significance level than analog alarms. The remaining half of alarm variables has been allocated to individual priorities in accordance with operation manuals. The whole system has been improved in the course of operation with the assistance of operational personnel.

The devised function, though quite simple in realization, is one of the ways how to reduce the number of alarm messages presented to the operator in critical situations. The experience gained in verification on conventional power unit makes the use of this system function on nuclear power unit desirable.

M. Lind

THE USE OF FLOW MODELS FOR DESIGN OF PLANT OPERATING
PROCEDURES

THE USE OF FLOW MODELS FOR DESIGN OF PLANT OPERATING PROCEDURES

M. Lind

IWG/NPPCI SPECIALISTS' MEETING ON PROCEDURES AND SYSTEMS FOR
ASSISTING AN OPERATOR DURING NORMAL AND ANOMALOUS NUCLEAR
POWER PLANT OPERATION SITUATIONS

INTRODUCTION

The successful operation of process plant is dependent on a variety of procedures, for e.g. plant control, testing, maintenance, etc., here we will consider so-called operating procedures which are provided for plant control. We will especially be concerned with the plant information which is a sufficient basis for a systematic approach to the design of operating procedures.

In general, a procedure is a set of rules (an algorithm) which is used to control operator activity in a certain task. Thus, an operating procedure describes how actions on the plant (manipulation of control inputs) should be made if a certain system goal should be accomplished. The sequencing of actions, i.e. their ordering in time, depends on plant structure and properties, nature of the control task considered (goal) and operating constraints.

If described in relation to actual actions on the plant (start motor, close valve etc.) there is no formal difference between an operating procedure and the program which must be provided for an automatic sequential control system performing the same task. Thus, the present discussion is also relevant for the design of sequence automatics for plant control. In the following the term "operating procedure" will refer to both procedures used by the operator in plant control, and to programs for sequential automatics. Naturally, there will be some differences between operator procedures and programs for automatics for the same task. This is because there are differences in the specific nature of the "man-machine" and the controller-plant interfaces. However, these differences will not be considered here as they are not related to the problem of plant control on the level of description used here.

In the paper we will show how operating procedures can be structured into logically consistent parts by a decomposition into sequential and concurrent action sets. The decomposition is shown to originate from the topology of the pattern of material and energy flow in the plant, and to the nature of the specific control task considered. This analysis provides valuable information of how plant structure can be used explicitly in procedure design. It is shown how a category of models called flow models developed by the writer, can be used to represent flow topology in material and energy processing plants. Flow models will be used as a way of dealing with plant topology in procedure design.

The observation which leads to the consideration of flow models for procedure design is that e.g. start-up procedures for apparently dissimilar plant components as pumps and boilers show some common structural features. The reason for this is that the components are functionally equivalent in certain phases of their operation. Functional equivalence of components or systems can be expressed by using the language of flow models.

CONTROL TASKS IN PLANT OPERATION

In the operation of process plant we can distinguish between two categories of control which are related to different aspects of the coordination of plant functions. These categories are important for the discussion of task structure presented in the following section.

The first category includes the controls provided for optimization and for maintaining plant integrity during transients caused by external disturbances or by programmed changes in the operating conditions as e.g. changes of setpoints. Characteristic of this type of controls is that they are provided for a certain operating regime, i.e. they are not applicable if operating regime is changed. In material and energy processing plants, this category of controls performs a coordination of the redistribution of mass and energy stored in plant components.

The coordination problems discussed above are related to plant operations where structural changes do not occur. The second category of controls includes coordination problems related to changes in plant functional structure. This occurs when an integrated process must be established from a set of hitherto functionally unrelated plant components. In order to allow two process components to be connected, operational conditions for the two components must be equalized. (A boiler must be filled, heated and produce steam before it can be connected to the turbine. The turbine must be on correct speed before it can be synchronized with the grid etc.).

The division of a control task into subtasks according to the categories above leads to a decomposition of the associated goal and procedure into subgoals and subprocedures. Furthermore, to each task corresponds a plant subsystem which again is divided into subsystems by the task decomposition. However, plant subsystems obtained in this way will in general be overlapping, i.e. they will share components because the goal decomposition is based on the functional requirements and not on physical structure. In the following we will give a more detailed discussion of the decomposition of tasks and by this way give a meaning to the concept of task structure.

STATE-ACTION DIAGRAMS AND TASK STRUCTURE

According to the discussion in the previous section we can consider the operation of a process plant as a complex of activities related to several goal levels. The decomposition of a task into subtasks depends on what should be accomplished, i.e. the overall functional requirements, and on what can be accomplished within the constraints given by actual plant structure, choice of components, operational limits, etc.

We will now introduce the concept of a state-action diagram which can be used to represent the operational requirements to a process plant. This type of diagram is closely related to

state-diagrams used in automata theory for the definition of sequential machines, i.e. systems which operate in discrete time and which can be in a discrete number of states. A simple example of a state-action diagram for power plant is shown in fig. 1. Here we have assumed that the plant can be in only two major states "No power" and "Full power". The states are indicated by circles and the arrows indicate possible transitions. To each arrow a set of actions in the system corresponds, specified in an operating procedure. A set of actions is indicated by a square box. It should be noted that if the actions are ignored (i.e. the square boxes are deleted), we obtain a state-diagram for the plant. Conversely, if the states are ignored, we get a representation of the action structure. This will also be denoted the procedure structure as every action set (square box) is prescribed in a procedure.

The concept of a state-action diagram introduced here is closely related to the so-called precedence networks used in project management for solving planning problems (see e.g. Burman, 1972). In addition to these formal similarities, there are, however, much deeper interrelations between the problems of procedure design for process plant and project planning problems. This will be discussed later in the present paper.

Thus the state-action diagram has two aspects when used for functional specification. It is a description of plant behaviour in terms of a set of states and the specified transitions between them, this information is contained in the state-diagram. Furthermore it is a specification to the plant environment of the relation between the individual control tasks involved in plant operation. In the state-action diagram a control task is defined by the structure shown in fig. 2.

It is seen that in relation to the task definition the initial plant state S_1 is a condition (the task is only initiated if the plant is in state S_1). Furthermore, the task goal is the final state S_2 . (The goal is to transfer the plant to the state S_2). The way in which the transfer is made depends on the procedure used, i.e. on properties of the plant considered and design heuristics. This will be discussed later. As a state-action diagram can be divided into tasks as shown in fig. 3, it is a representation of the task structure.

It is clear that the specification of system function presented in a state-action diagram is related to a given level of detail in the description of the plant. Thus different choices of levels of detail lead to different state-action diagrams for the same system. Increasing the level of detail in the description leads to a modification of the diagram, because goals may decompose into subgoals (states for subsystems). This is illustrated in fig. 4 in a particularly simple case.

However, this decomposition cannot always be made because it is necessary to take into account the nature of the control tasks involved. This is the case for systems with strong internal variable interactions. Such systems must be considered as functional "wholes", and the control tasks associated with the change of state cannot even partially be related to a subsystem but is related to the behaviour of the whole. Fig. 5 illustrates this situation.

Now we have discussed the decomposition of tasks induced by division of the plant into subsystems, and it is realized that this decomposition may lead to concurrent subtask structures. In addition to this, we will consider task decomposition in the time domain and this will lead to subtask sequences. Assume that we have a control task relating system states S_1 and S_5 . If it is then possible to define a sequence S_2, S_3, S_4 of intermediate system states, we can decompose the task into a sequence of subtasks as shown in fig. 6.

The two decomposition principles described above can be used to break down a control task into a hierarchy of subtasks. As mentioned earlier, this decomposition cannot be done without taking system structure into consideration. A specification of a task describes what should be obtained. The decomposition into subtasks describes how the specifications are met within the constraints given by the physical structure of the plant.

FLOW MODELS

The function of process plant can be described in several ways depending on the modelling language used. Flow models as defined by the writer describe the topology of the pattern of material and energy flow in the plant. In this section we will give a short description of the basic concepts of flow modelling. For more details, see Lind (1979).

In flow modelling, the basic assumption is that every material and energy process can be described as an interaction between two fundamental types of processes. These are storage and transport processes. Storage processes include simple accumulation phenomena, i.e. pile-up of material or energy in a volume. But in addition to accumulation phenomena, storage processes may also include chemical processes, i.e. changes of material composition and changes of phase. Transport processes include the transfer of material and energy between two locations in space by convection, conduction and diffusion phenomena.

A processing plant is then described as an interconnection of material and energy storage and transport processes. The interconnection between processes is denoted a boundary.

The underlined concepts above constitute the basic vocabulary of flow modelling. The concepts are summarized in fig. 7, and we have furthermore introduced symbols used to represent the different processes in modelling. Using these symbols, a graph called the flow structure can be constructed from e.g. a plant flow sheet.

The major difference between the flow structure and a flow sheet is that a flow structure is a plant description in terms of fundamental processes whereas a flow sheet is structured according to processing components (unit operations). This implies that

the flow structure contains information which is not explicit in a flow sheet. Furthermore, the fundamental nature of the flow modelling concept makes a flow structure a consistent category of models, i.e. rules for model modification can be given (see op cit). This is not the case for flow sheets.

In addition to the basic concepts defined above, the concept of a conditioned process and an aggregate is also used in flow modelling. A conditioned process is a process which can be influenced (controlled).

An aggregate is a collection of interrelated transport and storage processes. Aggregates are used for representing plant subsystems for which the internal structure is ignored. These concepts are summarized in fig. 8.

An example of a flow structure for a conventional power plant is shown in fig. 9. The flow structure describes plant functional structure in an intermediate operating regime during boiler start-up (boiler is filled with water and heating is initiated, steam produced is absorbed in the start-up system).

TYPES OF SYSTEM INTERACTION AND SYSTEM DECOMPOSITION

The description of a process plant by its flow structure makes a decomposition of the system into subsystems possible. The decomposition is in fact an integrated part of the modelling activity, as it is related to some basic decisions which should be made when formulating a system flow structure. The decomposition concerns the mode of interaction which two systems may have within the framework of flow models.

We have the following two basic types of interaction as illustrated in fig. 10.

Typical examples of interaction by conditioning are the influences on system operation from control systems or service systems which support main plant processes. Note that the conditioning subsystem may itself be a material and energy processing system. Interaction by exchange of material and energy covers the interconnection of the basic processes of storage and transport at a boundary and boundaries between more complex processing aggregates.

The major difference between the two types of interaction is that in the conditioning interaction a unique direction of control is given. (A change in operating conditions of A2 will not influence A1 whereas a change in A1 influences A2). In the case of interaction by exchange of material and energy, no unique direction of control can be given in general, as a change in operating conditions of either A3 or A4 may influence the other. The conditioning of A2 by A1 is a coordination of their functions, whereas the systems A3 and A4 are functionally integrated.

The functional integration can be broken by adding a conditioned transport process as shown in fig. 11. This modification implies that the functions of A3 and A4 can be coordinated.

Each plant system can now be decomposed into a main process system and its associated subsystems. The subsystems fall into two classes, conditioning and processing subsystems according to the basic types of interaction defined in fig. 10.

The main process includes processes which perform material and energy processes, the purpose of which is defined in relation to the system environment. Thus the main process may be a conditioning or a processing subsystem to another plant system.

The conditioning subsystems are different types of subsystems which either control the main process or establish and maintain proper function of the main system (lubricating systems, demineralizer and make-up systems, etc.).

Processing subsystems are subsystems which function as sources or sinks of material and/or energy in relation to the main system.

The decomposition is illustrated in fig. 12 where it is indicated that a main system may have several subsystems of the two types. The couplings of the main system to the environment are ignored in the figure.

Due to the recursive nature of the concept of system, a system can be decomposed into a hierarchy of subsystems as exemplified in fig. 13.

TASK DECOMPOSITION

If we now consider a given control task and the associated system, the decomposition of the system flow structure as described in the previous section will provide a division of the task into subtasks. This division depends on the nature of the task.

As discussed earlier, we have two categories of control tasks in process plant operation. The first includes changes of system state within the same operating regime, i.e. the system flow structure is unchanged. A change of state requires a coordination of the function of the conditioning subsystems for the system considered. This can be concluded from fig. 12 as the only way to change state of MS is to change the states of CS1, CS2 The sequence of changes required can be deduced from the detailed structure of the main system flow structure and the change of state to be obtained in the different subsystems of the main system. As an illustration, let us consider the example in fig. 14. Here the main system has a tree structure internally.

If we now assume that the state of aggregate A1 should be unchanged, then the changes of state of C1, C2 and C3 (i.e. the control actions on the main system) should be coordinated to obtain

this. This means that the conditioning of flows to A1 is an integrated task. If the state of A2 should be changed, then a control heuristic (or a suitable control system design method) must be chosen to determine the sequencing of the changes of state in C3, C4 and C5.

In a material and energy processing plant a proper heuristic would be to prevent transient pile-up of mass or energy in processing components (or aggregates). This heuristic which is related to plant safety would imply the following rule:

If the material/energy content within an aggregate should be reduced/increased, then the source flows should be reduced/increased and/or sink flows should be increased/reduced. The choice depends on requirements to be met in neighbour aggregates.

We will not go further in the details of how a control task of the first category is decomposed into sub-tasks. This would require a discussion of the set of heuristics which can be used in connection with material and energy processing plants. This is a topic for further studies.

From the discussion above we can conclude that control tasks of type 1 are integrated, i.e. the state-action diagram defining the task has the structure as shown in fig. 5.

The second category of control tasks which coordinate changes in the operating regime of a system will now be discussed on the basis of decomposition of flow structure.

A change in operating regime includes a change of flow structure, i.e. either a functional interconnection of hitherto unrelated systems or a disconnection of a functionally integrated system. However, these operations require that the subsystems involved are properly conditioned, i.e. they must be in a state which allows an interconnection or disconnection to be done. This is necessary in order to avoid transient phenomena which in the ultimate may cause component failures. This means that a control task of type 2 includes subtasks of type 1 (conditioning of subsystems before interconnection/disconnection).

Two systems which must be functionally integrated must have a potential for interconnection. This is usually provided by a conditioned transport node (representing e.g. a control valve). Thus we can base our discussion on the situation shown in fig. 15.

Here we have shown two systems decomposed into their subsystems (MS, CS and PS). The systems are interconnected by a conditioned transport node. Two states of the subsystem conditioning the transport process correspond to functional interconnection and disconnection (opened and closed valve). The subtasks related to the interconnection of MS1 and MS2 would then be (it is assumed that they are disconnected, i.e. it is a condition for the coordination task that CS1 is in proper state):

- 1) Conditioning of MS1, i.e. the state of CS1 must be changed.
- 2) Conditioning of MS2, i.e. the state of CS3 must be changed.
- 3) Coordination of MS1 and MS2. This includes the change of state of CS2.

It should be noted that all subtasks are of category 1. The state-action diagram corresponding to this interconnection task is shown in fig. 16. An analysis in the case of system disconnection will lead to a similar state-action diagram.

As before we will need heuristics to determine the sequence of subtasks. As an example we could mention the following heuristic

Material flow boundaries must be established before pure energetic boundaries. This heuristic prevent that extreme energy densities occur in aggregates (i.e. high pressures or temperatures).

But as before, a more detailed study is necessary to formulate a sufficient set of heuristics for material and energy processing plants.

As an example of a state-action diagram for a complex task fig. 17 is included. It shows the interrelations between subtasks in the first phases in the startup of a conventional boiler. The startup procedure is taken from Pedersen (1974) and described here into the format of a state-action diagram. In this example we can identify sequences of subtasks of the different categories discussed earlier. Furthermore, some of the underlying heuristics can be identified (e.g. fill the boiler drum with water and establish air/gas flow before starting the burners).

PROCEDURE DESIGN

The previous discussion have described how a control task can be decomposed into subtasks. It has been shown how the flow structure of the system and the nature of the control task determine the decomposition. Furthermore, it has been discussed how design heuristics can be used to determine the sequencing of the individual subtasks. In this way we have formulated a structured approach to procedure design. However the method do only consider the aspects of procedure structure which are related to plant topology. We have not considered the aspect of time and resources of material and energy. This bring us back to the discussion of the interrelations between procedure design and project planning problems.

The problem of project planning is usually separated into three phases(see e.g. Burman, 1972)

Planning: The planning phase include the analysis of the logic of the situation (interrelations between the individual jobs to be done) by arranging the jobs in an order of precedence. This correspond exactly to the decomposition of a control task into subtasks as described in the present paper. The result of the ordering of jobs is presented in a precedence diagram. Here we obtain a state-action diagram. These two diagrams are formally equivalent.

Scheduling: The scheduling phase include a conversion of the plan into a feasible schedule. This is obtained by analysing the plan (the precedence or the state-action diagram) with reference to the use of available resources i.e. time and material and energy supplies. This is one of the aspects of procedure design which is not covered in this paper. This means that scheduling is dependent on plant information as time constants of plant processes and of storage capacities. This plant information is not represented in the flow structure.

Supervision:The supervision phase include the monitoring and correction activities which must be made in order to ensure adherence to schedule (i.e. the planned operation). These aspects of operating procedures are discussed in Goodstein (1979).

OPERATOR SUPPORT

The method for procedure design presented above may be used as a basis for computerized on-line procedure construction. The operator could use the plant computer to generate procedures in situations which are not predicted by the designer.

Such a facility would be an integrated part of a system for computer assisted plant diagnosis.

REFERENCES

Burman, P.J.: Precedence networks for project planning and control. (Mc. GrawHill, 1972, London), 374 p.

Goodstein, L.P.: Procedures for the operator. Their role and support. This conference.

Lind, M.: Flow models of material and energy processing systems. Risø-M-2201 (in preparation).

Pedersen, O.M.: An analysis of operator's information and display requirements during power plant boiler start. Risø-M-1738, Dec. 1974.



Fig. 1. Subdivision of state-action diagram into tasks



Fig. 2. Diagram of a task



Fig. 3. Diagram of a task

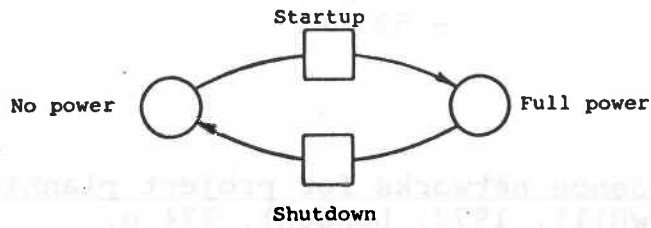


Fig. 1. Simple state-action diagram.

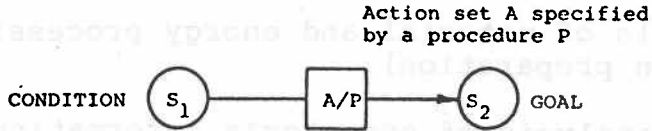


Fig. 2. A control task

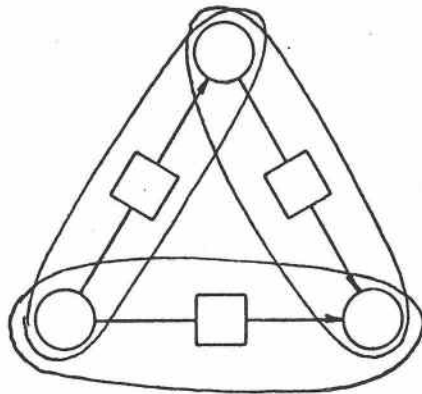


Fig. 3. Subdivision of state-action diagram into tasks

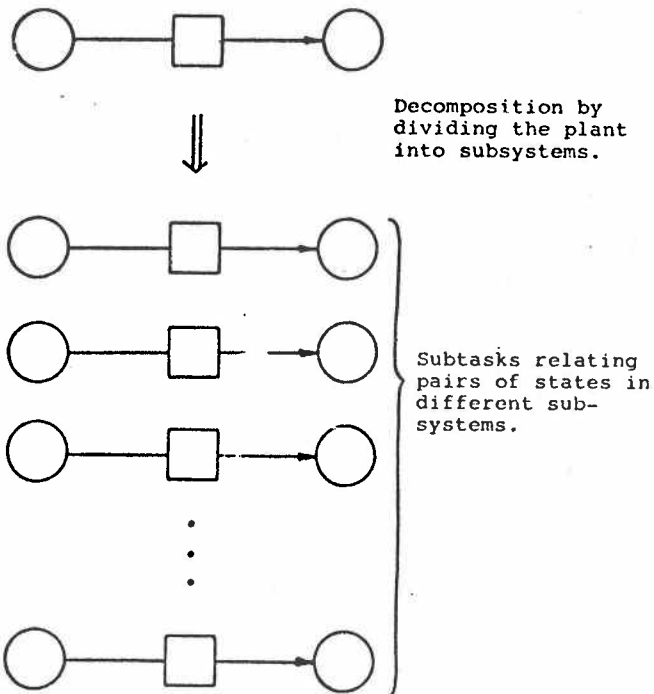


Fig. 4. Decomposition of a task into independent subtasks.

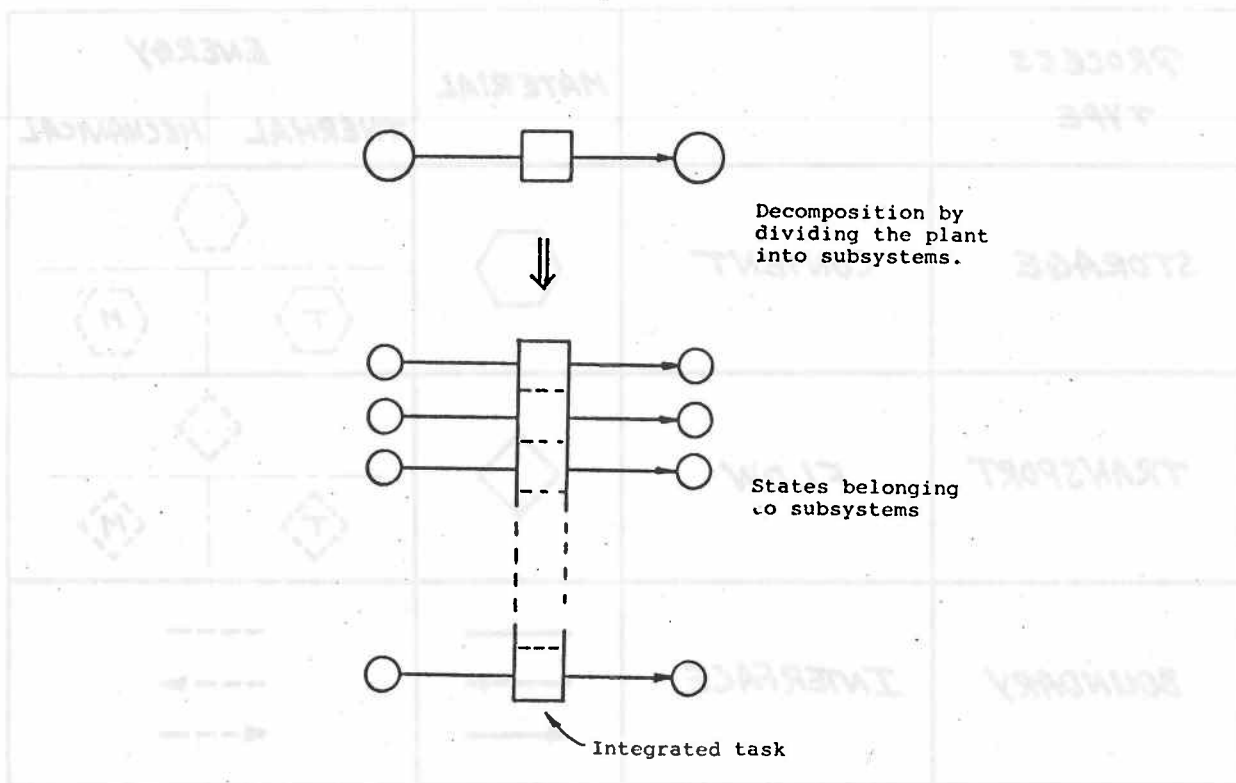


Fig. 5. Incomplete task decomposition when a functional whole is decomposed into subsystems

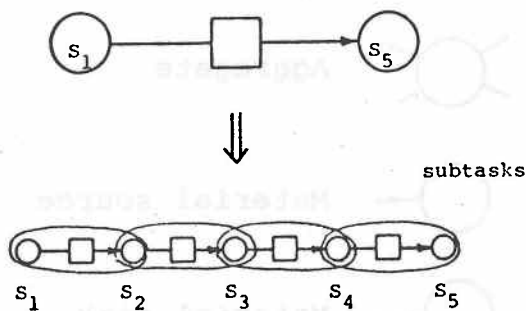


Fig. 6. Temporal task decomposition









PROCESS TYPE		MATERIAL	ENERGY	
			THERMAL	MECHANICAL
STORAGE	CONTENT			
TRANSPORT	FLOW			
BOUNDARY	INTERFACE			

Fig. 7. Flow modelling concepts and symbols.

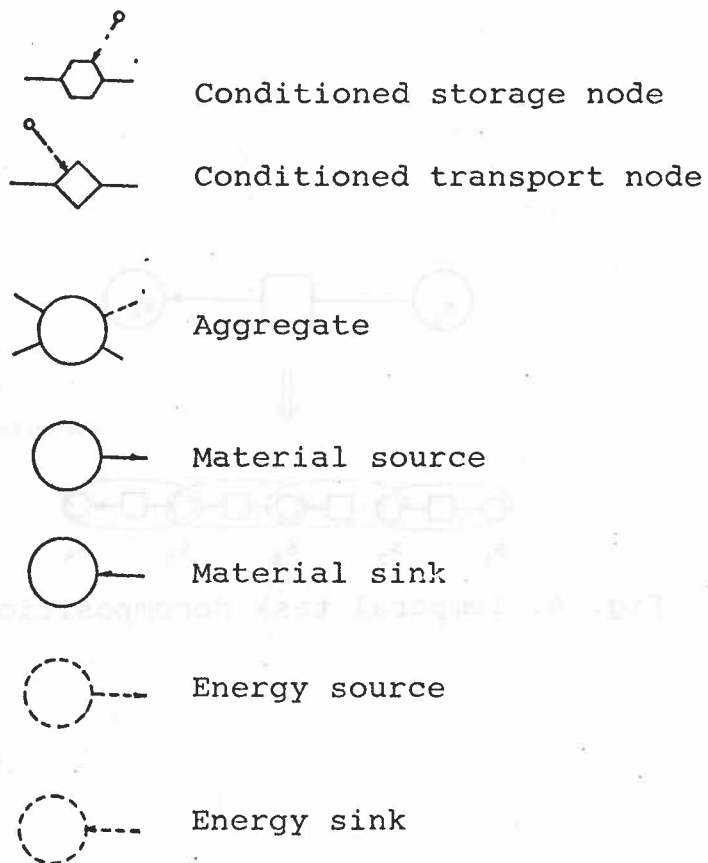


Fig. 8. Additional definitions

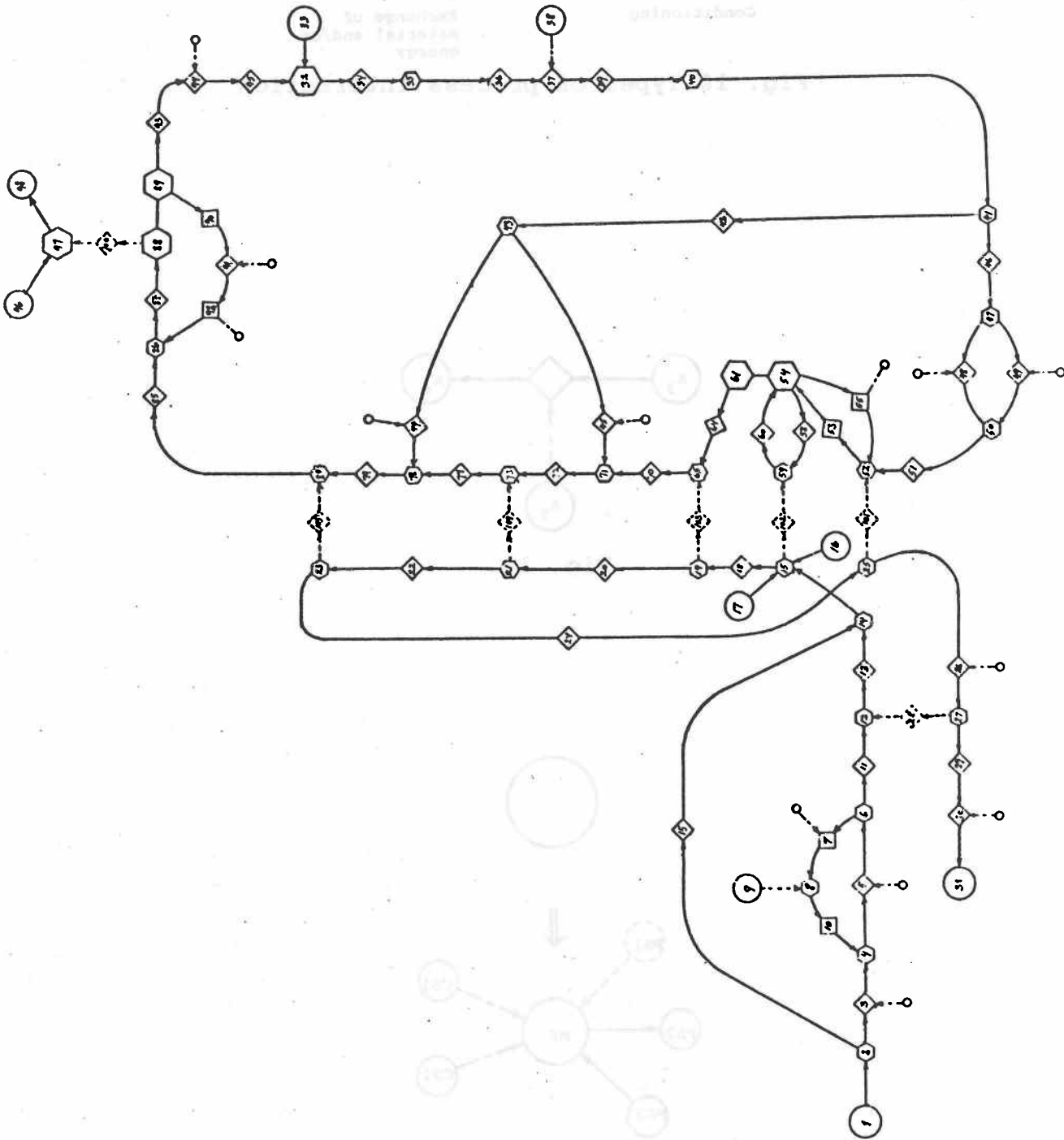


Fig. 9. Flow structure for a conventional power plant.

Fig. 12. Decomposition of system into main system and associated subsystems.



Fig. 10 Types of process interaction

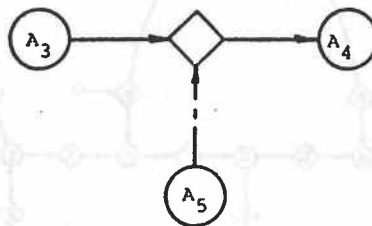


Fig. 11.

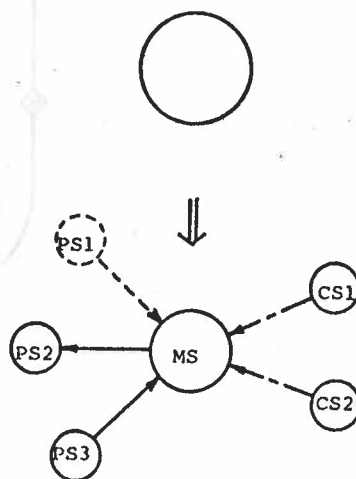


Fig. 12. Decomposition of system into main system and associated subsystems.

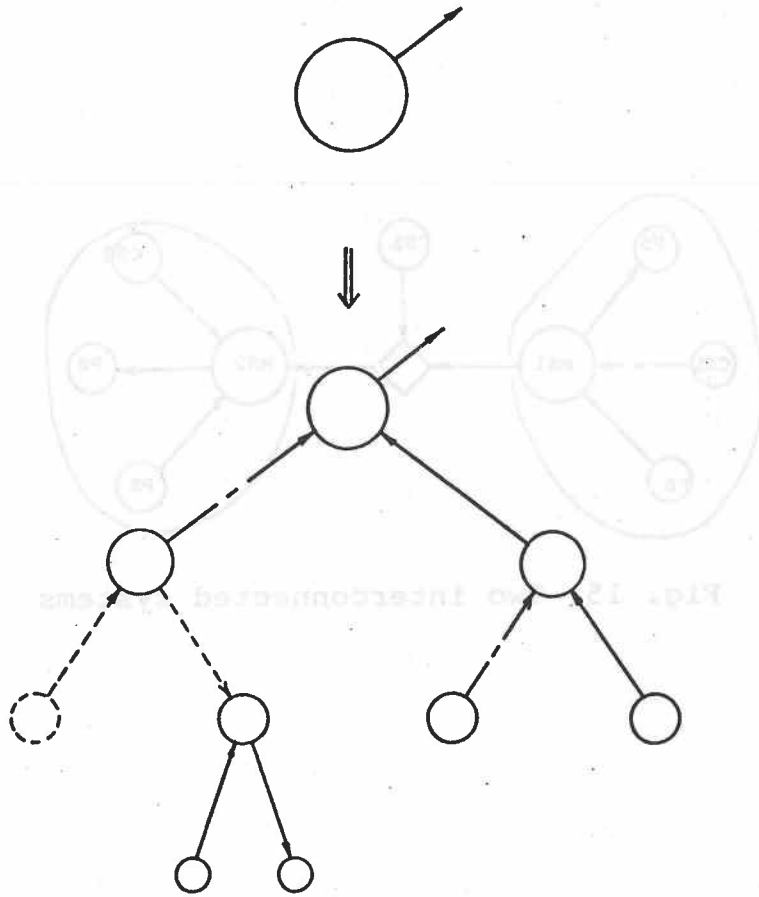


Fig. 13 Decomposition hierarchy.

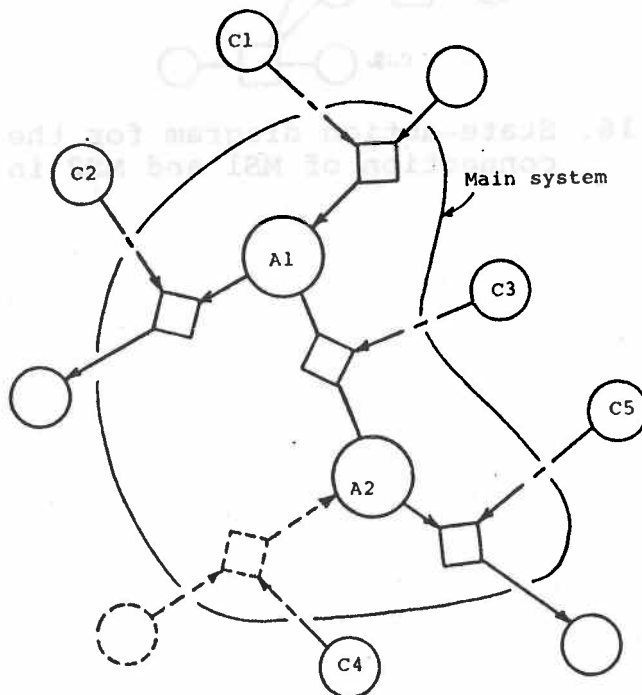


Fig. 14. Main system example.

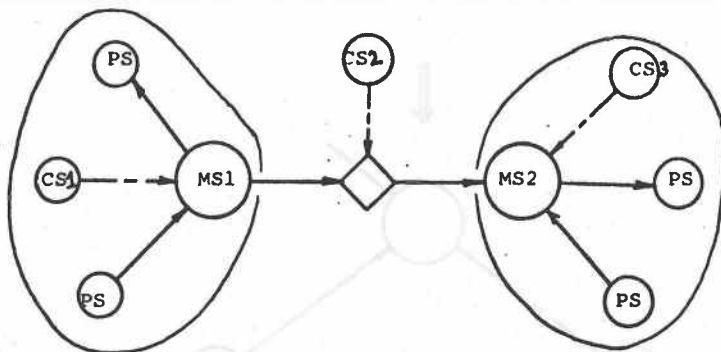


Fig. 15. Two interconnected systems

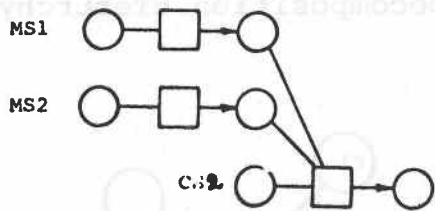


Fig. 16. State-action diagram for the inter-connection of MS1 and MS2 in fig. 15.

SYMBOLS:

COMPONENTS OR SUBSYSTEMS

AG Air/gas path

B Burner

BS Burner system

(B and subsystems)

D Drum

FP Feed pump

FPS Feedpump system

(FP and subsystems)

FWT Feed water tank

SP Steam flow paths

WFP Water flow paths

STATES

CE Content established

NR Not ready

O Operating

R Ready

S Stopped

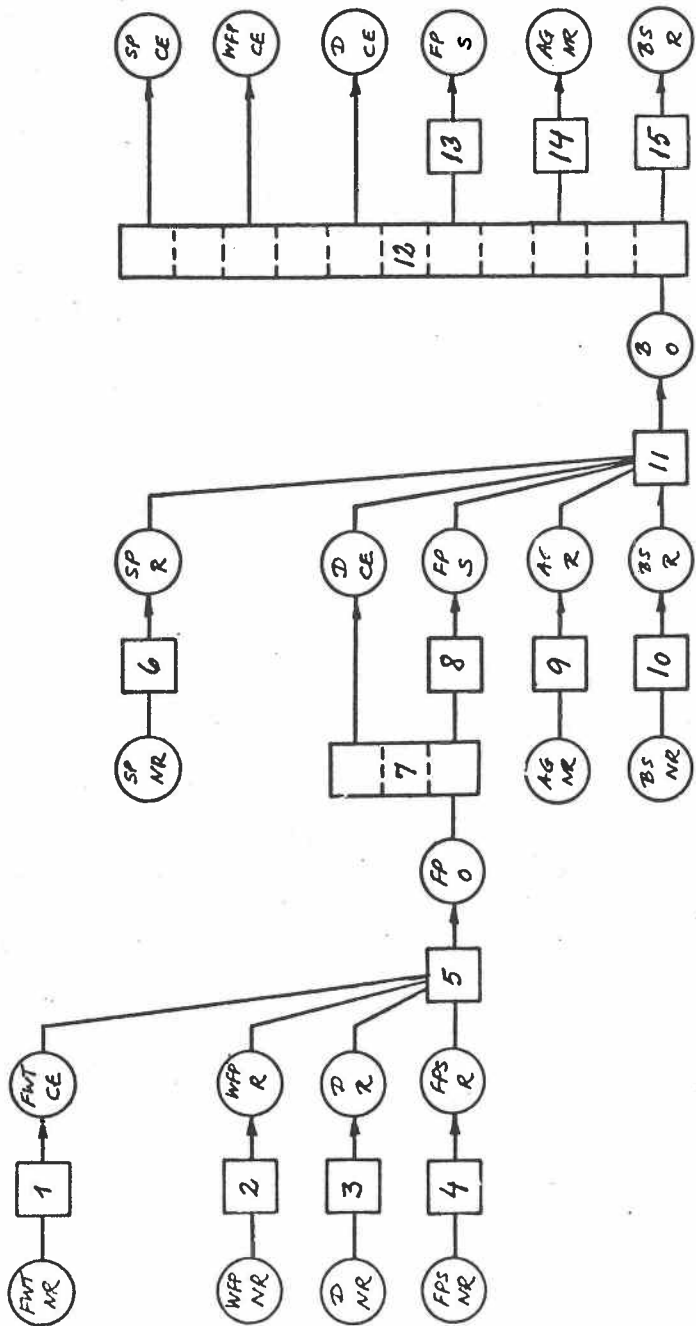


Fig. 17. State-action diagram for boiler startup.

T. Tamaoki, N. Naito, T. Tsunoda, M. Sato, A. Kameda
VERIFICATION TEST FOR ON-LINE DIAGNOSIS ALGORITHM BASED ON
NOISE ANALYSIS

IAEA/NPPCI Specialists' Meeting on
Procedures and Systems for Assisting an Operator During
Normal and Anomalous Nuclear Plant Operation Situations,
Munich, Federal Republic of Germany, 5-7 December 1979

Verification Test for On-Line Diagnosis Algorithm
based on Noise Analysis*

T. Tamaoki, N. Naito, T. Tsunoda
NAIG Research Laboratory,
Nippon Atomic Industry Group Co., Ltd.,
4-1, Ukishima-cho, Kawasaki-ku, Kawasaki-shi,
Kanagawa-ken, 210 Japan

M. Sato, A. Kameda
Advanced Reactor Engineering Department,
Toshiba Corporation,
25-5, 1-chome, Toranomon, Minato-ku,
Tokyo, 105 JAPAN

* This work was performed under contracts between
Power Reactor and Nuclear Fuel Development
Corporation and Toshiba Corporation.

Abstract

An on-line diagnosis algorithm was developed and its verification test was performed using a minicomputer. This algorithm identifies the plant state by analyzing various system noise patterns, such as power spectral densities, coherence functions etc., in three procedure steps. Each obtained noise pattern is examined by using the distances from its reference patterns prepared for various plant states. Then, the plant state is identified by synthesizing each result with an evaluation weight. This weight is determined automatically from the reference noise patterns prior to on-line diagnosis.

The test was performed with 50 MW(th) Steam Generator noise data recorded under various controller parameter values. The algorithm performance was evaluated based on a newly devised index.

The results obtained with one kind of weight showed the algorithm efficiency under the proper selection of noise patterns. Results for another kind of weight showed the robustness of the algorithm to this selection.

1. INTRODUCTION

Noise analysis is a highly efficient tool in the identification of reactor noise sources and the detection of plant abnormality. In order to develop a nuclear power plant diagnosis system based on noise analysis, the following tasks must be performed:

- (1) Reduce noise signals and clarify the relation between obtained noise patterns and plant operating states.
- (2) Judge whether an obtained noise pattern is normal or abnormal and identify the cause and degree of the abnormality if it was detected.

For item (1), many reports have been published on noise analysis for various operating reactors, which allowed much better understanding of noise patterns in FBR as well as LWR. Moreover, simulation diagnosis has been performed to develop a diagnosis system efficiently. On the contrary, for item (2), based on the relation between plant operating states and noise patterns, which was already learned, specialists on noise analysis have to judge whether the plant state is normal or abnormal by carefully observing the obtained noise patterns. It is, however, very difficult for them to identify the cause and degree of plant abnormality and subsequent consequences quickly, using a huge amount of noise patterns. For this reason, the authors have developed a diagnosis algorithm for an on-line computer.

Although several on-line diagnosis algorithms, based on noise analysis, have been reported, [1], [2] they treated only a detection problem to determine, with a power spectral density of neutron signal, whether the plant state has changed significantly from the normal state.

The algorithm proposed in this paper, however, treats not only the detection problem but the identification problem to determine the present plant state. The plant state is identified

by analyzing various noise patterns in forms of power spectral densities, coherence functions etc., with three statistical procedure steps.

The verification test for this algorithm was performed with recorded noise data for 50 MW(th) Steam Generator, situated at the O-arai Engineering Center of PNC.

2. ON-LINE DIAGNOSIS ALGORITHM BASED ON NOISE ANALYSIS

2.1 Basic procedure

A nuclear power plant contains various inherent noise sources. Process signals, excited by these noise sources, fluctuate through the plant response characteristics. Hence, these fluctuations contain information about the plant operating state. Noise analysis techniques can extract this information in the form of power spectral densities, coherence functions, correlation functions etc.. These noise analysis results show various patterns, according to the various plant operating states. If the relation between the noise patterns and the plant operating states were known, the present plant state can be identified by observing the obtained noise patterns (sample noise patterns).

An on-line diagnosis system, based on this concept, can be diagramed as in Fig. 1.

The reference noise patterns must be prepared beforehand in two ways. One way is on-line learning during the initial operating period. The other way is off-line learning, using a plant simulator to get the reference noise patterns under various abnormal states. In the latter case, the reference patterns can also be obtained by the theoretical calculations using the plant dynamic model. These reference noise patterns are stored with their identity labels for the plant operating states.

The discriminant system compares sample noise patterns with the reference noise patterns. If the sample noise patterns indicate a plant abnormality, this system gives such information as cause, degree and indicated counteractions to the operator through the display system.

To realize the above mentioned system, an algorithm to identify the plant state synthetically, using various kinds of noise analysis results, was developed as follows.

Figure 2 shows a flow diagram of the discriminant system based on the developed algorithm. The task of this system is performed by the following three procedure steps.

Step 1: This is the first step in the on-line diagnosis procedure. In this step, the most probable plant operating state is determined for each sample noise pattern by comparing with reference noise patterns.

Each noise pattern is described by a multidimensional vector,

whose components are selected parts of the noise analysis result. Then, the i 'th sample vector $X_i = [x_1, x_2, \dots, x_{n_i}]^T$ which belongs to the k 'th plant state should be positioned around the reference vector μ_{ik} in the n_i -dimensional space. This subspace is called the k 'th data class. The volume of the subspace constructed by these vectors is determined from their statistical nature. Thus the task in this step is to determine the subspace in which a certain sample vector is included. The distance between the sample vector and the reference vector can be used for this determination under the assumptions discussed in Section 2.2. The equation for this distance is

$$D_{ik} = (X_i - \mu_{ik})^T \Sigma_{ik}^{-1} (X_i - \mu_{ik}), \quad (1)$$

where Σ_{ik} means the covariance matrix for the i 'th sample vector included in the k 'th class. Superscript T denotes the transpose of a vector.

After distance D_{ik} is calculated for all classes, a certain class which minimizes D_{ik} is obtained. The discriminant system assumes that sample vector X_i is included in this class. This hypothesis is then tested, using the PDF (probability density function) for the distance. If the PDF for the sample vector was well approximated by the normal (Gaussian) distribution, D_{ik}^2 is a χ -square variate with n_i degrees of freedom. In this case, the hypothesis is adopted if $D_{ik}^2 \leq \chi^2(n_i, \epsilon_i)$, where ϵ_i denotes the given significance level. The value of $\chi^2(n_i, \epsilon_i)$ is obtained from the χ -square table. On the contrary, the hypothesis is abandoned if $D_{ik}^2 > \chi^2(n_i, \epsilon_i)$, and the system regards the sample vector to be included in the class which represents an unknown abnormal plant state. As the result of the above test, the system makes $b_{ik} = 1$, if the sample vector is regarded to belong to the k 'th class, or $b_{ik} = 0$, if otherwise. Thus, the discriminant matrix $B = \{b_{ik}\}$ is constructed finally.

Significance level ϵ_i is closely related to the false alarm rate. The value of ϵ_i should be determined by considering the system requirement for a low false alarm rate and the responsibility for quick abnormality detection.

The PDF for the sample vector will be discussed in Section 2.2.

Step 2: The most probable plant state is synthetically determined from the discriminant matrix in this step. The system examine the b_{ik} value for all sample vectors in each class. The simple summation, however, is meaningless since several sample vectors may show the same pattern at several different classes. Hence the quantity

$$g_k = \sum_{i=1}^m W_{ik} b_{ik} \quad (2)$$

was defined as the criterion function for the determination, where m denotes the number of vectors and W_{ik} is a weighting factor for each b_{ik} . The system calculates the value of g_k for

all classes. Then, the class which gives a maximum value of g_k is determined as the most probable plant state.

The weighting factor should be predetermined in Step 0.

Step 0: The quantities, $\mu_k = \{\mu_{ik}; i=1,2, \dots, m\}$, $\Sigma_k = \{\Sigma_{ik}; i=1, 2, \dots, m\}$ and W_{ik} should be prepared for the on-line diagnosis.

Reference vectors μ_k and covariance Σ_k are given to the discriminant system by learning. Weighting factor W_{ik} is determined using the values of μ_k and Σ_k in this step.

The distance from the k 'th class to the l 'th class can be written for the i 'th reference vector, as follows:

$$D_{ik}^2(l) = (\mu_{il} - \mu_{ik})^T \Sigma_{ik}^{-1} (\mu_{il} - \mu_{ik}). \quad (3)$$

Let k_0 , k_u and k_n denote the class of the normal plant state, the class of the unknown abnormal state and the l 'th class which minimizes $D_{ik}^2(l)$, respectively. Then, one weighting factor category is presented by

$$W_{ik} = \begin{cases} D_{ik_0}^2(k) / \sum_{j=1}^m D_{jk_0}^2(k) & \text{for } k \neq k_0 \text{ and } k \neq k_u \\ 1/m & \text{for } k = k_0 \text{ or } k = k_u. \end{cases} \quad (4)$$

Equation (4) means that the determination in Step 2 depends on such vectors that the pattern at class k is largely different from the pattern at class k_0 . This weighting factor category is called Category 1.

Another weighting factor category is presented by

$$W_{ik} = \begin{cases} P_{ik} / \sum_{j=1}^m P_{jk} & \text{for } k \neq k_u \\ 1/m & \text{for } k = k_u. \end{cases} \quad (5)$$

The quantity P_{ik} is given by

$$P_{ik} = \int_0^{D_{ik}^2(k_n)} p(\chi^2, n_i) d\chi^2, \quad (6)$$

where $p(\chi^2, n_i)$ denotes the PDF for the χ -square distribution with n_i degrees of freedom. The P_{ik} value approaches 1.0 for a large $D_{ik}^2(k_n)$. Thus, the weights approach the same value for such vectors that have large $D_{ik}^2(k_n)$ values. This weighting factor category is called Category 2. Category 2 is considered to be close to the evaluation by a skilled noise analyst.

Although some other W_{ik} categories could be easily presented, the verification test was conducted with the above two weight categories. Results will be shown in Section 4.

2.2 Statistical characteristics for sample noise patterns

Two basic assumptions in the authors' algorithm will be discussed in this section. They are concerned with the PDF and the covariance for the sample vectors.

PDF for sample vectors

The approach using Eq.(1) is efficient for sample vectors with symmetric PDF, especially with Gaussian PDF. For non-Gaussian cases, the discriminant threshold $\chi^2 (n_i, \epsilon_i)$ discussed in Step 1 should be modified, as discussed in Ref.[1].

If it was necessary to use a sample vector with a strongly skewed PDF, the original vector should be numerically transformed to a vector with a symmetric PDF. Consider two examples obtained by noise analysis in the frequency domain.

The PDF for the APSD (Auto-power Spectral Density), obtained from N blocks of time-series data by using the FFT (Fast Fourier Transform) technique, is given in Ref.[3] as follows:

$$p(a) = \begin{cases} N^N \cdot a^{N-1} \cdot \exp(-N \cdot a) / \Gamma(N), & \text{for } a \geq 0 \\ 0, & \text{for } a < 0, \end{cases} \quad (7)$$

where a denotes the value of the APSD normalized with its population mean, and $\Gamma(N)$ denotes the Gamma function. This original PDF is strongly skewed and well approximated by the log-normal PDF[2]. Thus, Eq.(1) can be used for the logarithm of the APSD. The PDF for the transformed APSD is described by the Gaussian PDF, whose mean value μ and variance σ^2 are respectively given by

$$\mu = \ln \frac{\alpha}{\sqrt{1 + 1/N}} \quad (8)$$

and

$$\sigma^2 = \ln(1 + 1/N), \quad (9)$$

where α denotes the population mean for the original APSD.

The PDF for the CF (Coherence Function) is also given in Ref.[2], as follows:

$$p(z) = \frac{2(1-\mu^2)^N}{\Gamma(N)\Gamma(N-1)} z(1-z^2)^{N-2} \sum_{j=0}^{\infty} \frac{\mu^{2j} \Gamma^2(N+j)}{\Gamma^2(j+1)} z^{2j}, \text{ for } 0 < z < 1, \quad (10)$$

where Z denotes the CF value and its population mean is denoted by μ . Although the form of this PDF varies with the values of μ and N, its skewness is rather small. Thus, the original PDF can be approximated by the Gaussian PDF, which has the same mean and variance values derived from Eq.(10). Variance σ^2 can be obtained from the approximate equation for normalized standard deviation s, as follows:

$$\begin{cases} s = \frac{1}{\mu\sqrt{N}}, & \text{for } \mu < 0.1 \\ \log(s) = -0.495 \log N - 4.647\mu^3 + 6.951 \mu^2 \\ \quad - 4.754\mu^2 + 3.394, & \text{for } \mu \geq 0.1, \end{cases} \quad (11)$$

where $s = 100 \sigma/\mu$.

Covariance for sample vectors

Strictly speaking, Eq.(1) is not an Euclidean distance measure, but a probabilistic one, termed the Mahalanobis distance. For example, covariability exists between the values of an APSD at two neighboring frequency points, owing to the window used in noise analysis[4]. If a sample vector is constructed from these neighboring frequency points, the cross term will appear in covariance matrix $\{i,k\}$. Thus, in general, it is necessary to orthogonalize the vector component axes, as shown in Ref.[1].

In this paper, however, the covariance matrix was assumed to be diagonal and each diagonal element was obtained theoretically by using Eq.(9), etc.. The reason will be discussed in Section 3.2.

3. NOISE PATTERNS FOR 50MW(th) STEAM GENERATOR

3.1 Noise measurement and data reduction

As verification for the on-line diagnosis algorithm, 50MW(th) Steam Generator noise data were measured and analyzed under various controller parameter values. Figure 3 shows the schematic diagram of 50 MW(th) Steam Generator control and instrumentation. In this experiment, control parameters for the differential pressure control system (PDIC-317) and the feedwater control system (FICA-301) were changed.

With the FICA-301, feedwater control valve position is controlled. With the PDIC-317, feedwater pump speed is controlled.

Experimental conditions, in which noise measurements were performed, are listed in TABLE I. Transfer function for these two controllers is given by $\frac{100}{P} (1 + \frac{1}{I \cdot S})$. Fourteen signals, from sensors marked by an asterisk in Fig. 3, were recorded for 60 minutes by an analog tape recorder under various P and I values.

The recorded signals were analyzed with a system which is composed of an A-D converter, a minicomputer (TOSBAC -40 C) and a CRT display with a hardcopy equipment. A blockdiagram of this system is shown in Fig. 4. As the result of analysis using FFT technique, APSDs, CFs and much other information were obtained. Figure 5 shows example APSDs obtained for feedwater flow rate under various plant states. In this data reduction, noise component in the 0.02 to 5 Hz frequency range was analyzed and the results for 256 frequency points were obtained.

It is found, from Fig. 5, that the fluctuation in feedwater flow rate is not so stable under plant states 1 ~ 3, because APSDs in low frequency range show large magnitude. Thus, plant state 6 was treated as a normal state in the verification test, though the PDIC-317 was under manual operation.

Among a great deal of reduced data, APSDs for eight signals and CFs between these signals were selected and prepared for the verification test, because these noise patterns, shown in TABLE II, are very sensitive to the change in plant operating state. Selected number of noise patterns, marked by an asterisk in TABLE II, were used in the verification test.

3.2 Reference vector learning

For calculating distance D_{ik} , reference vector μ_{ik} and covariance matrix Σ_{ik} must be determined.

In case of APSDs, the reference vector is given by

$$\mu_{ik} = \frac{1}{M} \sum_{j=1}^M y_{ik}^j, \quad (12)$$

where M denotes the trial number and y_{ik}^j denotes the k 'th class vector obtained at j 'th trial. Each vector is constructed with a logarithm of APSD, which is reduced from N blocks of data. The value of μ_{ik} approaches the population mean under a large M value.

On the contrary, in case of CFs, it can be shown by Eq.(10) that μ_{ik} depends on N and, thus, does not approach the population mean, even under a large M . For the sake of minimizing this effect, reference vectors were obtained with only one trial in which the 60 minutes (68 blocks of) data were analyzed by FFT. The sample vectors for the verification test were obtained from the 15 minutes (17 blocks) of data.

Although the covariance matrix is, in general, given by

$$\Sigma_{ik} = \frac{1}{M} \sum_{j=1}^M (y_{ik}^j - \mu_{ik})(y_{ik}^j - \mu_{ik})^T, \quad (13)$$

it was determined theoretically, as described in Section 2.2, for this reason.

4. VERIFICATION TEST

4.1 Performance index f_c

An off-line verification test for the discriminant system was performed using the minicomputer TOSBAC-40C under various conditions. Each test condition was different in regard to the number of vectors or vector components, as shown in TABLE III. Thirteen samples, obtained from seven plant states, were diagnosed by the discriminant system with two different weighting factor categories under each test condition.

To evaluate the proposed algorithm performance under these test results, a performance index f_c was introduced. Let g_t denote the value of g_k for the true data class in which the sample is included, and let g_m and g_s denote the maximum and second values of g_k , respectively. The performance index is given by

$$f_c = \begin{cases} \frac{g_t}{g_s+C_0} (g_t-g_s) , & \text{for } g_t = g_m \\ \frac{g_m}{g_t+C_0} (g_t-g_m) , & \text{for } g_t < g_m. \end{cases} \quad (12)$$

If the discriminant result was false, i.e. $g_t < g_m$, the f_c value becomes negative. The f_c value ranges from $-C_0$ to $+C_0$, and increases monotonically with the g_t value. In this paper, 1.0 was assigned to C_0 . Figure 6 shows f_c examples.

4.2 Test results

It can be seen from Fig.4 that the noise pattern in the low frequency range is useful for diagnosis. Hence, all vectors were constructed with values between 0.0195 Hz to the same frequency with 0.0195-Hz resolution. For the significance level $\epsilon_1, 1\%$ was given to all vectors.

Test results obtained with two weighting factor categories are shown in TABLE IV. It is shown that the discriminant system with Category 2 of the weighting factor diagnosed all samples correctly under all test conditions, except TC-3, in which only four vectors were used. The average values of f_c with Category 1 and Category 2 through all test conditions are 0.156 and 0.178, respectively. This difference is mainly due to the results for TC-4 and TC-5, and is evident especially in the results for samples No. 2 ~ 7. This can be said to hold true also for other test conditions, except TC-3, and can be interpreted as follows: All samples No.2 ~ 7 were obtained under plant state 2 or 3 as shown in TABLE IV. Some vectors used in the tests show quite different patterns under these plant states from the normal plant state 6. On the other hand, they show quite similar patterns under these two plant states, as shown in Fig. 4. For these vectors, weighting factors W_{i2} and W_{i3} for Category 1 show very large values and those for Category 2 show rather small values. Thus, the results for samples No.2 ~ 7 obtained with Category 1 weighting factor, are largely affected by a faulty construction of the discriminant matrix in Step 1 of the procedure. This effect is evident in TC-4 and TC-5, because many noise pattern at high frequency range under plant states 2 and 3 are very close to each other.

It can be said from the above discussion, that the discriminant system with Category 1 weight is apt to be affected by the selection of vector components, and that the system with Category 2 weight is robust to that selection, on the contrary. Thus, it is preferred to use Category 2 of the weighting factor.

5. CONCLUSIONS

An on-line diagnosis algorithm, based on noise analysis was developed and its verification test was performed with the recorded noise data of 50 MW(th) Steam Generator. This algorithm identifies the plant state by analyzing various sample noise patterns in three procedure steps. Each sample noise pattern is examined by using the distances from the reference noise patterns. The plant state is determined by synthesizing each result with the evaluation weight which is determined automatically from the reference noise patterns.

The algorithm with two weighting factor categories were tested and evaluated with a newly devised performance index. The results obtained with one category of weight show the efficiency of the algorithm under the proper selection of noise patterns. Those with another category of weight show robustness to this selection.

References

- [1] K.R. PIETY and J.C. ROBINSON, "An On-Line Reactor Surveillance Algorithm Based on Multivariate Analysis of Noise", Nucl. Sci. Eng. 59 (1976) 369.
- [2] M. IZUMI and H. IIDA, "Application of On-Line Digital Noise Analysis to Reactor Diagnosis in JMTR", J. Nucl. Sci. Technol. 10 (1973) 227.
- [3] N.R. GOODMAN, "On the Joint Estimation of the Spectra, Cosppectrum and Quadrature Spectrum of a Two-Dimensional Stationary Gaussian Process", Scientific Paper No. 10, Eng. Stat. Lab., N.Y. Univ. (1957) (Ph.D. Thesis, Princeton Univ.)
- [4] R.B. BLACKMAN and J.W. TUKEY, "The Measurement of Power Spectra from the Point of View of Communications Engineering", Bell System Tech. J., Jan. and Mar. (1958)

List of Figures

- Fig. 1 On-line diagnosis system based on noise analysis
- Fig. 2 Discriminant system flow diagram
- Fig. 3 50 MW(th) Steam Generator control and instrumentation system configuration

Fig. 4 Hardware configuration of noise analysis system

Fig. 5 APSDs of feedwater flow rate

Fig. 6 Examples of performance index, f_c

Plant state	Operating mode	Operating mode	Operating mode	Operating mode	Operating mode
1	Auto	Auto	Auto	Auto	Auto
2	Auto	Auto	Auto	Auto	Auto
3	Auto	Auto	Auto	Auto	Auto
4	Manual	Manual	Manual	Manual	Manual
5	Manual	Manual	Manual	Manual	Manual
6	Manual	Manual	Manual	Manual	Manual
7	Manual	Manual	Manual	Manual	Manual

Controller transfer function is given by $\frac{100}{s} (1 + \frac{1}{1.5s})$

TABLE 1 EXPERIMENTAL CONDITIONS

Plant state No	PDIC-317			FICA-301		
	Operating mode	P (%)	I (min)	Operating mode	P (%)	I (min)
1	Auto	300	2.0	Remote	150	1.0
2	Auto	350	2.0	Remote	150	1.0
3	Auto	400	2.0	Remote	150	1.0
4	Manual	—	—	Remote	150	0.2
5	Manual	—	—	Remote	50	2.0
6	Manual	—	—	Remote	150	1.0
7	Manual	—	—	Remote	150	0.5

Controller transfer function is given by $\frac{100}{P} (1 + \frac{1}{I \cdot s})$.

TABLE II NOISE PATTERNS USED FOR VERIFICATION TEST

No.	Noise pattern	Case		
		1	2	3
1	APSD of feedwater flow rate	*	*	
2	APSD of main steam flow rate	*	*	
3	APSD of feedwater pump speed	*	*	*
4	APSD of main steam pressure	*	*	
5	APSD of feedwater pressure	*	*	*
6	APSD of evaporator differential pressure	*		
7	APSD of superheater differential pressure	*		
8	APSD of evaporator outlet steam temperature	*	*	*
9	CF between main steam flow rate and main steam pressure	*	*	
10	CF between feedwater flow rate and main steam flow rate	*	*	
11	CF between feedwater flow rate and feedwater pressure	*	*	*
12	CF between feedwater pump speed and feedwater flow rate	*	*	
13	CF between feedwater pump speed and feedwater pressure	*	*	
14	CF between feedwater pressure and evaporator differential pressure	*	*	
15	CF between evaporator differential pressure and superheater differential pressure	*	*	
16	CF between superheater differential pressure and main steam pressure	*	*	

TABLE III VERIFICATION TEST CONDITIONS

Test condition No	Number of vectors (Case in TABLE II)	Number of vector components
TC-1	16 (Case 1)	10
TC-2	10 (Case 2)	10
TC-3	4 (Case 3)	10
TC-4	10 (Case 2)	20
TC-5	10 (Case 2)	30

TABLE IV f_c VALUES OBTAINED WITH TWO WEIGHTING FACTOR CATEGORIES

No.	Sample True class	TC-1		TC-2		TC-3		TC-4		TC-5	
		Category1	Category2	Category1	Category2	Category1	Category2	Category1	Category2	Category1	Category2
1	1	0.643	0.290	0.566	0.218	0.244	0.100	0.563	0.359	0.315	0.187
2	2	0.111	0.138	0.049	0.060	-0.989	-0.563	0.063	0.085	0.255	0.269
3	2	0.111	0.138	0.049	0.060	-0.989	-0.563	0.063	0.085	0.255	0.269
4	3	0.333	0.104	0.584	0.392	0.193	0.050	0.089	0.227	0.083	0.200
5	3	0.173	0.197	0.148	0.340	1.000	1.000	0.136	0.400	0.133	0.405
6	3	0.284	0.578	0.199	0.500	0.866	0.420	0.180	0.608	0.176	0.532
7	3	0.071	0.142	0.097	0.268	0.961	0.505	0.175	0.480	0.055	0.244
8	4	0.127	0.161	0.066	0.027	-0.044	-0.024	0.071	0.043	0.195	0.232
9	4	0.060	0.062	0.113	0.136	0.012	0.080	0.102	0.151	0.081	0.132
10	4	0.084	0.112	0.094	0.156	-0.009	-0.060	0.080	0.069	0.069	0.066
11	5	0.412	0.283	0.407	0.275	0.218	0.139	0.086	0.006	0.036	0.052
12	6	0.035	0.107	-0.005	0.044	0.109	0.107	-0.019	0.041	0.212	0.098
13	7	0.096	0.124	0.007	0.003	0.066	0.083	0.104	0.112	0.059	0.038
Average f_c value		0.195	0.187	0.183	0.191	0.126	0.098	0.130	0.205	0.148	0.210

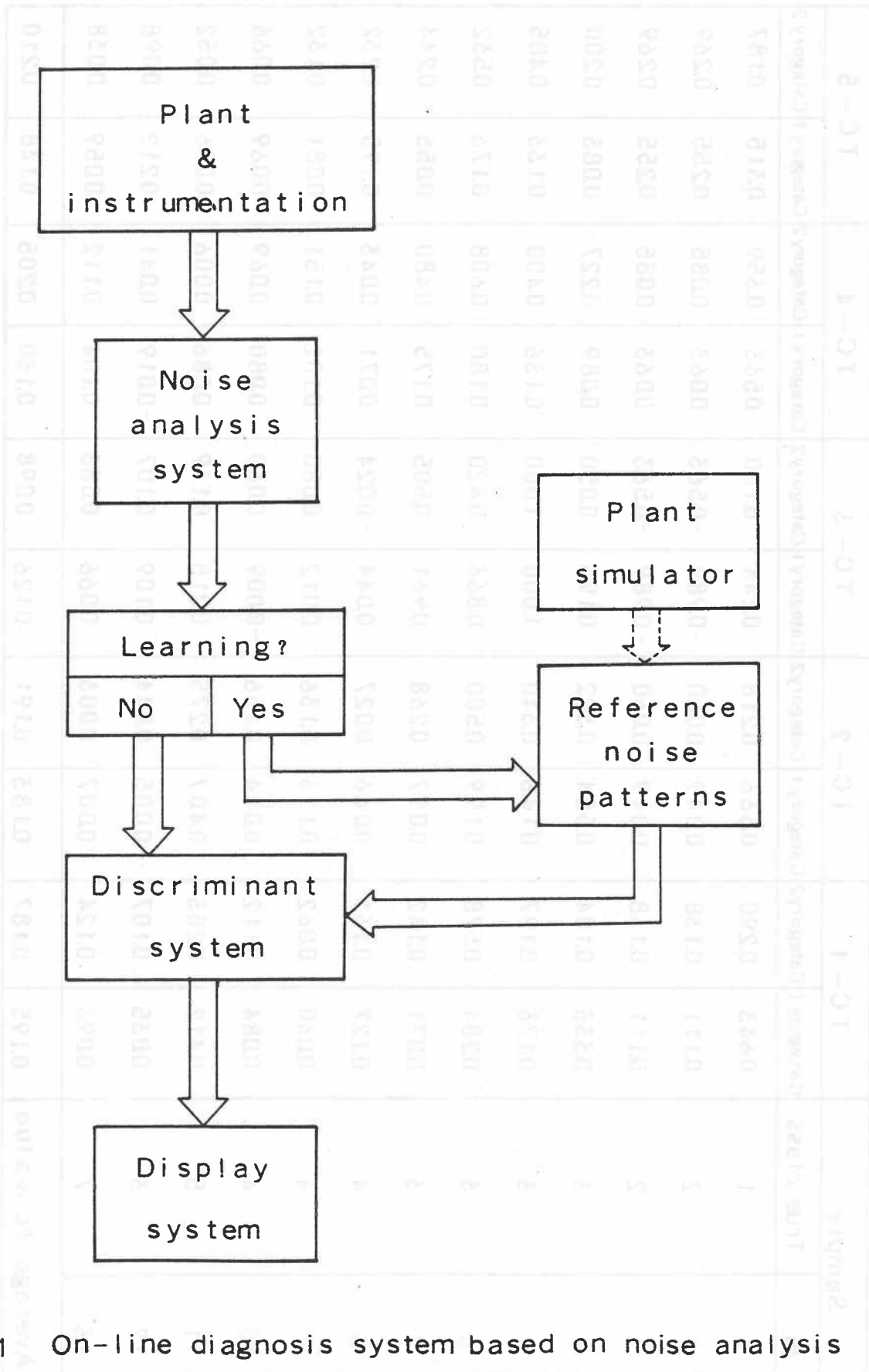


Fig. 1 On-line diagnosis system based on noise analysis

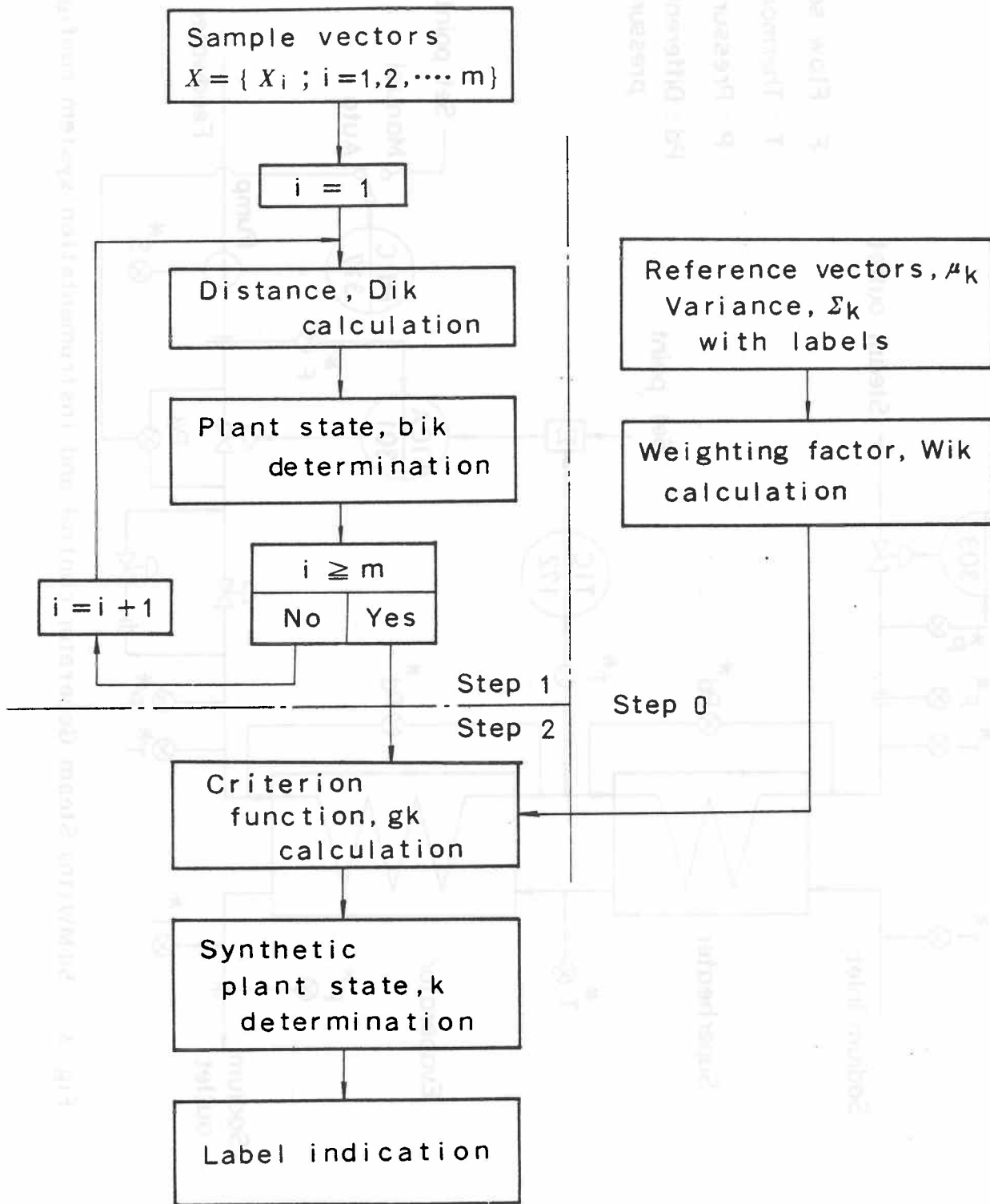


Fig. 2 Discriminant system flow diagram

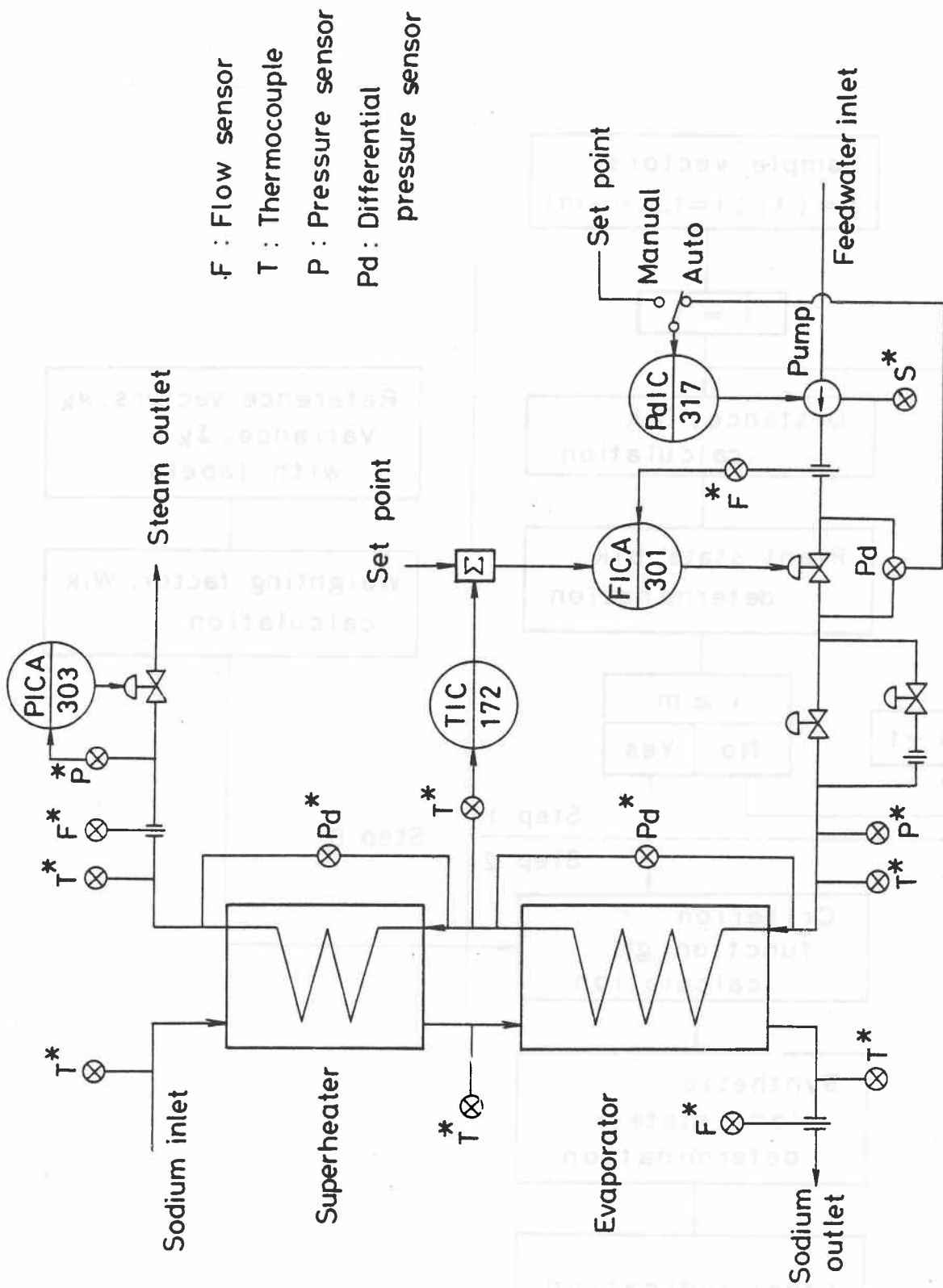


Fig. 3 50 MW(th) Steam Generator control and instrumentation system configuration

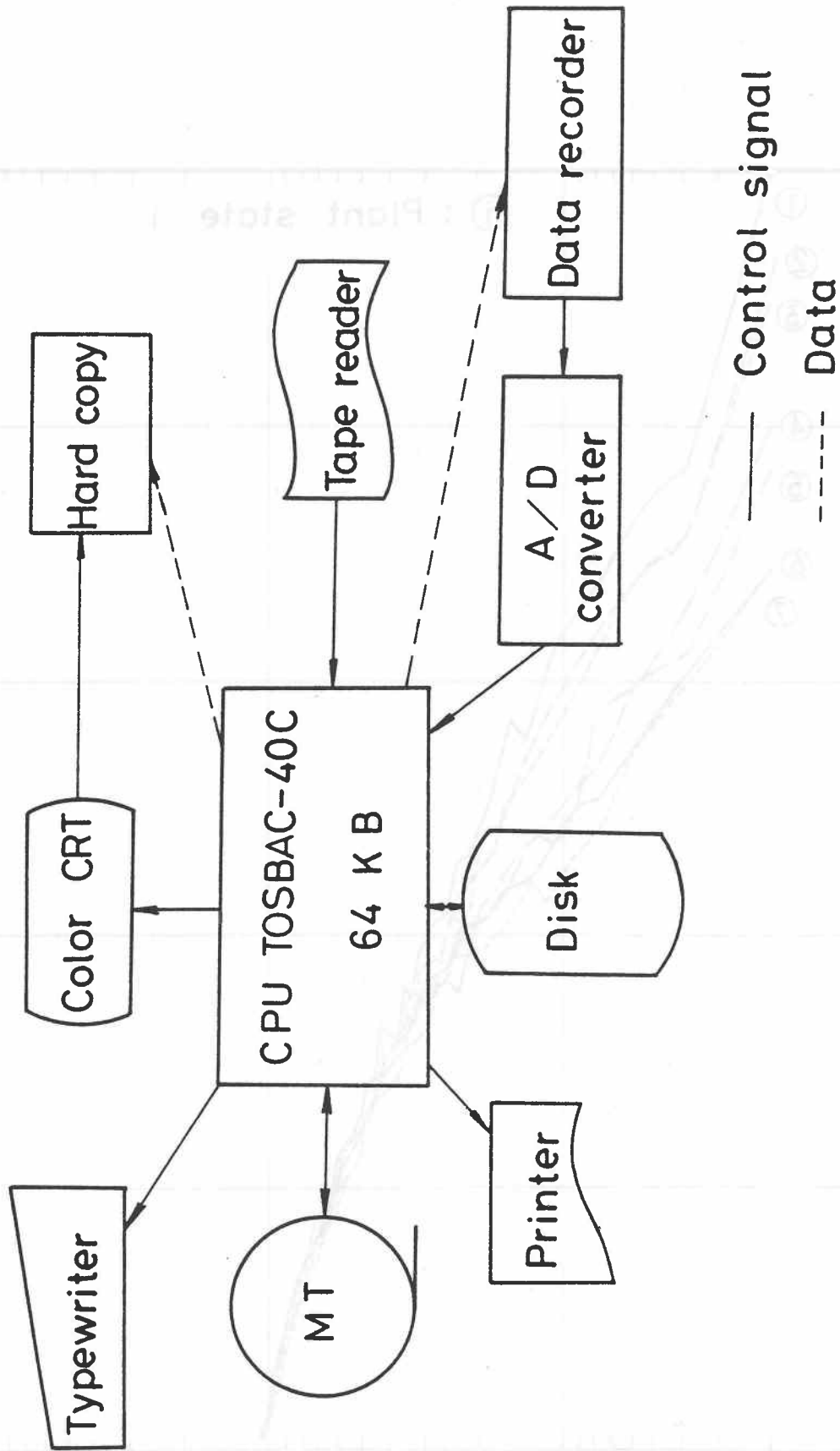


Fig. 4 Hardware configuration of noise analysis system

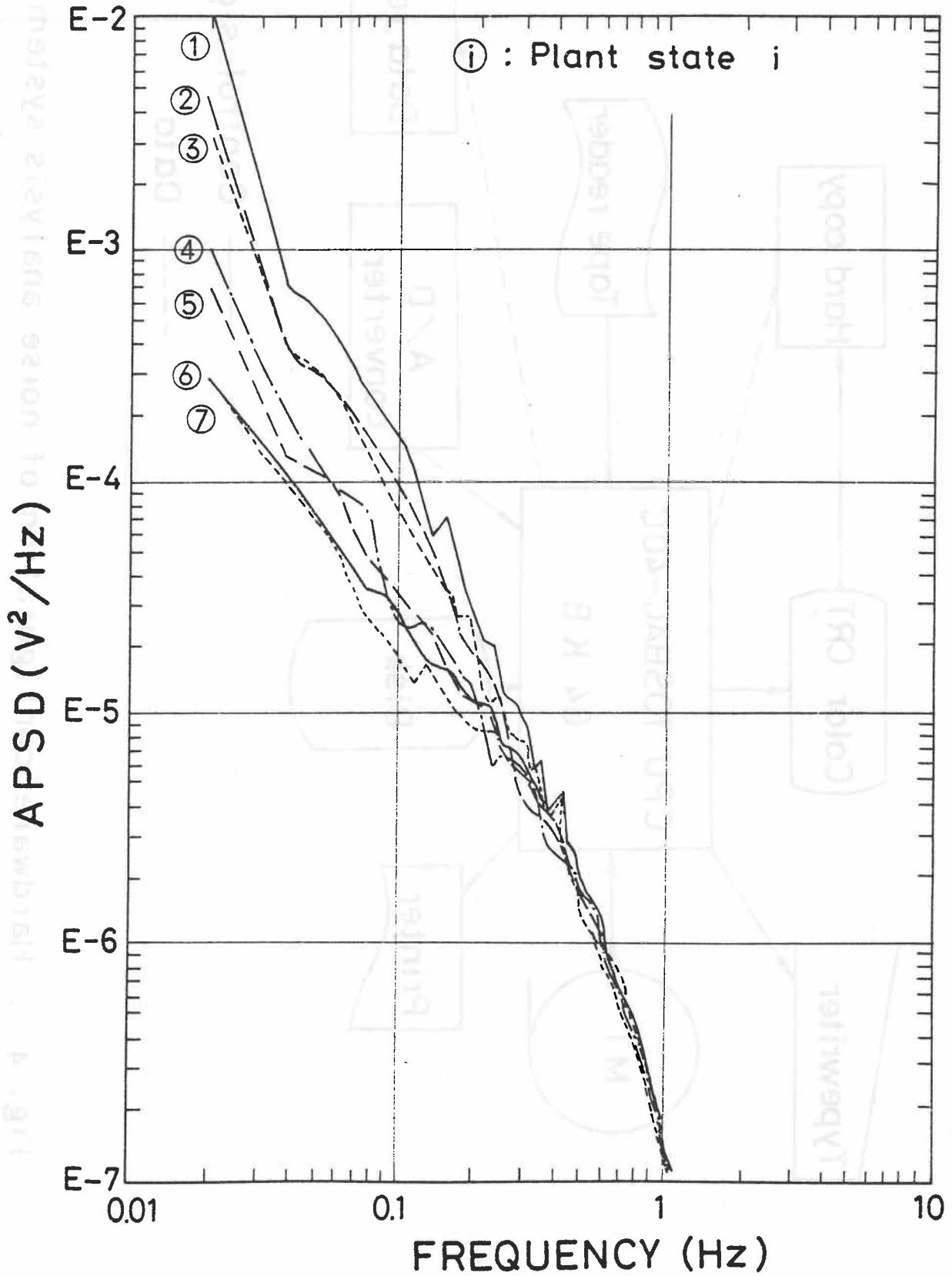


Fig. 5 APSDs of feedwater flow rate

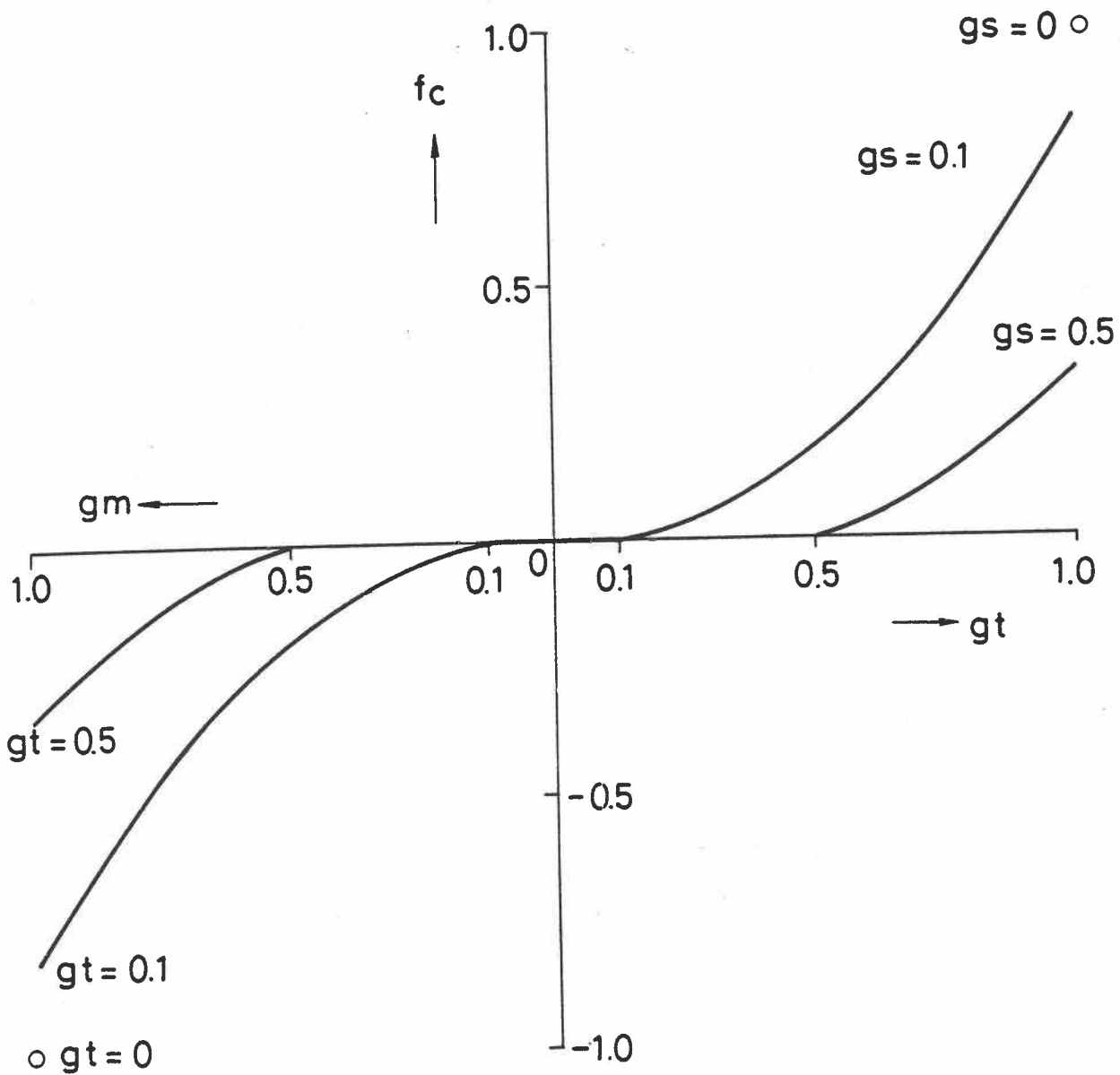


Fig. 6 Examples of performance index, f_c

R. Avenhaus, G. Spannagel

ANALYSIS OF PROCESS SIGNALS IN NUCLEAR INSTALLATIONS

ANALYSIS OF PROCESS SIGNALS IN NUCLEAR INSTALLATIONS

R. Avenhaus and G. Spannagel

Kernforschungszentrum Karlsruhe GmbH
Institut für Datenverarbeitung in der Technik
Postfach 3640, D-7500 Karlsruhe
Federal Republic of Germany

Paper to be presented at the
IAEA-NPPCI Specialists meeting on 'Procedure and systems for
assisting an operator during normal and anomalous nuclear power
plant operation situations', Munich, December 5-7, 1979

Abstract

In the framework of the 'Project of Reprocessing and Waste Treatment' of the Karlsruhe Nuclear Research Center, some time ago an activity has been initiated, the aim of which is to detect in time disturbances of production processes of nuclear installations with the help of process-signal analysis.

In this paper, the present state of this activity is described. Firstly, the basic approach will be discussed: by means of appropriate process models it is demonstrated which behaviour of the process will lead to which signals; vice versa, the investigations of these signals by decision theoretical methods will provide information on possible disturbances of the process. Secondly, the influence of process variations on the decision procedure will be discussed in some detail.

Implementation of this procedure in the GWK reprocessing plant, Karlsruhe, is underway.

1. Introduction

The control of complex processes demands for careful observation as well as comprehensive plant experience. Especially for the large German facility scheduled for the reprocessing of spent nuclear fuel these requirements will become a prerequisite. Therefore, it seemed to be meaningful to study methods and to propose tools which possibly support these objectives, using the GWK reprocessing plant for demonstration. Of course, besides tackling safety requirements these studies pursue an increase of the availability of the facility.

As to similar demands related to nuclear power plants considerable effort has been spent for a long time. For example, the Halden Program /1/, /2/ represents a well known investigation in this direction. However, compared with the conditions encountered at reactor stations the process behaviour at a reprocessing facility is quite different. Just for illustration it might be mentioned that reprocessing is essentially related to chemical procedures which, in case of anomalous behaviour, leave more time for counteraction compared to a similar situation at a nuclear reactor.

This investigation was confined to the anomalous process behaviour induced by hydraulic disturbances in the so-called '2. uranium cycle'; it should be pointed out that this analysis might be applied in general.

2. Anomalous hydraulic states in the 2. uranium cycle of the GWK reprocessing plant

As demonstrated in Figure 1 the 2. uranium cycle represents an essential part of that process branch responsible for the purification of the uranium product. A more detailed description of this cycle displays Figure 2: In the mixer-settler '2D' the uranium is transferred from the 2DF-stream (aqueous solution) to the 2DX-stream (organic solution); the fission products remain in the stream while entering the container '42.01.1/2' as the 2DW-stream. In the mixer-settler '2E' the uranium is transferred back into the aqueous solution (2EU-stream). As indicated, the fluids are usually transferred by airlifts, for example the 2DF-stream is transferred from the container '41.11' to the mixer-settler '2D' through the airlifts A113 and A131.

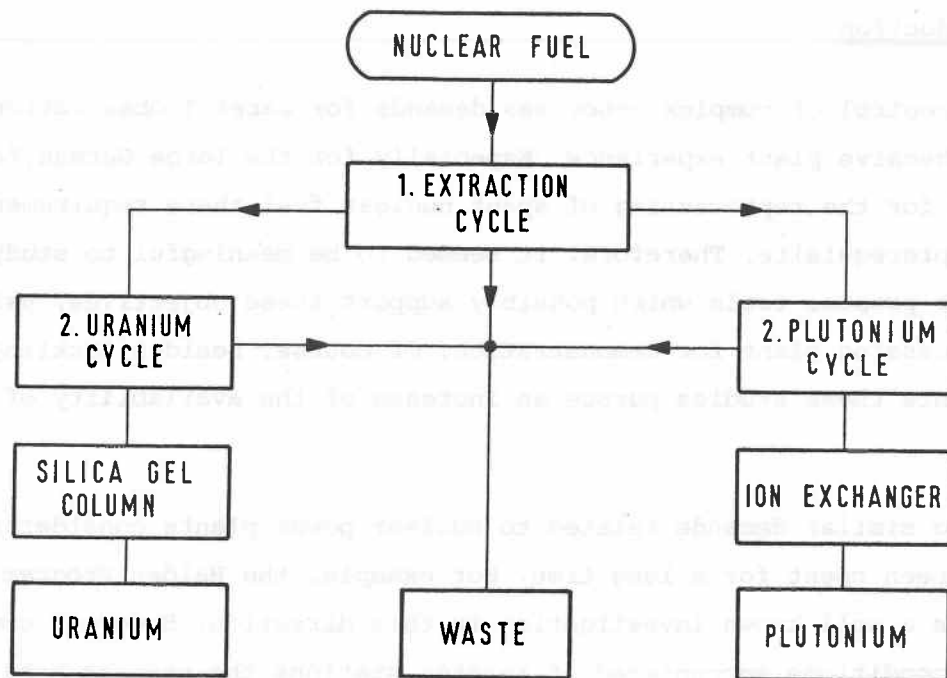


Fig. 1: Main process units of the WAK reprocessing plant

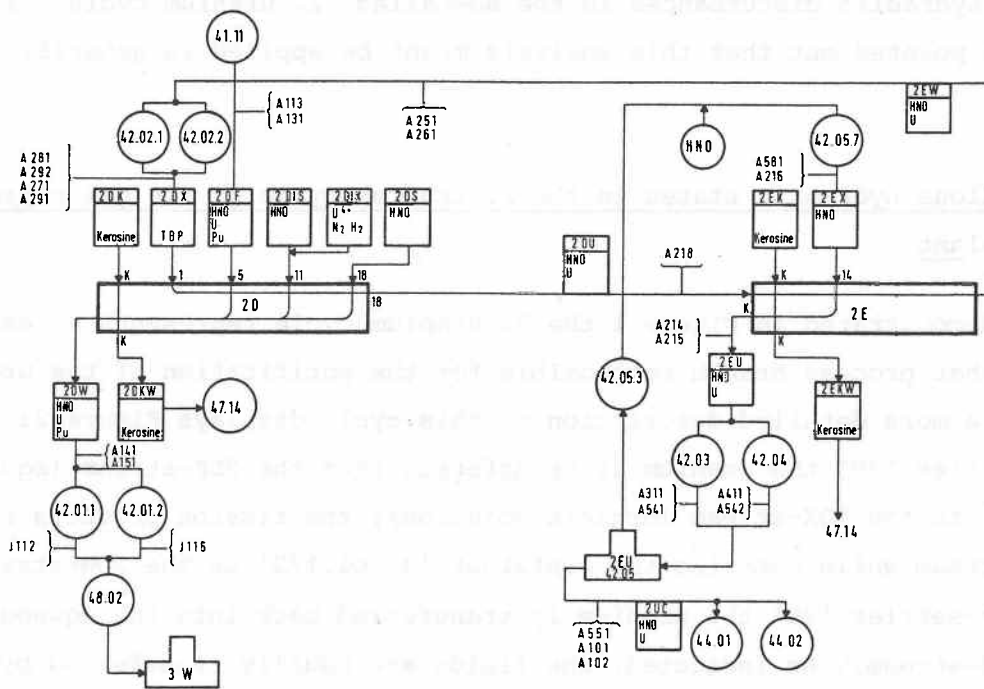


Fig. 2: The 2. uranium cycle of the WAK reprocessing plant

To control the liquid transfers, the change in terms of time of the container filling levels - recorded by dip tubes - is mainly used. In certain pipes the liquid flow can be measured directly; furthermore, the air flow of the airlifts and the level between the aqueous and organic solutions in the mixer-settlers can be observed.

The process state illustrated in Figure 3 will serve as an example for the mathematical analysis: If the transfer of the 2DW-stream is disturbed, the liquid level in the container 42.01.1/2 will vary less than it should. Furthermore, the separating layer in the mixer-settler '2D' will be increased until the level is reached of the point where the 2DK-stream leaves the mixer-settler. Then, together with the 2DKW-stream, that part of the DW-stream will also leave the mixer-settler, which cannot enter the container 42.01.1 because of the disturbance. The consequence is that the variation of the liquid level in the container 47.14 is greater than it should be.

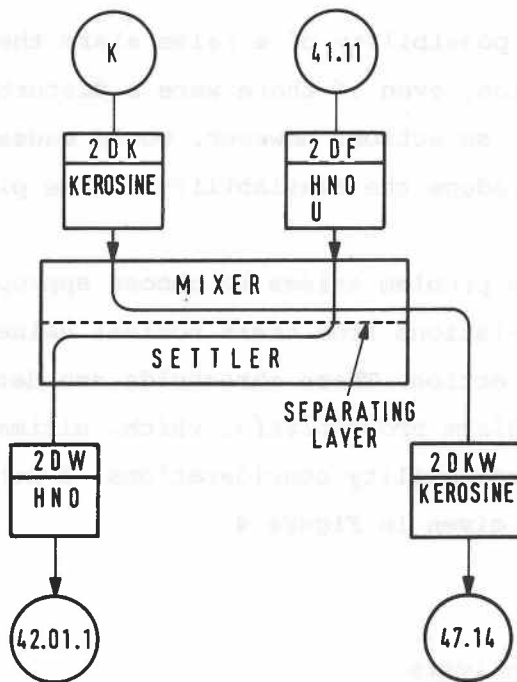


Fig. 3: Process section of the 2. uranium cycle used for mathematical analysis

Due to the restricted measurement devices available at the time being, three types of information can be used to diagnose disturbances: the varia-

tions of the liquid levels in the containers 42.01.1 and 47.14, and the position of the separating layer - the latter will be an indication of the beginning of a disturbance, expressed by a steadily increasing change from its regular position.

Due to technical circumstances this disturbance may have three causes: either a wrong adjustment of the air pressure, which influences the flow rate of the 2DW-stream, or a blocking of either the outlet of the mixer-settler '2D' or of the airlift 141/151.

If the operator in the Central Control Room recognizes that the signals deviate from their nominal values, and he, consequently, has to decide whether or not he shall take an action, he must take into account two aspects:

- The signals could deviate from their nominal values just because of measurement errors or process fluctuations not involving difficulties; thus, a shutdown would be false ('error of the first kind') and reduce the availability of the plant.
- Because of this possibility of a false alarm the operator could hesitate and take no action, even if there were a disturbance ('error of the second kind'); too late an action, however, would cause major technical difficulties and again reduce the availability of the plant.

Therefore, the problem arises to choose appropriate *significance thresholds* for signal deviations from their nominal values, above which the operator has to take an action. These thresholds are determined by the choice of appropriate *false alarm probabilities* which, ultimately, must be determined with the help of availability considerations. A schematical representation of these relations is given in Figure 4.

3. Mathematical Analysis

The following presentation of the mathematical analysis has to be relatively short; the interested reader will find further details in /3/.

Let us make the following assumptions:

- i) The 2DF-stream has a fixed value and must not be checked at all.

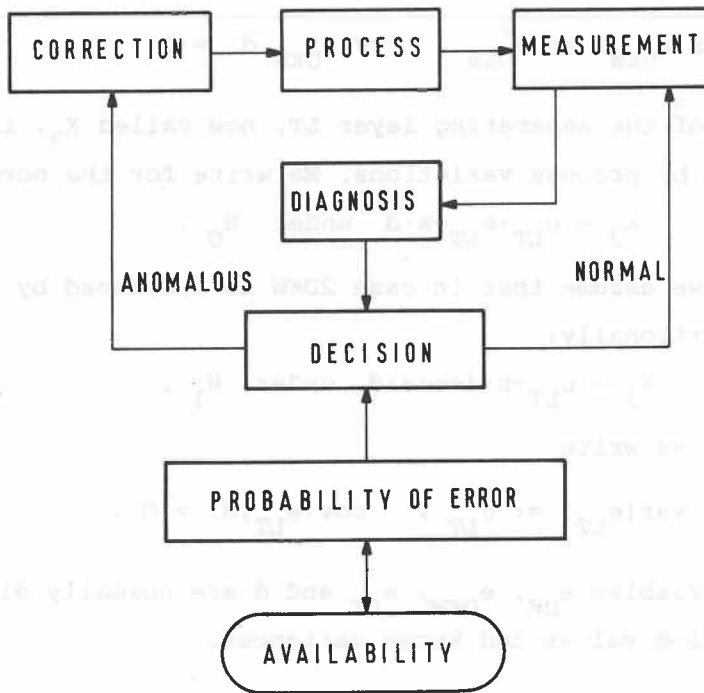


Fig. 4: Procedural model for the early detection of anomalous process states

- ii) The 2DW-stream can be disturbed, it can, however, not be checked directly; a decrease of 2DW leads to an increase of 2DKW by the value Δ .
- iii) The 2DK-stream now called X_1 , is subject to process variations which are, however, not considered to be disturbances; we write

$$X_1 := 2DK = \mu_{DK} + e_{DK} + d$$

where μ_{DK} is the nominal value, e_{DK} the measurement error and d the process variation, furthermore

$$\text{var}(e_{DK}) =: \sigma_{DK}^2, \quad \text{var}(d) =: \sigma_P^2, \quad \text{cov}(e_{DK}, d) = 0.$$

- iv) A process variation of 2DK influences directly 2DKW, now called X_2 , we write for the normal state (*null hypothesis* H_0),

$$X_2 := 2DKW = \mu_{DKW} + e_{DKW} + d \text{ under } H_0.$$

A decrease of the true value of 2DW by the value Δ leads to an increase of the true value of 2DKW by the same value Δ (*alternative hypothesis* H_1)

$$X_2 := 2DKW = \mu_{DKW} + \Delta + e_{DKW} + d \text{ under } H_1.$$

In both cases we write

$$\text{var}(e_{\text{DKW}}) =: \sigma_{\text{DKW}}^2, \quad \text{cov}(e_{\text{DKW}}, d) = 0.$$

- v) The position of the separating layer LT, now called X_3 , is proportionally influenced by process variations. We write for the normal state

$$X_3 = \mu_{\text{LT}} + e_{\text{LT}} + a \cdot d \quad \text{under } H_0.$$

Furthermore, we assume that in case 2DKW is increased by Δ , X_3 increases proportionally:

$$X_3 = \mu_{\text{LT}} + b \cdot \Delta + e_{\text{LT}} + a \cdot d \quad \text{under } H_1.$$

In both cases we write

$$\text{var}(e_{\text{LT}}) =: \sigma_{\text{LT}}^2, \quad \text{cov}(e_{\text{LT}}, d) = 0.$$

- vi) The random variables e_{DK} , e_{DKW} , e_{LT} and d are normally distributed with zero expectation values and known variances.

From these assumptions we immediately get the following expressions for the joint densities $f_i(\underline{x})$, $i=0,1$, of the random vector $\underline{X}' = (X_1, X_2, X_3)$ under the hypotheses H_0 and H_1

$$f_i(\underline{x}) = (2\pi)^{-\frac{3}{2}} \cdot \left| \underline{\Sigma} \right|^{-\frac{3}{2}} \cdot \exp - \frac{1}{2} (\underline{x} - \underline{\mu}_i)' \cdot \underline{\Sigma}^{-1} \cdot (\underline{x} - \underline{\mu}_i), \quad i=0,1,$$

where the covariance matrix $\underline{\Sigma}$ is given by

$$\underline{\Sigma} = \begin{pmatrix} \sigma_1^2 & \rho_{12} \sigma_1 \sigma_2 & \rho_{13} \sigma_1 \sigma_3 \\ \rho_{12} \sigma_1 \sigma_2 & \sigma_2^2 & \rho_{23} \sigma_2 \sigma_3 \\ \rho_{13} \sigma_1 \sigma_3 & \rho_{23} \sigma_2 \sigma_3 & \sigma_3^2 \end{pmatrix},$$

where the matrix elements are defined as follows

$$\sigma_1^2 := \text{var}(X_1) = \sigma_{\text{DK}}^2 + \sigma_{\text{P}}^2, \quad \rho_{12} \sigma_1 \sigma_2 := \text{cov}(X_1, X_2) = \sigma_{\text{P}}^2,$$

$$\sigma_2^2 := \text{var}(X_2) = \sigma_{\text{DKW}}^2 + \sigma_{\text{P}}^2, \quad \rho_{13} \sigma_1 \sigma_3 := \text{cov}(X_1, X_3) = a \cdot \sigma_{\text{P}}^2,$$

$$\sigma_3^2 := \text{var}(X_3) = \sigma_{\text{LT}}^2 + a^2 \cdot \sigma_{\text{P}}^2, \quad \rho_{23} \sigma_2 \sigma_3 := \text{cov}(X_2, X_3) = a \cdot \sigma_{\text{P}}^2,$$

and where the expectation vectors $\underline{\mu}_i$, $i=0,1$, are given by

$$\begin{aligned} \mu'_0 &:= (\mu_{DK}, \mu_{DKW}, \mu_{LT}) \\ \mu'_1 &:= \mu'_0 + \underline{\Delta}, \quad \underline{\Delta} := (0, \Delta, b \cdot \Delta) \end{aligned}$$

The optimal test in the sense of a guarantee of the highest probability of detecting a disturbance for a fixed false alarm probability is given by the *Neyman Pearson test* /4/. The critical region of this test, i.e., that region of \underline{x} -values which leads to an acceptance of the alternative hypothesis H_1 , is defined by the set

$$\{\underline{x} = (x_1, x_2, x_3) : \frac{f_1(\underline{x})}{f_0(\underline{x})} > K\}$$

where K has to be determined in such a way that the false alarm probability does not exceed a given value.

The calculation gives - up to a constant factor - the following test statistics

$$\begin{aligned} &\sigma_2 \cdot \sigma_3 \cdot [\sigma_3 \cdot (-\rho_{12} + \rho_{13} \cdot \rho_{23}) + b \cdot \sigma_2 \cdot (\rho_{12} \cdot \rho_{23} - \rho_{13})] \cdot x_1 + \\ &+ \sigma_1 \cdot \sigma_3 \cdot [\sigma_3 \cdot (1 - \rho_{13}^2) + b \cdot \sigma_2 \cdot (-\rho_{23} + \rho_{12} \cdot \rho_{13})] \cdot x_2 + \\ &+ \sigma_1 \cdot \sigma_2 \cdot [\sigma_3 \cdot (-\rho_{23} + \rho_{12} \cdot \rho_{13}) + b \cdot \sigma_2 \cdot (1 - \rho_{12}^2)] \cdot x_3 \end{aligned}$$

which does not depend upon the value of Δ , i.e., this test is a *uniformly most powerful* test.

Because of our assumptions this test statistics is a normally distributed random variable; therefore, it principally would not be difficult to determine the power of this test. As the determination of the variance, however, leads to long algebraic forms, we will discuss here only the *special case* $a=b=1$ which in practice might be achieved by appropriate scale transformations.

Returning to the process related nomenclature, in this case the test statistics is reduced to

$$-\sigma_P^2 \cdot (\sigma_{LT}^2 + \sigma_{DKW}^2) \cdot 2DK + \sigma_{LT}^2 \cdot (\sigma_{DK}^2 + \sigma_P^2) \cdot 2DW + \sigma_{DKW}^2 \cdot (\sigma_{DK}^2 + \sigma_P^2) \cdot LT,$$

and the probability $1-\beta$ to detect a disturbance Δ with a given false alarm probability α is

$$1-\beta = \Phi \left(\frac{\Delta}{\sqrt{\frac{\sigma_{LT}^2}{\sigma_{LT}^2 + \sigma_{DKW}^2} \sigma_{DKW}^2 + \frac{\sigma_P^2}{\sigma_P^2 + \sigma_{DK}^2} \sigma_{DK}^2}} - U_{1-\alpha} \right),$$

where $\phi(\cdot)$ is the normal distribution function and U its inverse.

If the uncertainty of the position of the separating layer is much larger than the uncertainty of the measurement of 2DKW, i.e., if $\sigma_{LT}^2 \gg \sigma_{DKW}^2$, we get for the detection probability

$$1-\beta = \phi\left(\frac{\Delta}{\sqrt{\sigma_{DKW}^2 + \frac{\sigma_P^2}{\sigma_P^2 + \sigma_{DK}^2} \cdot \sigma_{DK}^2}} - U_{1-\alpha}\right)$$

Now, as we have

$$\text{var}\left(2DKW - \frac{\sigma_P^2}{\sigma_P^2 + \sigma_{DK}^2} \cdot 2DK\right) = \sigma_{DKW}^2 + \frac{\sigma_P^2}{\sigma_{DK}^2 + \sigma_P^2} \cdot \sigma_{DK}^2$$

this means that the Neyman-Pearson test statistics is given by

$$2DKW - \frac{\sigma_P^2}{\sigma_P^2 + \sigma_{DK}^2} \cdot 2DK$$

Furthermore, because of

$$\sigma_{DKW}^2 + \frac{\sigma_P^2}{\sigma_P^2 + \sigma_{DK}^2} \cdot \sigma_{DK}^2 = \begin{cases} \sigma_{DKW}^2 + \sigma_{DK}^2 & \sigma_{DK}^2 \ll \sigma_P^2 \\ \sigma_{DKW}^2 + \sigma_P^2 & \sigma_{DK}^2 \gg \sigma_P^2 \end{cases} \text{ for}$$

we get the following intuitive result:

- i) In case the measurement error of 2DK is small compared to the process variation, we use the *difference* 2DKW-2DK as test statistics, this way the process variation is completely eliminated.
- ii) In the opposite case *simply* 2DKW is taken as test statistics.

If the process variation is large compared to the measurement uncertainty of 2DK, i.e., if $\sigma_P^2 \gg \sigma_{DK}^2$, we get for the detection probability

$$1-\beta = \phi\left(\frac{\Delta}{\sqrt{\frac{\sigma_{LT}^2}{\sigma_{LT}^2 + \sigma_{DKW}^2} \cdot \sigma_{DKW}^2 + \sigma_{DK}^2}} - U_{1-\alpha}\right)$$

which means that in this case the Neyman Pearson test statistics is given by

$$\frac{\sigma_{LT}^2}{\sigma_{LT}^2 + \sigma_{DKW}^2} \cdot 2DKW + \frac{\sigma_{DKW}^2}{\sigma_{LT}^2 + \sigma_{DKW}^2} \cdot LT - 2DKW$$

It should be noted here that the Neyman Pearson test is, as already mentioned, the best test in the sense of the power of the test (probability of detection), but that other test procedures might be preferred for *practical reasons*, e.g., one might be interested in performing separate tests for all measurements, or one might prefer a sequential procedure /5/. We will not present such alternatives, but discuss in which way the value of the false alarm probability can be determined with the help of *availability* considerations.

Let us assume that the test is performed at equidistant time points, and furthermore, that at such a time point the process is disturbed in the way described above with probability p . The losses in production time are in case of a shut down

- a if there is no disturbance,
- b if there is a disturbance and action is taken, and
- c if there is a disturbance and no action is taken,

here, we assume $0 < a < b < c$. The expected loss in time then is

- $a \cdot \alpha + 0 \cdot (1 - \alpha)$ if there is no disturbance
- $b \cdot (1 - \beta) + c \cdot \beta$ if there is a disturbance,

therefore, the (unconditioned) expected loss in time $E(\alpha)$ is

$$E(\alpha) = a \cdot \alpha \cdot (1 - p) + (b + (c - b) \cdot \beta) \cdot p$$

As the derivative of β with respect to α is a negative, monotonously increasing function of α , there exists exactly one optimum value α_{opt} with the following properties:

- i) α_{opt} decreases with increasing a for fixed b, c and p : If the time loss in case of a false alarm is large, then one should be careful with shut downs.
- ii) α_{opt} increases with increasing $c - b$ for fixed a and p : If the time loss in case of a not detected disturbance is relatively large, then one should not hesitate to shut down the cycle.
- iii) α_{opt} increases with increasing p for fixed a, b and c : If the frequency of disturbances is large, one should not hesitate to shut down the cycle.

4. Numerical Illustration

For simplicity we only consider the case that the uncertainty of the position of the separating layer is much larger than the measurement uncertainties and the process variation. We assume

$$\begin{aligned} \mu_{2DK} &= 1 \text{ [l/h]} & \sigma_{DK}^2 &= .10^2 \text{ [(l/h)}^2\text{]} \\ \mu_{2DKW} &= 4 \text{ [l/h]}^* & \sigma_{DKW}^2 &= .12^2 \text{ [(l/h)}^2\text{]} \end{aligned}$$

Experience shows that the process variation is of the order of 10 %, in the following we consider the two cases $\sigma_p^2 = .10^2$ and $.15^2 \text{ [(l/h)}^2\text{]}$.

In Figure 5 the results of the determination of the power of the test as

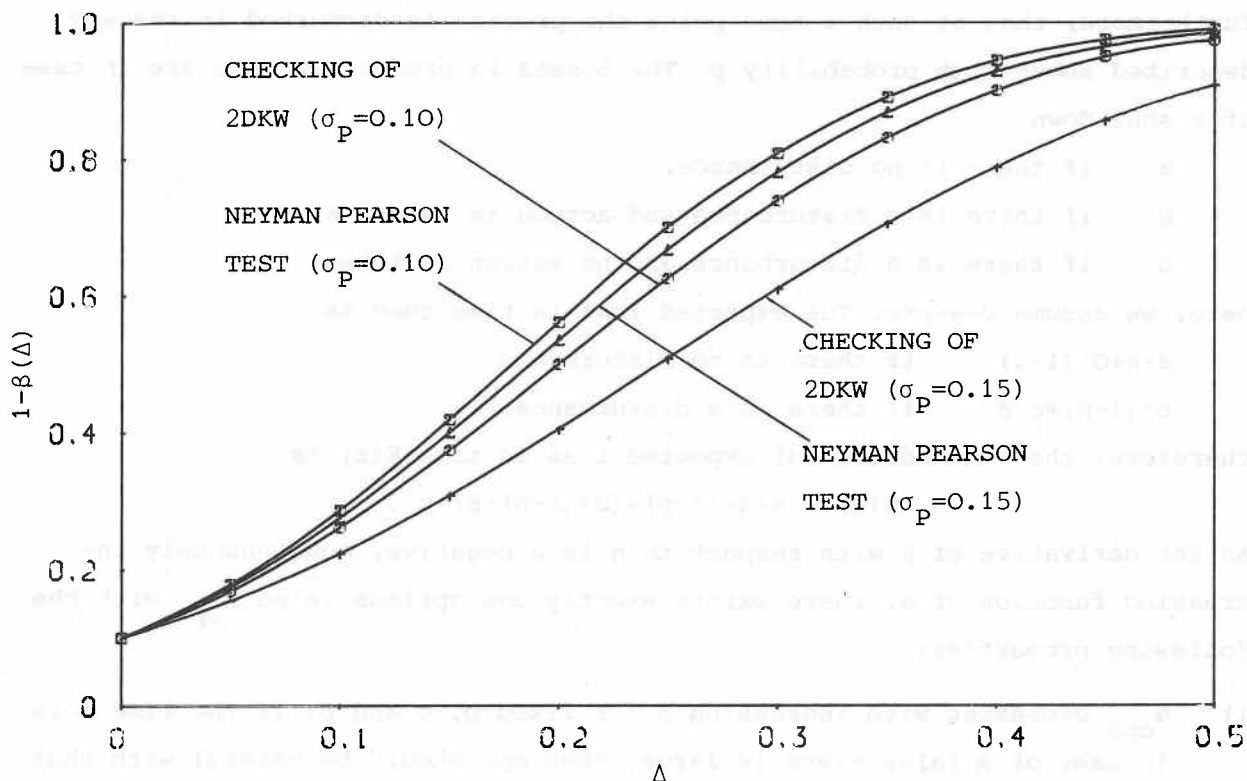


Fig. 5: Probability of detection as function of the disturbance Δ for a false alarm rate $\alpha=0.1$ for different test procedures and for different process variations

*) It should be noted that the 2DKW-stream alone has a lower value; this stream, however, is measured together with three further Kerosine streams, which leads to the value given.

a function of the disturbance Δ is shown: One can see in which way the process variation influences the probability of detection and furthermore, how much better the Neyman Pearson test procedure is compared to the test procedure which is simply based on the 2DKW flow.

A difficulty with respect to the determination of the optimal values of the false alarm probability is given by the fact that it depends upon the value Δ of the disturbance. For illustrative purposes we assume $\Delta^2 = \sigma_{DKW}^2 + \sigma_P^2 \cdot \sigma_{DK}^2 / (\sigma_P^2 + \sigma_{DK}^2)$, and furthermore $a=1$ resp. $2[h]$, $b=6[h]$ and $c=12[h]$. The result of the calculation is shown in Figure 6 which approves the qualitative discussion given before.

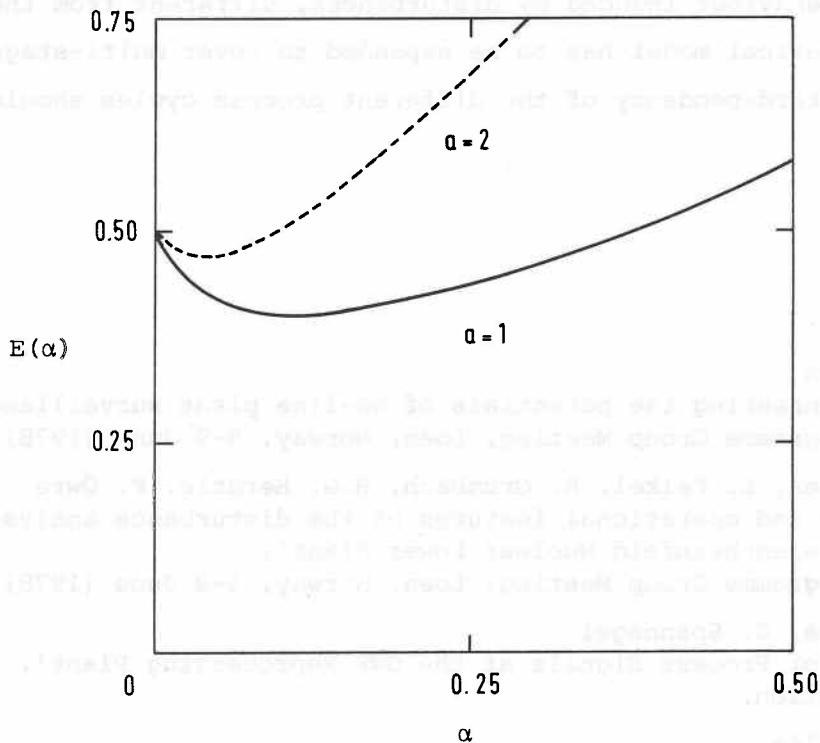


Fig. 6: Dependence of the expected loss in time $E(\alpha)$ on the false alarm probability with the parameter 'a' (loss in production time in case of shut-down if there is no disturbance)

5. Present status of the study

As already mentioned, for the 2. uranium cycle the anomalous process behaviour induced by hydraulic disturbances has been investigated and thereby

also single-stage decisions required for the control were identified. For the time being the formalism related to these decisions has been documented as a computer program. The program has been implemented on a Varian computer and it has been tested by simulation of the signals to be expected from the measurement instruments of this cycle. At the beginning of the next year first results are expected to be obtained during routine operation at the WAK reprocessing plant. To assist the operators, the information derived from the statistical treatment of the process signals is displayed in a condensed pattern; it should be noted that the computer has no access to switching process equipment.

In the future the analysis will be extended to include further cycles and the anomalous behaviour induced by disturbances, different from the hydraulic ones. The theoretical model has to be expanded to cover multi-stage decisions. Finally, the interdependency of the different process cycles should be taken into account.

6. References

- /1/ R. Grumbach
'Factors enhancing the potentials of on-line plant surveillance systems',
Halden Programme Group Meeting, Loen, Norway, 5-9 June (1978).
- /2/ W.E. Büttner, L. Felkel, R. Grumbach, H.G. Herdtle, F. Öwre
'Data base and operational features of the disturbance analysis system
for the Grafenrheinfeld Nuclear Power Plant',
Halden Programme Group Meeting, Loen, Norway, 5-9 June (1978).
- /3/ R. Avenhaus, G. Spannagel
'Analysis of Process Signals at the GWK Reprocessing Plant',
in preparation.
- /4/ K.A. Brownlee
'Statistical Theory and Methodology in Science and Technology',
John Wiley & Sons, New York (1967).
- /5/ R. Avenhaus, G. Spannagel
'Berücksichtigung von Prozeßschwankungen bei der Modellbildung zur Pro-
zeßsignalanalyse',
PWA-113/78, Kernforschungszentrum Karlsruhe.

W. Ehrenberger

SOFTWARE VERIFICATION IN ON-LINE SYSTEMS

SOFTWARE VERIFICATION IN ON-LINE SYSTEMS

W. Ehrenberger

Gesellschaft für Reaktorsicherheit (GRS) mbH, Forschungsgelände
Garching

IAEA/NPPCI specialists meeting on procedures and systems for
assisting an operator during normal and anomalous nuclear
power plant operation situations, Munich, December 5-7, 1979

ABSTRACT

Operator assistance is more and more provided by computers. Computers contain programs, whose quality should be above a certain level, before they are allowed to be used in reactor control rooms. Several possibilities for gaining software reliability figures are discussed in this paper.

By supervising the testing procedure of a program, one can estimate the number of remaining programming errors. Such an estimation, however, is not very accurate.

With mathematical proving procedures one can gain some knowledge on program properties. Such proving procedures are important for the verification of general WHILE-loops, which tend to be error prone.

The program analysis decomposes a program into its parts. First the program structure is made visible, which includes the data movements and the control flow. From this analysis test cases can be derived that lead to a complete test. Program analysis can be done by hand or automatically.

A statistical program test normally requires a large number of test runs. This number is diminished if details concerning both the program to be tested or its use are known in advance.

1. INTRODUCTION

The development of computer programs is an error prone process. This is well-known since a fairly long time, but it was only recently that quantitative estimates on the number of errors to be expected in a particular part of code have been provided. Based on observations and programs from different authors, Ottenstein, Schneider and Halstead recently published a theory on the number of bugs to be expected in a program part. See reference /1/.

In the future part of the information for the reactor operator will be preprocessed by computer software. It is desirable, to have not only an intuitive confidence in the correctness of these preprocessing programs, but to know quantitatively how many programming errors are still residual or what the probability of a program failure during plant operation really is. Such figures are important above all, if these programs have to be licensed. As a rule one will try to decide whether a program is error free or not. As we will see later, such a decision is not feasible in all cases; in some cases it is feasible, connected at the expense of excessive cost. So, in many cases we'll content ourselves with a probability statement, saying, for instance

- the probability of a program failure per run is smaller than \tilde{p} ; or
- the number of probably still present bugs in the program is smaller than $\tilde{\epsilon}$.

The paper will give an overview on methods, that lead to the intended statements.

Before we go into details, we have to say some words on terminology. Understandably, the interest in software quality in general and in software reliability in particular increases throughout the world. So far, however, no general solution of the problem has been reached. But several institutions and committees are dealing with this subject and are trying to establish rules and to fix a reasonable terminology. This terminology normally is based on the already existing theory

of hardware-reliability. In the following, we use the terms as they have been proposed by the technical committee "Safety and Security" of the "European Workshop on Industrial Computer Systems". The general understanding is that correctness or failing of a program can only be determined against a formal or informal functional requirements specification. For the following we always assume that such a specification exists. That means, if we have derived functional properties of a program, we are able to say, whether these properties are consistent with the functional requirements; ~~or~~, if we have made a test, it is always possible to decide unambiguously, whether the received test result fits to the requirements.

Based on this, we define:

- a program error is an inconsistency between the actual program code and the correct program code.
- a program failure occurs, if a program error is encountered during program execution. The failure becomes obvious by program output which is inconsistent with the specified output for that particular case.

2. SUPERVISING THE DEBUGGING PROCEDURE

Towards the end of its development process every program is debugged. During the debugging procedure the still residual errors are, hopefully completely, removed. In the course of this procedure the number of errors is diminished, if no new errors are introduced by removing old ones. As a rule, one can assume that an arbitrary program has less errors at the end of the debugging procedure, than at its beginning. Several authors derived mathematical models on the diminishing of the number of errors in the course of this procedure. Several kinds of detailed assumptions on the debugging process are feasible. The ultimately gained formulas depend on these assumptions and vary widely as well in their form as in their applicability. Some of these models for instance lead to the expected value of the number of still remaining programming errors; others to an expectation for the mean time between

two program failures during real operation (See fig. 1).

It is not the intention of this paper, to go into details on this subject. The interested reader is referred to publications /2,3,4,6,7,8,20,21/.

The models are well suited for estimating the time still necessary to end the debugging process. They are also suitable to get a figure for the expected cost before the program can be delivered. They have, however, the following shortcomings in common

- the model parameters can be evaluated only relatively unprecisely;
- therefore the results to be gained are not too accurate;
- most models fail, if no failures are encountered;
- many debugging procedures do not proceed, as assumed. In particular this is the case if towards the end of the debugging process a large number of errors still has to be removed.

Due to these reasons, these kinds of models are not sufficient for evaluating high reliability standards. The author's intuitive assumption is that the failure probabilities per demand which can be verified by means of these models will not be below 10^{-2} or 10^{-3} . In most cases, these figures are insufficient. They, however, might be sufficient, if the investigated program is only a part of a system, in particular, if there exists an additional diverse program which fulfills the same tasks. In this particular case the total system may guarantee relatively safe operation characteristics, by using unreliable components. Safety then is gained at the expense of availability - if we restrict our considerations to simple systems. Should then availability aspects dominate, we believe that supervising the debugging procedure alone is not sufficient for guaranteeing reliability figures as they have to be required for software in nuclear power plants.

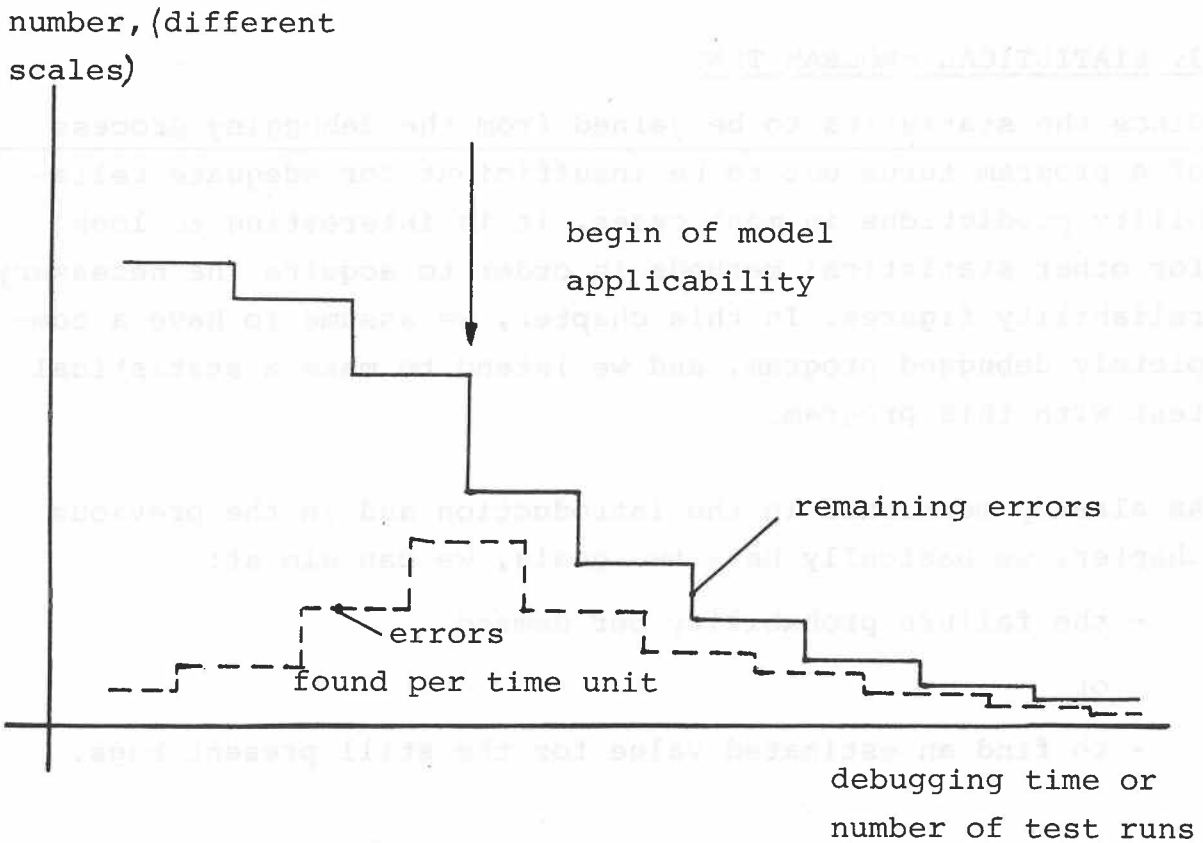


Fig. 1: Supervision of the debugging process, reliability growth models

The models are to be used for larger systems. Starting from the begin of integration testing the number of found and removed bugs is recorded. Normally this number increases for a certain time and becomes gradually smaller later. Some models estimate the number of still remaining errors, others estimate the program MTBF during operation. The models normally are applicable from the time on where the number of detected and removed errors per time unit decreases. In some models the time steps vary. Some even assume a certain probability for introducing new errors during the removal of old ones.

3. STATISTICAL PROGRAM TEST

Since the statistics to be gained from the debugging process of a program turns out to be insufficient for adequate reliability predictions in most cases, it is interesting to look for other statistical methods in order to acquire the necessary reliability figures. In this chapter, we assume to have a completely debugged program, and we intend to make a statistical test with this program.

As already mentioned in the introduction and in the previous chapter, we basically have two goals, we can aim at:

- the failure probability per demand
- or
- to find an estimated value for the still present bugs.

If we aim at the first figure, our test will be organized such that it offers input data to the test object with the same distribution as they are supposed to come during on-line operation. If we are interested in the number of potentially remaining bugs in the program, our test will touch all program parts with the same probability. In the first case it is indispensable to have a detailed knowledge on the demand distribution during on-line operation. If our knowledge on this distribution is not exact, it certainly is feasible to construct a test according to that knowledge; it will, however, lead to more or less inaccurate results and presumably require a larger number of test cases than in that case where the detailed knowledge exists. The same applies in a similar way to the test according to the errors in the program: In order to construct such a test, we need to know how the individual program parts are to be reached by the program counter, how we can induce particular data movements or arrange that specific memory locations are used. Therefore it is helpful and, to a certain degree necessary, to have a detailed knowledge on the internals of the test object. How such a knowledge can be gained, will be discussed later in this paper.

The number of required independent test cases can be calculated from the theory of statistics. Since we assume to have a completely, or nearly completely debugged program, we can use the Poisson distribution. If our intended result is:

With a level of confidence of 95% the failure probability per demand is smaller than 10^{-k} , then the number of necessary test cases equals

$$n_{95} \approx 3 \cdot 10^k.$$

The same number of test cases is required, if we want to show with this level of confidence that the probability to have a programming error left in the code is smaller than 10^{-k} . If the level of confidence should be 99%, the number of test runs we need is

$$n_{99} \approx 4,6 \cdot 10^k.$$

These figures apply, if no failure occurred.

If we know about the relationship between the demands to the program from the nuclear reactor and the frequency of the use of particular program parts or data areas that is connected with these demands, we are able to convert a figure gained from one of the above mentioned tests into the respective figure of the other test. This applies in particular, if our test could not consider the entire program, but was structured according to the theory of stratified samples.

n	probability to touch each of the 4000 items
50 000	$1 - 1,49 \cdot 10^{-2} + 1,10 \cdot 10^{-4} - \dots$
75 000	$1 - 2,87 \cdot 10^{-5} + 4 \cdot 10^{-10} - \dots$
100 000	$1 - 5,54 \cdot 10^{-8} + 1,52 \cdot 10^{-15} - \dots$
200 000	$1 - 7,66 \cdot 10^{-19} + 2,9 \cdot 10^{-37} - \dots$

Table 1: Probability to check 4000 distinct items in the course of n test runs.

Another kind of statistical approach deals with the following question:

- What is the probability that all demands that can potentially come from the technical process, have been applied to the program?

or

- What is the probability that each program property has been touched at least once through our statistical test?

An answer to this question is given in table 1 for a particular number of items. In our case, these items can either be program properties or demands coming from the technical process. A necessary prerequisite is that the test ensures that all of these 4000 distinct items are touched with the same probability. It is not difficult, to construct a test where these items are the demands from the technical process; if, however, these items are particular program properties, it is not easy, to fulfill the prerequisite. Then the number of test cases should be estimated, where the prerequisite is fulfilled. Only these should be counted for n .

For the program to be used for operator information or in the man-machine-interface, it is not very probable that one can make efficient use of the last consideration. This is because the number of potential reactions of the technical process and the number of program properties which treat these demands as well, are quite large. But in most cases it will be useful to apply statistical tests for certain kinds of demands or to specific program parts. Details concerning this kind of tests have been published in references /30,31,32/.

4. SYSTEMATIC TEST

In the two preceding chapters we have seen that statistical methods need a considerable amount of effort in order to show whether the required reliability figures have been met. Here,

we discuss whether systematic methods are superior either in terms of results or of overall cost.

The first systematic means to be employed is a careful prove-reading of the produced code. This prove-reading checks:

- has the documentation the appropriate form?
- does the contents of the documents reveal any discrepancies to the required functions?
- have the agreed programming and coding standards been met?

As is known from personal experience and from the literature as well /29/ this can reveal a lot of errors. Also to explain the function of a particular piece of code to another person can lead to the detection of many programming errors. For reactor software one will certainly use this possibility.

Further checks are connected with specific kinds of tests, for instance:

- test of all explicitly specified requirements;
- test of the major part of the assumed cases of plant behaviour;
- test of all critical time conditions;
- execute each arc of the program graph at least once;
- execute each reference to each memory location at least once;
- execute the maximum number of loop repetitions;
- execute all arithmetically critical mappings at all critical points;
- check whether the boundaries of the different subareas of the input domain are positioned correctly.

In order to be able to perform such kind of tests it is necessary to know details about the internals of the program. These details can be gained by careful analysis.

5. PROGRAM ANALYSIS

Program analysis can be made manually or automatically. If it is done automatically a prerequisite is that the relevant analyser accepts the used programming language. Normally, analysers are designed for high level languages, see for instance references /23,24,25,26,27,28/. In reference /22/ an automatic aid for analysing a specific kind of assembler programs is described.

Program analyses can aim to answer one or more of the following questions:

- a.) Did the already executed test cases perform a complete test, such that no errors are left?
- b.) What is the minimal number of necessary test cases in order to get a complete test and how are these test runs to be arranged?
- c.) Does the program, or do parts of the program implement specified requirements and can one show this without test?

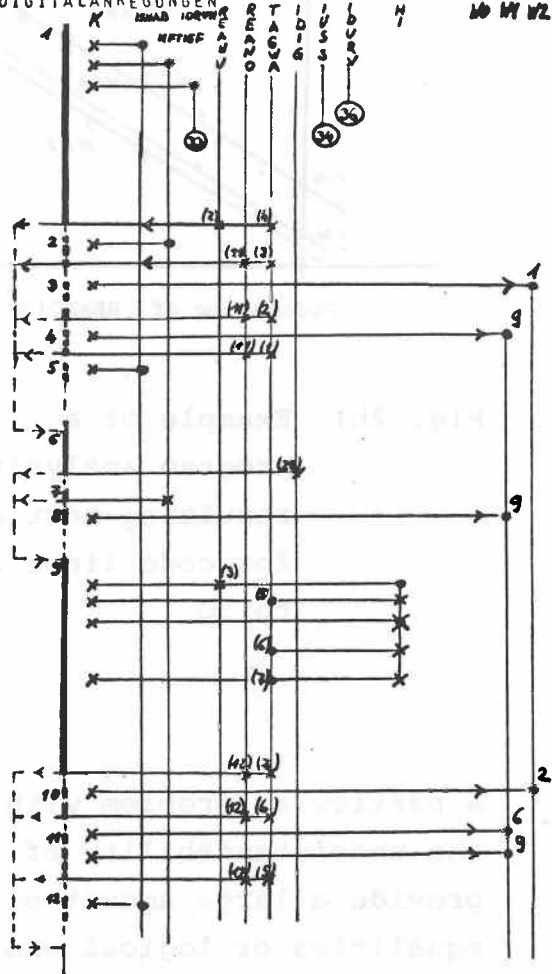
The analysis uses a mixture of decomposition of the code, formal proofs and tests in order to get the required knowledge about the consistency of a program with its functional requirements. In most cases the result of the analysis are test conditions that must be offered to the program. In other cases the analysis may reveal by itself structures that can be compared with the requirement specification. This is only possible if the specification is provided in a suitable form and sufficiently detailed.

By investigating the branching conditions in the program and evaluating the revers functions of the mappings that lead to the values of data which influence branchings, it is possible to determine which set of input conditions leads to which path. Having received this, one can either select a suitable number of inputs related to one specific path and execute that path in reality, or one can execute that path symbolically. It is discussed to perform that symbolic execution by automated tools, see e.g. /34,35/.

```

1
2
3
4 SUBROUTINE TAFAN (IDIG, TAGWA, REANO, REANU, IUSS, IDURV, WO, W1, W2)
5 DIMENSION IDIG(32), TAGWA(40), REANO(13), REANU(3)
6 INTEGER WO, W1, W2
7
8 C
9 C UNTERPROGRAMM ZUR BEHANDLUNG DER ANALOGEN GRENZWERTVERLETZUNGEI
10 C UND DER MIT ANALOGWERTEN VERKNUEPFTEN DIGITALANREGUNGEN
11 C
12 ISNAB=0
13 NFTIEF = 0
14 IDRUTI = 0
15
16 CCCCC ENDE DER VORBESETZUNGEN,
17 C
18 C MFUD
19 C
20 IF (REANU(2)-TAGWA(4)) 9,9,20
21 7 NFTIEF = 1
22 10 IF (REANO(11)-TAGWA(3)) 20,12,12
23 12 CALL SETBIT(W2,1)
24 IF (REANO(11)-TAGWA(2)) 20,14,14
25 14 CALL SETBIT(W1,9)
26 IF (REANO(11)-TAGWA(1)) 20,16,16
27 16 ISNAB=1
28
29 C
30 C UBKA
31 C
32 20 IF (IDIG(29)) 30,30,25
33 25 IF (NFTIEF) 30,30,26
34 26 CALL SETBIT(W1,9)
35
36 C
37 C KEDU
38 C
39 30 HI = 0.8*REANU(3)
40 TAGWA(5) = 0.160 + HI
41 HI = 0.080 + HI
42 TAGWA(6) = HI
43 TAGWA(7) = HI - 0.024
44
45 C
46 C NFLD
47 C
48 IF (REANU(12)-TAGWA(7)) 40,31,31
49 31 CALL SETBIT(W2,2)
50 35 IF (REANO(12)-TAGWA(6)) 40,36,36
51 36 CALL SETBIT(W1,6)
52 CALL SETBIT(W1,9)
53 IF (REANU(12)-TAGWA(5)) 40,37,37
54 37 ISNAB=1

```



REANU2 < TAGWA4	REANO11 ≥ TAGWA3	REANO11 ≥ TAGWA2	REANO11 ≥ TAGWA1
0	1		
1	0		
1	1	0	
1	1	1	0
1	1	1	1

empty places:
value irrelevant

Fig. 2a: Example of a program analysis: Begin of the manual analysis and finally resulting test cases for code lines 19 to 26, from /17/.

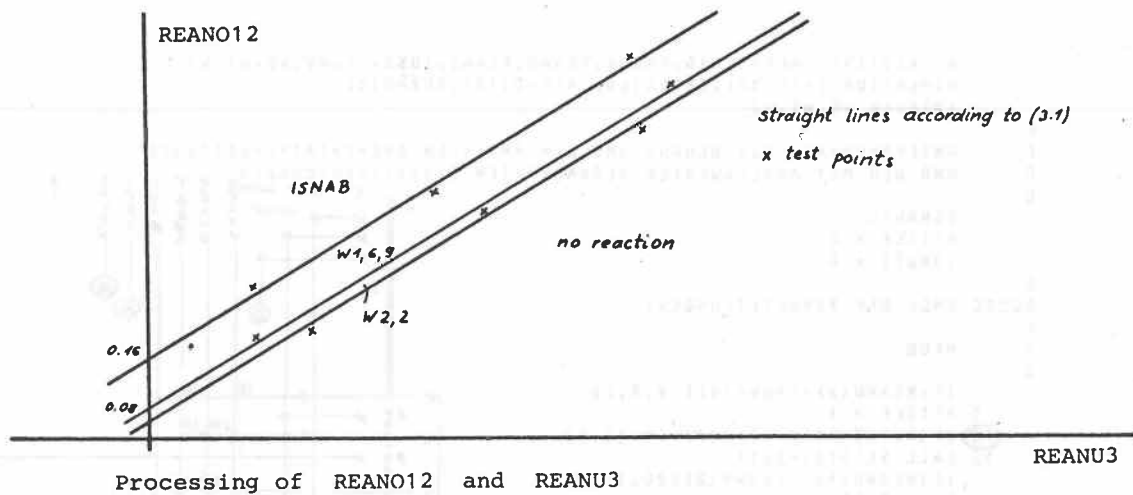


Fig. 2b: Example of a program analysis: resulting test cases for code lines 27 to 50

REANO 12 \geq TAGWA10	REANO 12 \geq TAGWA9	REANO12 \geq TAGWA8
0		
1	0	
1	1	0
1	1	1

A particular problem with automatic program analysers is the understandability of their output. Some of these tools provide a large amount of data, that come out in form of inequalities or logical expressions. It is quite difficult to interpret this output correctly and to associate with it a meaning in relation to the program specification. Here some additional manual work is necessary as a rule. Recently, however, particular effort is taken to make the output easy to understand.

The reader, who is interested in details on the theory of testing and program analysis is referred to the papers /16,17, 19/. /17/ and /19/ in particular also deal with manual analysis of programs.

6. PROOF TECHNIQUES

The systematic verification methods discussed so far do not apply for general WHILE-loops or recursive procedures. This is, because in these structures the result of one repetition may be input of the next repetition. If such structures are used, it is more or less indispensable to employ mathematical proof techniques. These techniques usually use the principle of induction. Normally the mathematical effort to be taken is considerable. Perhaps this is the reason why this area has attracted a lot of interest and has led to a considerable number of publications. See for instance references /9,10,11,12,13,14,15/. The methods derived and discussed, however, do not seem to be suitable for use by the broad public. All the proof techniques require full intuitive understanding of the programmed problem and the derivation of so called loop-invariants or loop-assertions by hand. Only a part of the proving effort itself can be automated.

Since human activities can not be avoided in essential parts, the whole techniques are rather error prone. Therefore we hope that software for nuclear power plants avoids structures which require inductive proofs.

7. VALIDATION CONCEPT

If computers are being used to assist the operator of a nuclear power plant, it is reasonable to require a failure probability per demand, which is less than the human failure probability. From past investigations of human error rates we can estimate that programs need failure probabilities per demand below 10^{-4} or 10^{-5} . With the experience gained so far, it is very improbable that these figures can be verified by means of supervising the debugging process alone. Concerning statistical testing the number of necessary test runs would be in the order of magnitude of 30 000 to 460 000. The cost and effort involved in performing so many runs would be considerable. Therefore it is rational to look for an appropriate synthesis of the previously discussed methods.

One should reasonably supervise the debugging process, try to gain some estimates from this and perform some of the systematic test efforts that are included in chapter 4. If an automatic tool is available, one should try to make as much use of it, as possible. Having done this, one can decide which supplementary manual program analysis and testing is feasible without too much effort. Having executed this analysis and the related test cases, one should try to find out, which portion of all possible demands to the program or which portion of the code itself has been verified. Then, the effort for statistical testing of the rest of the demands or the rest of the code should be estimated. In many cases it will turn out that the remaining necessary verification work will not be too large.

Last not least we point out that in most cases it will not be sufficient to rely very much on a burn-in phase or an on-line testing phase of software during plant operation. As can be shown by statistics, the probability to get sufficient confidence in the correct program execution by a preliminary operation, is very low and as a rule unsatisfactory. The burn-in phase may be indispensable for hard wired equipment, it can certainly also reveal software errors, but it usually will comprise only a very limited amount of the possible plant demands. Therefore a more or less formal validation procedure, preferably by independent persons, is considered necessary. This opinion also reflects the current discussion in national and international computer safety committees.

8. CONCLUSION

Currently a lot of techniques for verifying and validating the correctness of computer programs are available. None of these techniques, however, is able to verify realistic programs with minimal cost. In most cases minimum effort will be reached by a suitable, problem depending, mixture of different techniques. In the future automated testing tools will become dominant. For any on-line reactor application it is considered important not only to rely on intuitive understanding or on the results of a preliminary on-line test, but to use a formal validation approach.

9. ACKNOWLEDGEMENT

The author thanks his colleagues Dr. Pühr-Westerheide and M. Kersken for proof-reading this manuskript and many helpful suggestions.

10. REFERENCES

- /1/ O t t e n s t e i n, L.M., S c h n e i d e r, V.B.,
H a l s t e a d, M.H.: Predicting the Number of Bugs
Expected in a Program Module
Computer Science Department, Purdue University
West-Lafayette, Ind., CSD-TR 205, oct 1976.
- /2/ S h o o m a n, Martin L.: Operational Testing and
Software Reliability Estimation during Program Develop-
ment. 1973 IEEE Symposium on Computer Software Reliabili-
ty; IEEE Cat.No. 73 CHO 741-9CSR.
- /3/ M o r a n d a, P.B., J e l i n s k i, Z.:
Software Reliability Predictions. MDAC Paper
WD 2482, August 1975.
- /4/ M o r a n d a, P.B.: Prediction of Software Reliability
During Debugging. MDAC Paper
WD 2471 April 1975.
- /5/ L i t t l e w o o d, B., V e r a l l, J.L.:
A Bayesian Reliability Growth Model for Computer Software.
As /2/.
- /6/ H a l l e n d a l, G., H e d i n, A., Ö s t r a n d, A.:
A Model for Software Reliability Prediction for Control
Computers. The Royal Institute of Technology, Sweden,
TTS 7502, 1975.
- /7/ A n d e r s s o n, H., P e i r a m, L., S t r a n d b e r g,
K.: A Study of Software Reliability. 8th International
Teletraffic Congress Melbourne 1976.
- /8/ F o r m a n, E.: Statistical Models and Methods for
Measuring Software Reliability. Dissertation, The George
Washington University; Xerox University Microfilms,
Ann Arbor Michigan 48 106, 1975.

- /9/ B a s u, S.K., M i s r a, J.: Some Classes of Naturally Provable Programs, 2nd International Conference on Software Engineering, 1976, IEEE Cat.No.76 CH 1125-4C.
- /10/ B a s u, S.K., M i s r a, J.: Proving Loop Programs. IEEE Transactions on Software Engineering, Vol. SE1, March 1975.
- /11/ G e r h a r d, S.L.: Knowledge about Programs: A Model and Case Study. Sigplan Notices, Boston, Vol.10, No.6, 1975.
- /12/ K i n g, J.C.: A Program Verifier. Proceedings of the IFIP Congress 1971.
- /13/ L o n d o n, R.L.: Proving Programs Correct: Some Techniques and Examples. Bit 10 (1970), 168-182.
- /14/ M a n n a, Z., P n u e l l, A.: Axiomatic Approach to Total Correctness of Programs. Stanford University, STAN-CS-73-382, AIM-210, 1973.
- /15/ R e y n o l d s, C., Y e h, R.T.: Induction as a Basis for Program Verification. 2nd International Conference on Software Engineering 1976, IEEE Cat.No. 76 CH 1125-4C.
- /16/ G o o d e n o u g h, J.B., G e r h a r d, S.L.: Toward a Theory of Test Data Selection. International Conference on Reliable Software 1975, IEEE Cat.No.75CHO 940-7CSR.
- /17/ E h r e n b e r g e r, W., P u h r - W e s t e r h e i d e, P.: Analytical Software Verification, Agard Conference Preprint 261, Meeting of the Avionics Panel in Ankara, April 1979
- /18/ F r e y, H.: Glossary of Terms and Definitions Related to Safety of Industrial Computer Systems, IFAC Symposium SAFECOMP, Stuttgart 1979

- /19/ E h r e n b e r g e r, W., R a u c h, G., O k r o y, K.:
Programanalysis - A Method for the Verification of Soft-
ware for the Control of a Nuclear Reactor. As /15/.
- /20/ R e m u s, H., Z i l l e s, S.: Prediction and Manage-
ment of Program Quality, 4th International Conference on
Software Engineering, Munich 1979, IEEE Cat.No. 79
CH 1479-5C
- /21/ B o l o g n a, S., E h r e n b e r g e r, W.:
Applicability of Statistical Software Reliability Models
for Reactor Safety Software Verification, Comitato
Nazionale Energia Nucleare, Report RT/ING (79) 1
- /22/ Projekt Prozeßlenkung mit DV-Anlagen. Abschlußbericht des
Förderungsvorhabens P 4.1/6, KWU Berichte RE 26/013/77,
RE 26/046/77, RE 23/047/77.
- /23/ R a m a m o o r t h y, C.V., H o, S.F.: Testing Large
Software with Automated Software Evaluation Systems. as /16/.
- /24/ R a m a m o o r t h y, C.V., H o, S.F.: On the Automated
Generation of Program Test Data. as /15/.
- /25/ M i l l e r, E.F.jr., M e l t o n, R.A.: Automated
Generation of Testcase Datasets. as /16/.
- /26/ O k r o y, K.: Automation der Analyse von PEARL-Programmen.
PDV-E97, KFK-Karlsruhe, 1977.
- /27/ G m e i n e r, L.: SADAT - Ein automatisches Testsystem
für FORTRAN-Programme. Wie /26/.
- /28/ B o l o g n a, S., T a y l o r, J.R.: Validation of
Safety Related Software. IAEA/NPPCI Specialist Meeting
on Computerized Control and Safety Systems in Nuclear
Power Plants, July 1977.
- /29/ B r u g g e r e, T.H.: Software Engineering: Management,
Personnel and Methodology. As /20/.

- /30/ E h r e n b e r g e r, W., P l ö g e r t, K.:
Einsatz statischer Methoden zur Gewinnung von Zuverlässigkeitskenngrößen von Programmen. KFK-PDV-Bericht Nr. 151, June 1978.
- /31/ E h r e n b e r g e r, W., P l ö g e r t, K.:
Statistical Verification of Reactor Protection Software. International Symposium on Nuclear Power Plant Control. Cannes, April 1978.
- /32/ E h r e n b e r g e r, W., H o f e r, H., H o e r m a n n, H.:
Probability Considerations Concerning the Test of the Correct Performance of a Process Computer by Means of a Second Computer. IFAC Congress Boston, Mass., 1975.
- /33/ L o n g, A.B., R a m a m o o r t h y, C.V., H o, S.F., S o, H.H., R e e v e s, H.L., S t r a k e r, E.A.:
Validation of Nuclear Power Plant Safety System Software, IAEA Meeting, Pittsburgh, July 1977.
- /34/ H o w d e n, W.E.: Symbolic Testing and a DISSECT Symbolic Evaluation System, Computer Science Tech. Report 11, Applied Pysics and Information Science , University of California, San Diego, may 1976
- /35/ C l a r k e, L.A.: A System to Gererate Test Data and Symbolically Execute Programs, IEEE Trans.on Software Eng. Vol. SE2, sept. 1976

E. Holló

OPERATOR-INTERACTIVE SURVEILLANCE METHOD OF PERIODIC INSPECTION
OF ACTIVE ENGINEERED SAFETY SYSTEM OF WWER 440 TYPE REACTORS

Operator-interactive Surveillance Method of Periodic
Inspection of Active Engineered Safety System of
WWER 440 Type Reactors

Előd Holló

Institute for Electrical Power Research

- Budapest, Hungary -

INTRODUCTION

The main tasks of the engineered safety systems /ESS/ of the WWER-440 type reactors are to cool the active zone in the event of loss of coolant in the primary circuit, to decrease the reactivity of the zone in this case, and to reduce the pressure and temperature amplitudes in the hermetic rooms. To perform these tasks they have to ensure the flooding of the active zone with cold boron containing water, to remove its remanent heat, and to condensate the steam present in the hermetic rooms by means of both water injection and steam bubbling.

In compliance with the above listed tasks, functionally the ESS's can be divided into two main parts: the emergency core cooling system and the pressure reduction system of hermetic rooms. Both parts consist of passive and active subsystems, their availability has periodically to be checked during the normal operation of the nuclear power plant. The passive subsystems are checked during the annual shutdown period of the reactors when their reloading having been finished, the active subsystems may and have to be checked during the normal operation of the plant, too. This can be performed by the appropriate execution of the operating start-up instructions concerning these systems, while the effectiveness of their checking can be increased by computerized data processing.

In this paper a simple method resulting satisfactory information for the operator to qualify the ESS's is presented.

1. BRIEF DESCRIPTION OF THE ACTIVE ESS'S OF
WVER-440 TYPE REACTORS

The active ESS's of the WVER type reactors consist of the high- and low-pressure emergency core cooling subsystems and of the spraying system of the hermetic rooms. Their typical block scheme is shown in Fig. 1. For safety reasons a triple redundancy per subsystems is customary. In respect of the pipe connection, each of the subsystems consists of a pump for different function /high-pressure, low-pressure and spray pump/, a tank containing boric-acid solution, and the closing-regulating fittings. The low-pressure and injection pumps work to a common tank, the latter returning the water accumulated on the floor of the hermetic rooms in a closed system through heat-exchanger to the spraying-nozzle. For filtering the radiactive iodine possibly present in the hermetic rooms, various chemicals are added into the input of the spray pump.

The subsystems of the active ESS's are in stand-by condition in the course of the nominal operation of the power plant and begin to work only in the case of disturbances. Their operation is initiated from the pressure and water level of the primary cooling circuit and from the pressure of the hermetic rooms, resp. depending on various conditions. Such conditions causing interaction may be for instance a 40-60 % reduction of the water level of the pressurizer, 10-80% decrease of the primary-circuit pressure or a pressure increase of 10-15% in the hermetic rooms.

The periodical checking of the subsystems of active ESS's during normal operation consists of a state control and functional control test. The state control can be performed by means of local measurements and visual inspection only

during the shutdown of the reactor, while the functional tests can be performed during operation, too, periodically by starting up of the subsystems. The latter is made possible by the redundancy of the subsystems, the installation of recirculating test-pipelines /dotted line in Fig.1/, and the built-in instrumentation.

2. PRINCIPLE OF THE FUNCTIONAL TESTING METHODS

2.1. The present testing methods

In compliance with the present operating instructions the functional tests of the active ESS's are performed manually by the operators. The manual activity concerns partly the starting-up of the pumps through the recirculating test-pipes and partly the evaluation of the data measured by the instruments in the control room. The evaluation covers the limit-value checking in the traditional sense and the determination of several dynamic characteristics, e.g. the time needed for reaching the load condition. Practically the limit-value checks mean the examination whether the measured parameters lie in the permissible operating ranges round the theoretical working point determined by the static characteristic curves of the equipments /see Fig. 2/a./.

The theoretical hydraulic working point of the testing water loops P (Q_T , H_T) is determined by the static characteristics of the pump-motor unit / $H_{PM} = f(Q_{PM})$ / and the pipeline-tank unit / $H_{PT} = F(Q_{PT})$ /. The permissible operating range is set up by the values ΔH and ΔQ , this has to cover the actually measured working point P (Q_M , H_M). In this case the qualification of the system is CORRECT, else INCORRECT. The qualification is performed by the instruments located in the control room by using the adjusted threshold-levels and by giving warning signals for the operators.

In the case of the qualification SATISFACTORY, the sensitivity of judgment can further be refined by taking the measuring errors into account. In this case the operating range loaded by the measuring errors of ΔH_M and ΔQ_M has to be produced with its limits being as follows:

$$Q_M - \Delta Q_M < Q < Q_M + \Delta Q_M$$

$$H_M - \Delta H_M < H < H_M + \Delta H_M$$

If the actual operating range thus formed lies fully in the permissible operating range of

$$Q_T - \Delta Q < Q < Q_T + \Delta Q$$

$$H_T - \Delta H < H < H_T + \Delta H$$

the result of the qualification is CORRECT, else ACCEPTABLE. At present this is judged on the basis of the measurement results by the operators, manually /Fig. 2/b./

2.2. Principle of the suggested computer-based method

According to the present practice, the checking of the subsystems of active ESS's refers to the global functional qualification of all technological equipment in the testing loop. With the fact taken into consideration, that in a power plant unit 3 to 9 subsystems dependent on redundancy are built in, in the course of the periodic checking considerable manual work is incumbent on the operators. The development and increase in capacity of the computer-aided plant-control systems has made possible to release the operators from the mechanical part of the evaluating work and to further refine the criteria of the functional judgement.

So far, the permissible limit values of the measured parameters have been considered to be constant in the full operating range /threshold limits set on indicating instrument/. If, with the assumption of computer-aided evaluation, the permissible operating range is determined with the help of the static characteristic curves of the equipments, qualification criteria of a more sensitive nature with a better adaptability to the changing operating circumstances but still simple in their formulation can be set up. The basic idea of the method has been well known [1, 2]. The process supposes that instead of the theoretical characteristics of the equipment a band of characteristics is given which includes in implicit form the permissible parameter deviations. The permissible operating range is cut out by the bands of characteristics of equipments being in functional relation with each other. A disadvantage of the method is that the comparison of the actual working-point ranges loaded by measuring errors and the permissible working-point ranges confined by curves requires a rather complicate evaluation /see Fig.3./.

The features of the suggested, simplified method are the following:

1. Checking using the bands of characteristics of the equipments being in functional interrelation is performed individually and independently from each other. The qualification is carried out by investigating whether the measured working-point or rather its range determined by the measurement errors is located entirely or partially inside or outside the permissible working-point range.
2. The permissible working-point range is determined by the permissible band of characteristic curves and by the axes of abscissas and ordinates at the two sides, respectively.

3. The qualification takes place by comparing the permissible and the actual operating ranges of the equipments. This may be CORRECT, ACCEPTABLE, or INCORRECT depending on whether the measured operating range lies fully or partially in the permissible range, or the measured working point is located outside the bands, resp.

For the subsystems of the active ESS's the state of the pipeline-tank unit pertaining to the testing loop /leakage, blockage/ and the functional operation of the pump-motor unit can be checked with the suggested method. The determination of the input data of the computerized process is indicated in Fig. 4 and the individual steps of the qualifying algorithm are contained in Fig. 6.

4. The qualification of the entire functional system is CORRECT, if the function of all the equipments is CORRECT, and it is INCORRECT, if the operation of any or several equipments is INCORRECT. In other cases the qualification is ACCEPTABLE.

The process of the system qualification for the subsystems of the active ESS's is illustrated by Fig. 5.

3. ROLE OF THE OPERATORS DURING THE FUNCTIONAL CHECKING

In every phase of the suggested computer-based checking method the operators have significant role:

START-UP MEASUREMENT - The selection of the safety subsystem to be examined, the switch over of the pump to the testing loop, and its starting are performed by the operators. The measurement takes place automatically with a cycle time determined by the computer. According to the present condition, the water flow rate in the testing loop is indicated only by the instruments in the control room, the suggested method makes their connection to the computer necessary. The primary processing of the data, as averaging, credibility test, etc., is performed by the computer automatically.

EVALUATION - The secondary evaluation of the measurement data, the qualification of the active ESS's sub-systems are accomplished by the computer under the surveillance of the operator. For these purposes an interactive display should be made available to the operator, on which the evaluation is started, the results appear, and through which interactions into the process of analysis can be made. The operator interactions into the evaluation process represent answers given to the questions put by the computer. Thus, the operator has a dynamic chance to choose among

- system examination with constant limit values /traditional method, see Fig.2/,
- equipment and system examination, resp., on the basis of dynamically changing limit values /characteristics curve method, see Figs 4 and 5/, and
- repeating the evaluation several times.

The repeatability of the evaluation using various criteria is also useful because thus the operators may ascertain the correctness of the signals obtained in the control room and can solve the inconsistency between the results obtained with the two methods.

DISPLAY - The results can be displayed alphanumerically or graphically in the course or at the end of the evaluation in the form chosen by the operator. If alphanumerical display is chosen, first the identifier of the qualified system or equipment and the result of the qualification are displayed, while, if further informations are required, also the method of examination /fixed or dynamic limit values/ and the measured and/or permissible parameter values can be displayed. Essentially, the graphic display corresponds to Figs. 2 through 4.

INTERACTION - Beyond the interaction into the process of evaluation, in dependence from the result obtained, the operator switches back the tested active ESS subsystem in operational stand -by condition /CORRECT/ or passes it for repair /INCORRECT/ or may impose increased checking frequency and attention, resp., on the same /ACCEPTABLE/.

The block diagram of the complex process of functional examination and the description of the secondary evaluation on flow-diagram level are contained in Figs 7 and 8.

4. APPLICABILITY AND ADVANTAGES/DISADVANTAGES OF THE SUGGESTED METHOD

The scope of application of the suggested method may cover the followings:

- the global qualification of the functional operation and state of the active ESS subsystems and their components at a given working point. If the qualification is performed for several working points, within the limits determined by the testing loop a simple and quick proving and verifying of the static characteristics is made possible,
- the method is primarily suggested for facilitating the operational work of the personnel, for periodic examinations on process control computers. Beside this, however, the method can also be realized on automatic data acquisition systems or on big data processing computers during start-up measurements, too.
- The conditions and limitations of the applicability are the followings:

- for the evaluation the accurate measurement of the parameters determining the operational working-point range is necessary. Accuracy becomes a limitation of applicability if the measuring error is comparable with the band width of the permissible working-point range, i.e. $2x \Delta H_M > H_{\max} - H_{\min}$ and $2x \Delta Q_M > Q_{\max} - Q_{\min}$, resp.
- the static characteristic-bands of equipments occurs as input data, their determination is one of the greatest problems in practice. In ideal cases these are determined by the planning or manufacturing company. In other cases their determination forms the task of the personnel putting the system into operation or operating it on the basis of technical and safety considerations. For example, if the dependence of the characteristic curves on RPM /n/ is known, i.e. $H_{PM} = f(Q_{PM}; n)$, also the fluctuation of n sets out a band, which may be used,
- in the course of evaluation it was assumed, that the rate of change of characteristic curves possessing local maximum or minimum values round the local point isn't too big. Otherwise it may happen, that the nodes of a working-point range are located inside the permissible band of curves, however, some of its parts may be placed outside the band and thus the results of evaluation may be incorrect.

As a summary it may be stated that the suggested computer-based method has considerable advantages in comparison to the traditional manual system-tests. These advantages manifest themselves primarily in the enlargement of the scope of checking /system-equipment examination, consideration of fixed-dynamic limit values/, in the quality change of display /alphanumeric, graphical concentrated display

of the results/, in raising the work of the operators to a higher level /interactive control instead of manual calculation/. It should be noted, however, that before introducing the method a more detailed a-priori know-ledge of the active secondary safety systems /exact determination of the characteristic-bands, valuation of the accuracy and scope of the measuring system/ is necessary.

LITERATURE

- [1] Hawickhorst, W.: Voruntersuchungen zur Funktionsprüfung Technischer Sicherheitseinrichtungen mit Prozessrechnern, MRR 116, Jan. 1973.
- [2] Holló, E.: State and Function Control of Main Equipments and Sub-systems of Paks Nuclear Power Plant's Primary Circuit /in Hungarian/, VEIKI - HTF 46, 1975.

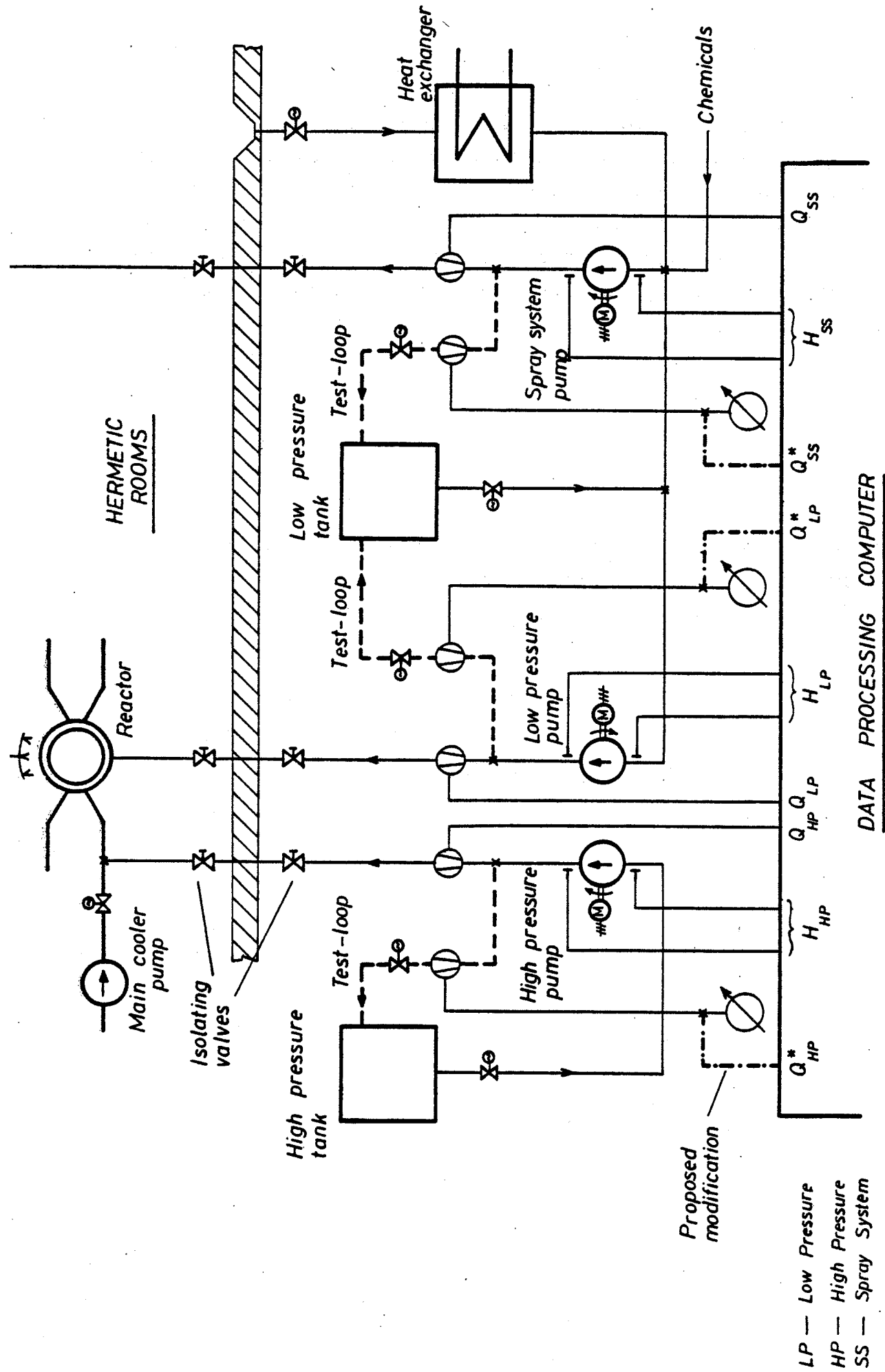
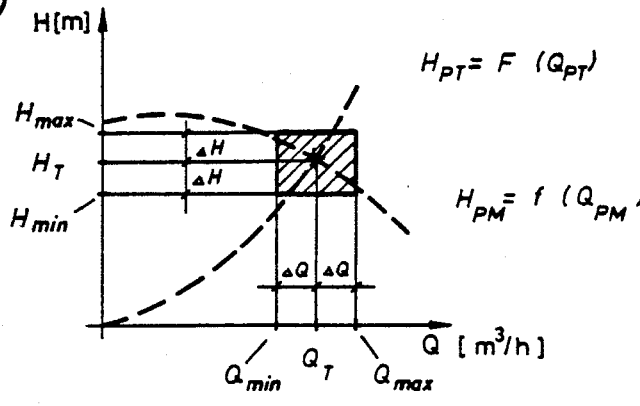


Figure 1.

General scheme of AES subsystems of WWER-440 reactors

a.)



Indexes:
 M - Measured
 T - Theoretical
 PT - Pipe-Tank
 PM - Pump-Motor

$\Delta Q, \Delta H$ — Permissible deviations
 $\Delta Q_M, \Delta H_M$ — Measurement errors

b.)

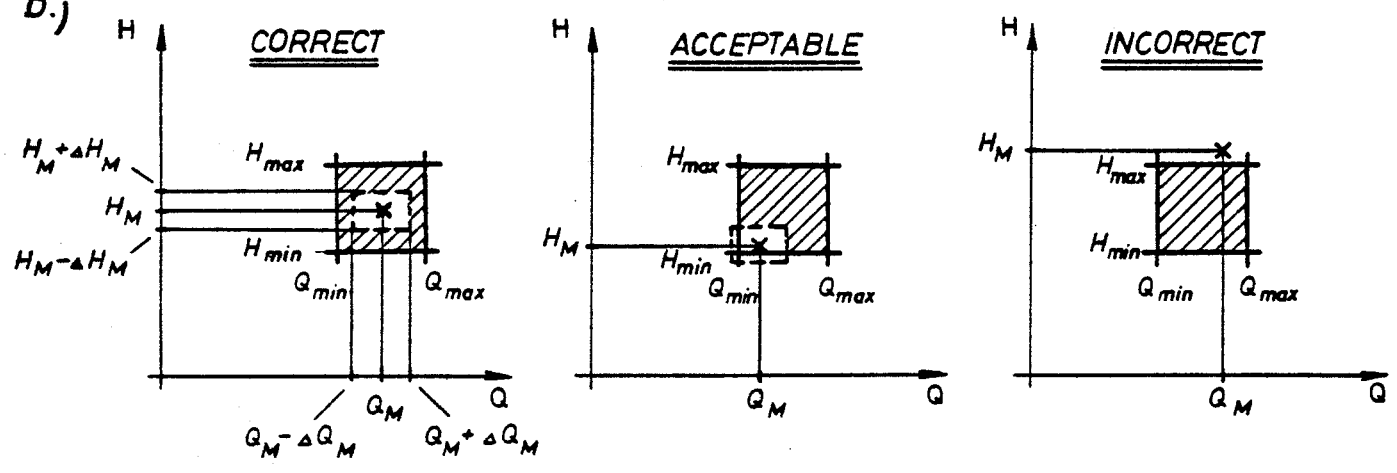


Figure 2.

System control with fixed parameter limits

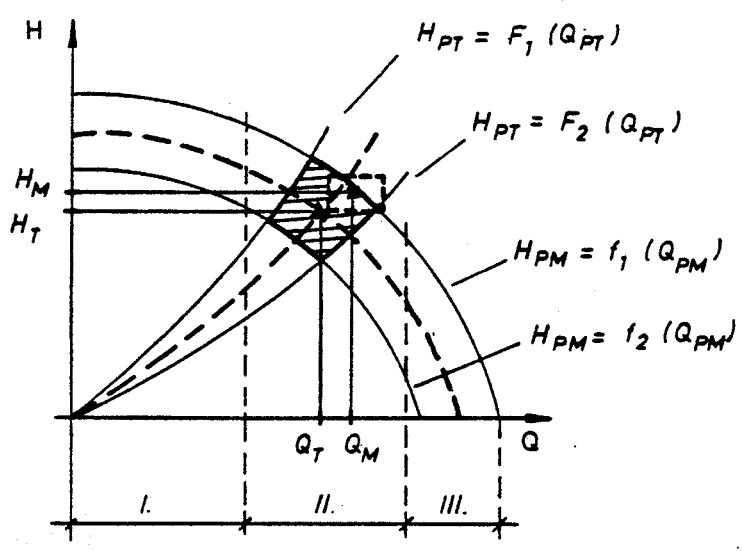
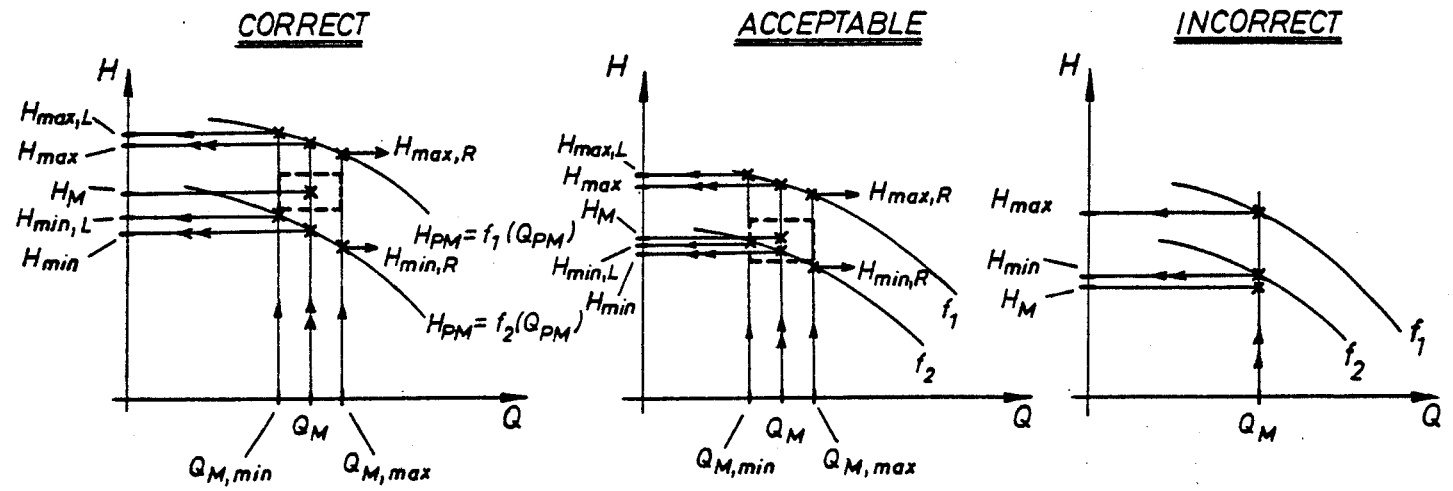


Figure 3.

System control with dynamic parameter limits

a.) Pump-motor



b.) Pipe-tank

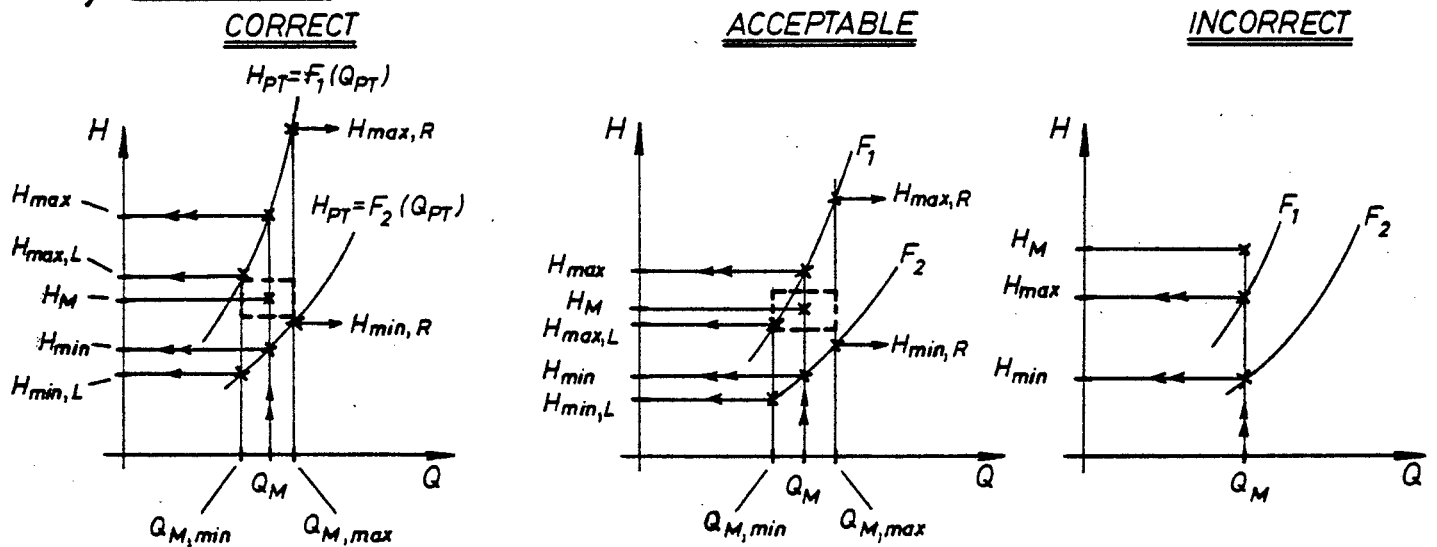


Figure 4.

Equipment control with dynamic parameter limits

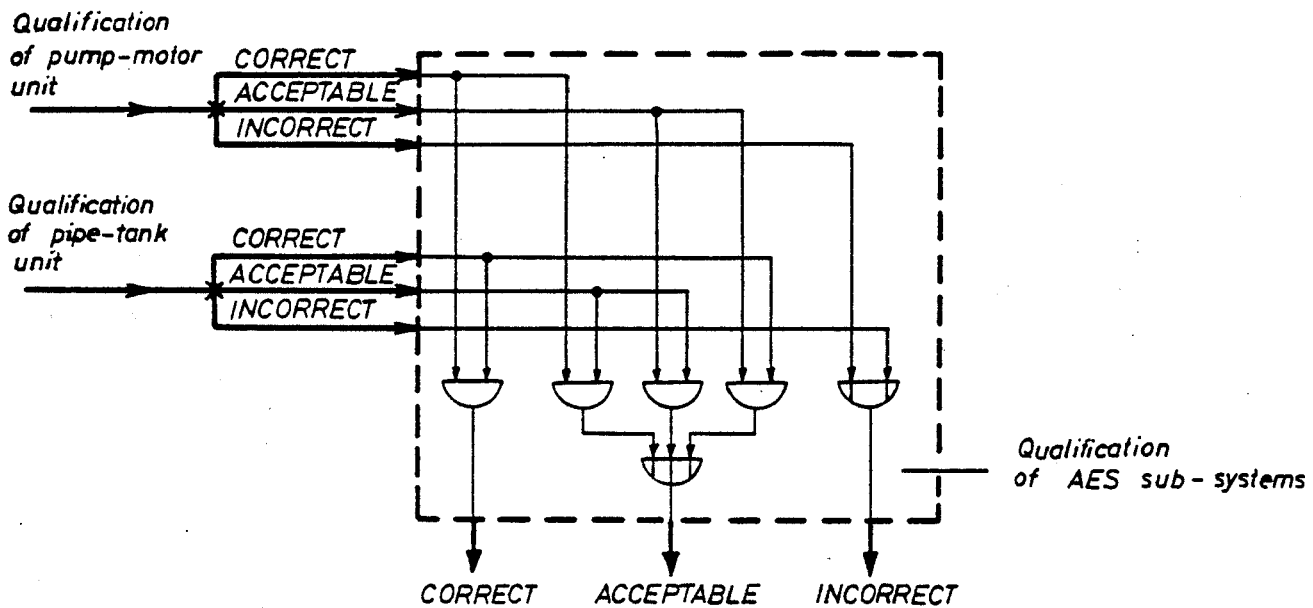
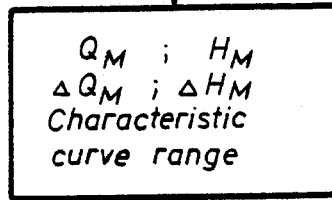


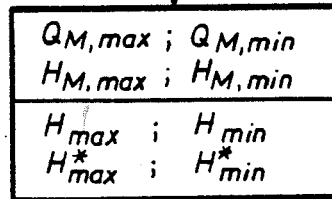
Figure 5.

System control based on equipment qualification

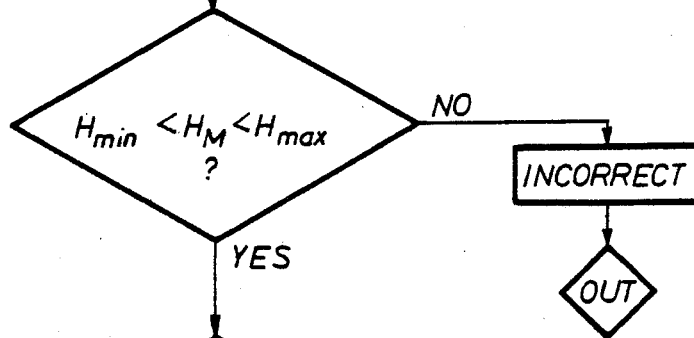
Input data



Determination of parameter bounds



Set point is inside the permissible domain?



Set point with error domain of measurement is inside the permissible domain?

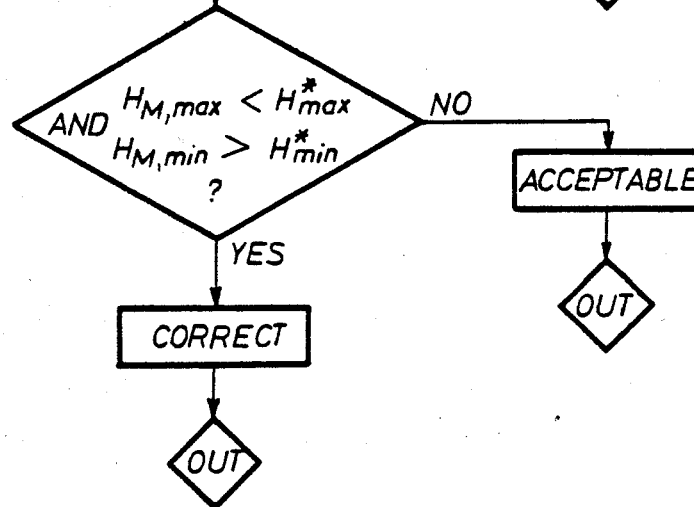


Figure 6.

Algorithm of equipment qualification

$Q_M; H_M$ — Measured set point value

$\left. \begin{matrix} Q_{M,max}; Q_{M,min} \\ H_{M,max}; Q_{M,min} \end{matrix} \right\}$ — Measured set point domain with measurement errors

$$Q_{M,max} = Q_M + \Delta Q_M ; Q_{M,min} = Q_M - \Delta Q_M$$

$$H_{M,max} = H_M + \Delta H_M ; H_{M,min} = H_M - \Delta H_M$$

$\left. \begin{matrix} H_{max}; H_{min} \\ H_{max}^*; H_{min}^* \end{matrix} \right\}$ — Permissible set point ordinate limits (see Fig. 4.)

$$H_{max}^* = \min (H_{max,L}; H_{max,R})$$

$$H_{min}^* = \max (H_{min,L}; H_{min,R})$$

	for pump-motor unit	for pipe-tank unit
H_{max}	$= f_1 (Q_M)$	$= F_1 (Q_M)$
H_{min}	$= f_2 (Q_M)$	$= F_2 (Q_M)$
$H_{max,L}$	$= f_1 (Q_{M,min})$	$= F_1 (Q_{M,min})$
$H_{max,R}$	$= f_1 (Q_{M,max})$	$= F_1 (Q_{M,max})$
$H_{min,L}$	$= f_2 (Q_{M,min})$	$= F_2 (Q_{M,min})$
$H_{min,R}$	$= f_2 (Q_{M,max})$	$= F_2 (Q_{M,max})$

Figure 6. (cont.)

Determination of parameter bounds

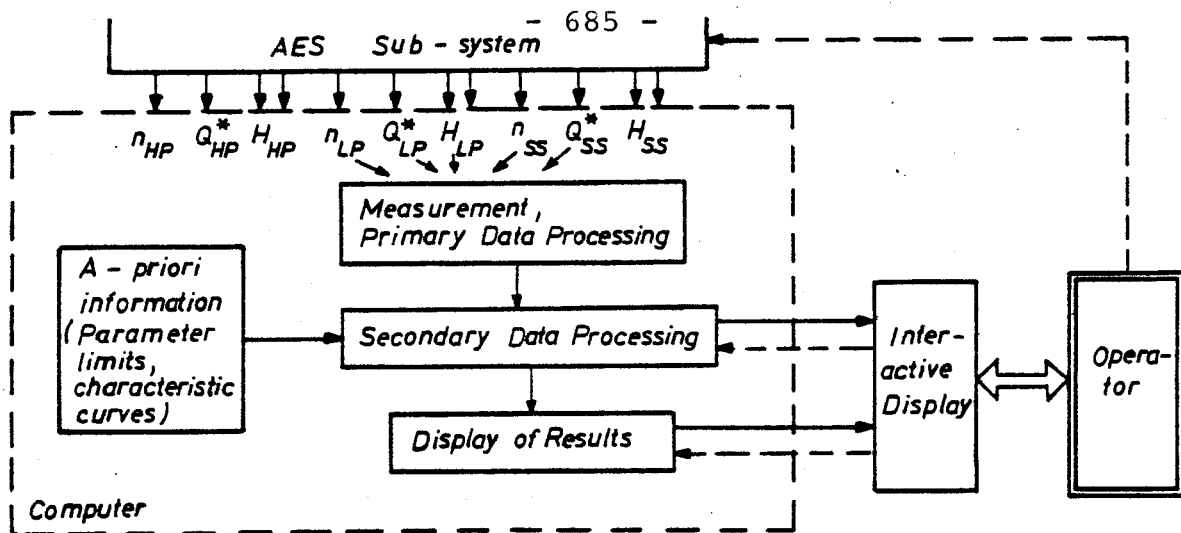


Figure 7.

Block scheme of computerized inspection of AES sub-systems

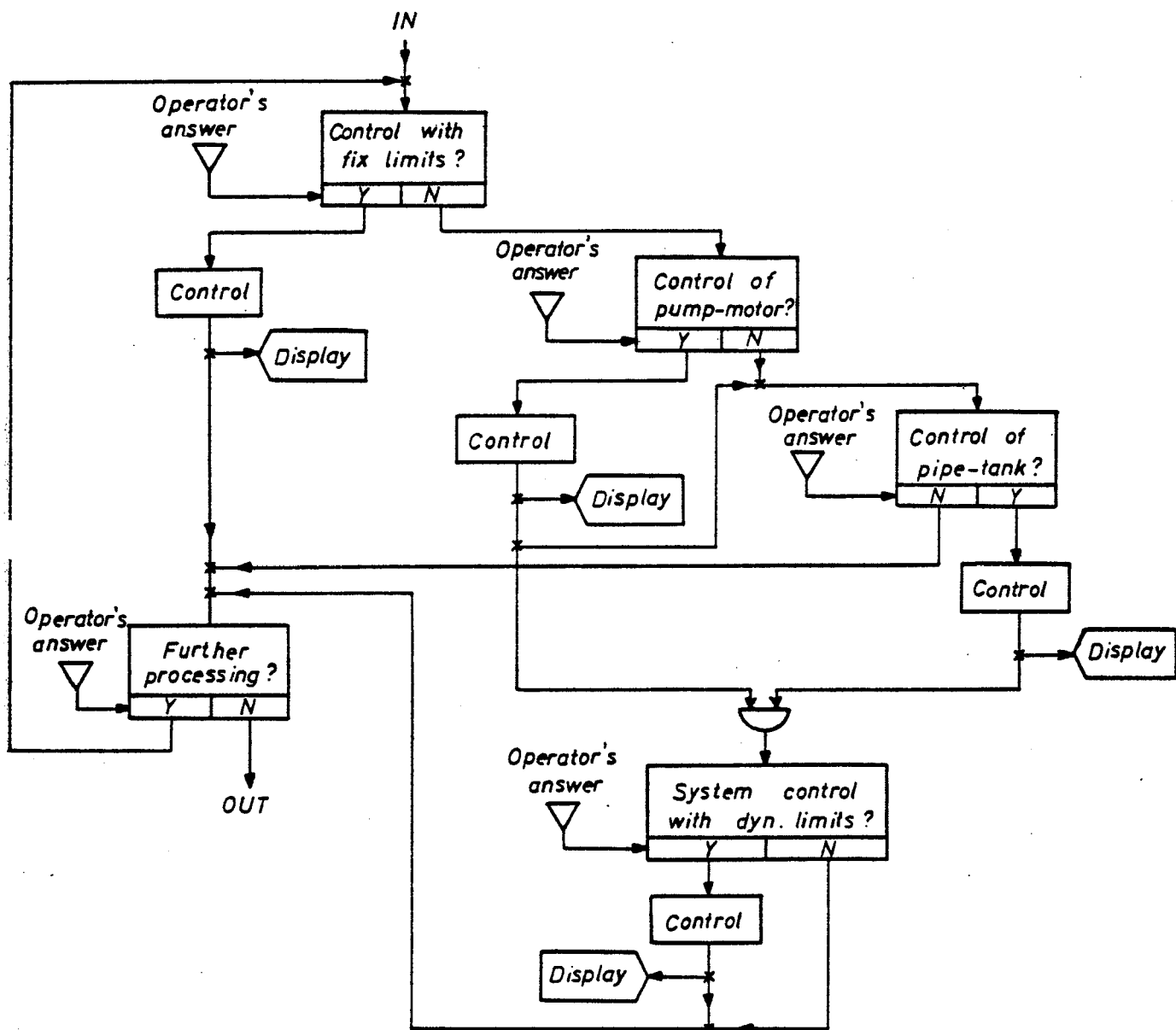


Figure 8.

Flow chart of secondary data processing

CONTENTS

Session VI

MAN-MACHINE COMMUNICATION

Chairperson: E.S. Patterson

Secretary: L. Felkel

E.S. Patterson, L. Felkel SUMMARY OF SESSION VI	689
E.S. Patterson COMMENTS MADE AT THE IAEA/NPPCI SPECIALISTS' MEETING, SESSION VI	695
D. Martin, D. Grensemann A MODERN APPROACH FOR THE REALISATION OF THE MAN- MACHINE INFORMATION SYSTEM	705
F. Frischenschlager ANALYSIS AND PRESENTATION OF ANNUNCIATIONS IN NUCLEAR POWER PLANTS	725
T.J. Bjørlo, J.K. Trengereid COORDINATION OF OPERATOR SUPPORTING SYSTEMS AND PROCEDURES	739
D.M. Hunns PSYCHOLOGY OF COMMUNICATIONS	757
K. Netland MEASUREMENT OF OPERATOR PERFORMANCE - AN EXPERIENCE SETUP	777

L.P. Goodstein

PROCEDURES FOR THE OPERATOR, THEIR ROLE AND SUPPORT

793

J. Decuyper, S. Reynaud, A. Hoepner, Rolland

A GOOD OPERATOR-PROCESS RELATION RESEARCH IN CREYS-
MALVILLE PROJECT

813

Written Contribution

E.S. Patterson

OUTLOOK FOR THE USE OF COMPUTERS FOR PROTECTION
SYSTEMS AND AUTOMATIC CONTROL IN NUCLEAR POWER
PLANTS

829

E.S. Patterson, L. Felkel

SUMMARY OF SESSION VI

Session VI of the specialists' meeting was devoted to "Man-machine Communication". Seven papers were presented, each of which viewed the man-machine communication problem in nuclear power plants from a different angle. As was pointed out in most of the contributions, the problems arising with man-machine communication are not at all new. However, the application of colour cathode ray tubes will change the outlook of future control rooms considerably. The use of process computers for preprocessing plant data and providing diagnostic tools may also have some impact on the role of the operator in modern control room concepts.

The first paper in this session, which was presented by Mssrs. Martin and Grensemann dealt with the construction of systems being ultimately used together with colour cathode ray tubes. It explicitly showed how tools have been developed for simplifying the construction of plant diagrams supplemented with on-line data from the process. The process of designing a system with the presented tools, was outlined as opposed to the conventional way such a system is designed, and its advantages were shown.

The next paper was given by Mr. Frischenschlager. The paper described an analytical method to classify alarms and status indications, in general the process and control system data, into different relevant groups according to activity characteristics and responsibilities of the control room personell. Also here colour CRT's have been used for displaying the alarms and status indications, the classification of the alarms being denoted by different colours.

Mr. Bjørlo presented recent developments in the field of operator supporting systems and procedures at the OECD Halden Reactor Project. Again it was pointed out that colour cathode ray tubes are considered to be a very good tool for displaying information from the process in a comprehensive way. It was also emphasized that a variety of systems supporting the operator (among them the disturbance analysis system and the core surveillance system) need integration in an advanced control room concept. Such an advanced concept was proposed and exists as an experimental facility at the Halden Project.

Mr. Hunns approached the problem from a psychological point of view. The paper outlined how mental models can be used to find out psychological error mechanisms which account for many accidents. A practical test has been carried out and is described in the paper.

The experimental set-up for the measurement of operator performance has already been mentioned in Mr. Bjørlo's paper. Mr. Netland now described the experimental set-up in detail and how the measurements of operator performance has been carried out. Factors are described which are influencing the operator performance. The paper also describes a simulator for a pressurized water reactor which was used for performing the studies.

The paper by Mr. Goodstein was about written procedures for the operator. It describes the different problems arising with the construction of procedures to achieve the desired goals. The paper also shows how the procedural support can be computer-based.

The last paper in this session was presented by Mr. Decuyper which described the operator process relation research for the french plant of Creys-Malville. Also here it was shown how colour cathode ray tubes can be successfully utilized. The operators have been subject to a special training program which also included training on a simulator which could simulate incidental or accidental situations.

All the papers pointed out the applicability of colour cathode ray tubes for conveying the information needed by the operator in due time. However, since the relations between man and machine are utterly complex, the session showed that considerable efforts have to be made in the next few years to obtain results which are readily applicable in nuclear power plant control rooms.

E.S. Patterson

COMMENTS MADE AT THE IAEA/NPPCI SPECIALISTS' MEETING,
SESSION VI

THE NEED FOR CRITERIA
AND PHILISOPHICAL DEVELOPMENT
FOR HUMAN FACTORS ACCOUNTABILITY
IN NUCLEAR POWER PLANTS

COMMENTS MADE AT THE IAEA/NPPCI
SPECIALISTS MEETING
SESSION 6
DECEMBER 7, 1979
MUNICH

by

E. S. PATTERSON
BABCOCK & WILCOX CO.
LYNCHBURG, VA., USA

SUMMARY

The following is not a scientific paper but rather a commentary for the purpose of identifying specific areas where there is a serious need for criteria and philosophical development that will permit designers to move rapidly to account for human factors in nuclear power plants. While only a few specific problems are discussed, it is recognized that the need for engineering criteria exists for a much broader range of human behavioral problems.

DISCUSSION

Recent events in the USA has created an atmosphere in which many people feel that we must quickly improve the man-machine interface to reduce the probability of operator error in nuclear power plants and to improve the chances of the operator having all of the important factors and controls available in a form that will permit him to quickly identify the state of the plant and correct any situation of safety significance. The sudden demand to quickly solve human factors problems has caused me to be concerned that we may rush into implementing solutions before we fully understand the full significance of what we are doing and fail to recognize that specific solutions may raise new problems of human behavior. In other words, before a proposed human engineering solution is implemented, its full potential impact upon human behavior should be assessed to make sure it does not initiate more problems than it corrects. We need a well understood philosophy to guide us in such matters and none exists today.

Design Approach

At this moment, there is no agreement on how the designer should approach his task of accounting for human factors in a nuclear power plant. It is my suggestion that the starting point should be an understanding of the human behavior of the society that inhabits the nuclear power plant. This includes an understanding of the plant organizations, the responsibility and authority of each member of the society and in what way each member of the society interacts with every other member and in particular how these interactions may affect the behavior of the people who are important to the safety of the plant.

Operator

The designer must completely understand what is expected of the plant operator, his authority, and his function for every operating state of the plant. I suggest that we need a consensus agreement of what the operators function should be together with an identification of the authority and support he must have in order to properly execute his function.

Operator Response

We can design for two basic kinds of operator reaction to a stimulus: (a) an operative conditioned reaction⁽¹⁾ approximately reflexive, (b) a stop, think, analyze, apply intellectual learning and form a reaction plan, reaction.

If we choose to design for an operative conditioned response it means that at any time the stimuli occurs, the operator will respond without questioning the validity of the stimuli and without considering the logic or validity of his actions. If the stimuli are in error or the condition response incorrect, the operator will still perform his conditioned response with no pause to consider the validity of what he is doing; if he doesn't react in this manner, then the operative conditioning process was faulty.

If we choose to design for a stop-analyze the problem response we must accept the probability of faulty reasoning and the distracting effects of such things as stress and confusion. On the positive side, if the original stimuli are in error, or if the standard response is incorrect, there is a good likelihood of the operator discovering the error and initiating the correct response. Training the operator to analyze the problem before responding also increases the probability for a correct response to an unthought of problem.

There are clearly the elements of a dilemma here: with operative conditioning, the response is assured but the instrumentation initiating the stimuli must not error, the predetermined response must be the right one and all responses must be predetermined. With a stop-analyze the problem philosophy, the opportunity exists for the operator to discover and correct for errors; however, the probability exists for stress and other factors to impair the operators mental power. The decision to invoke one or the other of these philosophies of operator response as the basis for a given design should not be left to the individual designer. Therefore we should seek a consensus agreement of when and to what extent we are going to invoke operative conditioning as a design basis.

Operative Conditioning

Operative conditioning works as long as the proper response to a given stimuli results in a positive reward. In this discussion, it is assumed that the response to a false stimuli, thought by the operator to be valid, will always in some way result in a negative reward. Therefore, an operator who is trained to respond in a specific manner to a specific stimuli, an alarm or other indication, will fail to respond correctly after the occurrence of a certain number of false alarms. If the alarm or indication is in error a certain number of times, the operator may even ignore it. Precisely how many times stimuli may be in error without affecting the operators response is not well defined. We must agree upon the frequency that can be tolerated in stimuli errors.

Assume that an alarm error occurs frequently enough to create operator mistrust and possibly even cause the operator to ignore it. Assume also it is now corrected and no longer actuates in error. What must be done to restore the operators

confidence and assure that he will once again respond in the desired manner? We need an answer which we can all agree to.

This is by no means a satisfactory discussion of operative conditioning and the events that can occur in an operating plant that may affect the operators conditioned response or condition the operator to respond in an unintended manner; however, I suggest that this phenomenon of human behavior should be thoroughly understood by every one working in human factors accountability.

Automation

It has been recognized for a long time that an extensive use of automation will reduce the chance for human error and the need for human skills. Automation reduces the need for the operator, removes him from the process, and creates its own special problems not the least of which is operator boredom. The assignment of meaningless keep-busy tasks on the assumption that they will keep the operator alert is not an answer and can lead to other behavioral problems. Before we commit to a high level of automation, we should seek a concensus solution for the boredom problem.

If the operators function, which we have not agreed to, is to take manual control of the plant when the automatic control systems fail (I consider protection systems automatic control systems), then we must agree upon how many automatic functions will absolutely be operable for any given state of the plant. Remember that in a highly automated process the operator will rapidly lose his manual operating skill from simple disuse. This is no trivial problem and we must have an agreed to concensus of what I call, automation failure criteria.

Software Error

The technological power of computers has rapidly increased since the May 1976 IAEA/NPPCI Specialists Meeting on the Application of Computers in Protection and Control; however the issues of 1976 centering upon the detection of software errors are still with us. (I remind you that the primary origin of software errors is human error.) Virtually no progress has been made in proving that software errors absolutely do or do not exist in a program. The rapidly rising demand for the reduction in the probability for human error cannot be met without the extensive use of computers for control and safety related functions, therefore the software error issues of 1976 must be quickly resolved if we are to significantly reduce human error.

Judgement Criteria

A device is proposed or designed to aid the operator and reduce human error. How do we judge the merits of the device? How do we measure whether or not its usage will sufficiently reduce the probability of human error? Once accepted and installed in a plant what kinds of problems arise when the device fails at a critical time? The need for an acceptable judgement criteria is clear.

Scope

While the operator has been the principal subject in this discussion we must not overlook the fact that he is not the only human who must routinely interface with the plant machine. The maintenance personnel have their own human factors problems as do the radiological health and security personnel. To what extent should we apply human factors engineering to the total nuclear plant? How far should we go? This is a problem that again requires a consensus solution and criteria.

CONCLUSION

Human factors accountability in nuclear power plants is a broad subject. If we are to make rapid progress in this field we need an extensive development of philosophy and criteria to guide the designer in executing his task. It is suggested that work to satisfy this need begin by considering the plant as a small society and applying our knowledge of human behavior to all the human activities within the plant that may affect plant safety. This work should then form the basis for the development of criteria that can be understood and applied by the designer. The technology for reducing human error, will be computer technology; therefore, we must move quickly to resolve the software error issues of 1976.

Acknowledgement

The author wishes to acknowledge the valuable assistance given him by Mr. William J. Patterson, a practicing psychologist with Mineral Springs Industries of Blue Ridge, Georgia.

(1) NOTE: In this discussion, the author uses the terms operative conditioning and conditioned response to refer to the process whereby a human is trained to behave in a specific predetermined manner, to take specific invariant physical actions in response to specific stimuli. The assumption is that the operative conditioned response may be developed to the level approaching a reflexive action eliminating any chance for logic and reason to play a part in the response process. It is recognized that to be effective an operative conditioned response must be followed by reinforcement, a positive reward for the doer. The author is fully aware of the broader view of operative conditioning held by many Behavioral Psychologists and apologizes for this narrow approach.

D. Martin, D. Grensemann

A MODERN APPROACH FOR THE REALISATION OF THE MAN-MACHINE
INFORMATION SYSTEM

Specialists' Meeting on "Procedures and Systems for Assisting an Operator During Normal and Anomalous Nuclear Power Plant Operation Situations"

5. - 7. December 1979, Munich

A MODERN APPROACH FOR THE REALISATION OF THE MAN-MACHINE INFORMATION SYSTEM

D. Martin

D. Grensemann

BROWN, BOVERI & CIE Mannheim

1. INTRODUCTION

In particular in the area of nuclear power plant a new approach is required to problems in the control engineering resulting from:

- fundamental reconsideration of the safety philosophy
- the long project implementation time-spans with changing specifications.

It has been recognized that improvements in the field of operator communication and control room engineering will contribute directly to the optimisation and safety of the plant. These improvements are required firstly due to the ever increasing quantities of data to be processed in the control system and secondly to attain a fuller integration of the operator into the control process.

The operator can be both the weakest link as well as the strongest link in the control system depending on how he is informed, what possibilities he has to interpret this information, how he reacts (training and integration) etc.

The man-machine interface in all its phases is the key to the link.

The paper covers the background which allows a new approach, the description of this approach for the man-machine interface, the advantages expected and finally the future of such an approach.

2. BACKGROUND

The man-machine interface has been increasingly supported by computer systems and colour display units (VDU's) since 1970 but the methods used today mostly evolved in the early seventies. A new approach is required for the eighties. This is however only possible based on experience gained in the past and due to the availability of new technology at the present.

The factors influencing this development are as follows:

- Higher demands on the man-machine interface due to the processing of larger quantities of data but with presentation in a more concise form (no ambiguities). Can this component of the control system also be made fail-safe?
- The uncertainty as to new requirements related to the man-machine interface. This is particularly the case with nuclear technology due to licensing problems, improving safety standards etc.
- The prodigious advances in computer technology have resulted in dramatic decreases in system costs with simultaneous increases in performance. The "silicon chip revolution" has had a great impact on the control system - in particular on devices such as coloured displays.
- Increasing costs of software engineering offset many of the benefits obtained by improved hardware. This effect has also to be counteracted by new methods.
- Fault tolerant computer systems can now be effectively implemented which allow a full integration of the computer-based information system into the control system. These systems are based on multi-computer configurations with distributed functionality.

- Software engineering has matured to the point where a truly structured approach can be applied. The difficulties experienced with the interface between the functional requirements and the software solution are better understood.

We now have practical systems at our disposal which go beyond the current requirement of control engineering. But to fully benefit from these advances we have to bridge the gap between the software engineer and the unknowns of the plant operator interface - a modern approach is required.

3. A MODERN APPROACH

A step is required which not only utilises the latest technology but is also open-ended for the control engineering advances to be expected in the next decade - as stated previously primarily in the field of man-machine communication.

We believe this new approach is the development of computer based tools for a defined field of activity as opposed to dedicated solutions to specific individual problems. This tool is characterised by, and covers the previously stated areas as follows:

- The tool is produced by computer specialists with an understanding of the man-machine interface problem.
- The tool will be used by control system engineers, planners, plant operators etc. without specific computer know-how.
- The tool thus serves to bridge the gap between the two disciplines
- Since specific solutions are not generated new forms of presentation and selection, data quantities and qualities, recognition methods etc. can be implemented without further expensive software engineering.

The man-machine interface is in development using this approach due to the experience gained in both nuclear and fossil power plant with computer based information systems utilising colour display communication.

The advantages are stated in section 5. of the paper and some thoughts to other application areas which could benefit from this approach are given in section 6.

4. A TOOL FOR MAN-MACHINE COMMUNICATION

It is possible to summarise the basis to the man-machine interface into 3 conditions:

- high flexibility is required at the present and increasingly so in the future
- there is a large unexploited potential for computer-based information-systems using colour display techniques.
- the planning and implementation effort for this application with current methods can be radically reduced.

The tool considered is a combination of three major components (see also Fig. 1.)

- a mini-computer hardware and basic software system which
 - . is adaptable to multi-computer configurations,
 - . operates as a self-sufficient general purpose computer with good data handling properties
 - . has characteristics appropriate to a high-performance process computer
- a software package which defines the functionality and has defined interfaces to a data acquisition system as well as to the planning tasks

- a high performance colour video display controlled by a micro-computer, based on television raster techniques, and supporting a wide range of operating elements [1].

The tool has been given the name VISCOMP - VISual COmmunication Man-Process. Dependent on the project implementation phase VISCOMP functions either autonomously (planning and definition phases) or in conjunction with a data acquisition system [2] during the operational phase on the plant. The relationship of the required components to the project phases is illustrated in Table 1.

The functions of VISCOMP and their relationships to the project implementation phases are as follows:

- Functions supported during design and planning phase

- . Picture generation. The required output presentations are structured directly on the display i.e. the picture layout and construction.
- . The pictures are adapted to the specific project, that is the connection is made to the process data and the output conditions (e.g. colour, flash, new symbol etc.) are defined, i.e. the parameters are defined.
- . The completed pictures are "compiled" and checked for plausibility. They can now be optically accepted and the documentation for each picture with its complete definition - including non-visible conditions - is documented automatically by the computer.

- Functions supported during the integration and commissioning phase

- . picture correction in limited form is possible on the on-line system e.g. parameter definition. Restructuring is only possible if a full complement of off-line hardware is available.

- . the archiving of completed and checked pictures, logging of modifications
 - . the selection of "commissioning pictures" - specially defined outputs to support the commissioning engineer, these include for example the output of scanned variables in raw format, internal parameters etc.
- Functions supported during the operational phase
- . picture selection via functional keyboard
 - . picture selection via interactive "marking" of previously defined targets
 - . by appropriate planning it is possible to step through picture sets by "marking" fault areas (disturbance tracking)
 - . optical scanning of large pictures i.e. areas longer than one screen size (rolling map technique)
 - . allocation of outputs to selected display monitors
 - . cyclic and spontaneous updating of the selected pictures
 - . evaluation of pre-defined conditions

The main feature of VISCOMP is that one system (hardware components and software) is used at all times. To illustrate the working and ease of use of VISCOMP some of the features named above will now be described more fully.

Picture Structuring

Figure 2 illustrates the interactive definition of a picture using a light-pen, a virtual keyboard (blended into lower region of screen) and an α -numerical keyboard.

A picture size can be a multiple of a screen size. This enables large quantities of data and areas to be defined whereby at output time the operator is only confronted with a section of the picture at any one time.

Overview pictures can be scanned over e.g. with a track-ball.

A picture consists of a combination of single items which are classified into 4 levels of detail as follows:

- The smallest item is a single addressed point on the screen. In this case the screen consists of 448 x 288 points (total 129024), whereby a picture (= multiple screen) can contain 1024 x 1024 points. This type of item is used dynamically to form continuous curves e.g. as illustrated in figure 7 or for static characteristic boundary envelopes e.g. for pumps.
- The screen is divided for most purposes into a matrix of 32 lines each of 64 columns. Each position thus defined consists of a symbol or character in a 7 x 9 point matrix. The generation of such an item is illustrated in figure 3. VISCOMP uses up to 256 such items, whereby as can be seen in the example 64 are usually dedicated to the upper-case character set and the remaining 192 are used for project specific SYMBOLS. Libraries of such symbol sets are produced interactively and referenced later by symbolic name.
- The third level of item is the so called SHAPE or ELEMENT. A SHAPE is a defined set of connecting SYMBOLS. For example plant aggregates and specific components can be defined as SHAPES - an example is given for a turbine in figure 4, in this case a 7 x 5 combination of SYMBOLS:

Libraries of such SHAPE sets are produced interactively and referenced later by symbolic name. An ELEMENT is also presented as a set of SYMBOLS but has dynamic properties, examples are:

- Text strings to be defined later
- Fields to contain analog and binary process signals
- Window areas to contain sequence of events messages
- Window areas to display analog variables in the form of curves
- Bar chart fields in vertical and horizontal directions.

- The highest level of item is the generation of the total picture itself. This is illustrated in figure 5 where SYMBOLS and SHAPES are combined with powerful editing functions to form the PICTURE. ELEMENTS will also be structured-in to complete the PICTURE so that the end result for the operator then appears as in figure 7 or 8 (inclusion of e.g. text, analog variables, bar charts, curves and alarm messages).

Parameter Definition

Parameters comprise those data which are specific to a particular project, and take two forms namely:

- Parameters which have to be modified at any time e.g. technological limits, log configurations, signal group definitions etc. These parameters are mainly applicable to sets of data.
- Parameters which are specific to a particular picture and complete the picture definition by connecting project specific values to PICTURE ELEMENTS.

In the first case the parameters are modifiable in all project phases whereby in the second case they can only be set before PICTURE compile time. However in both cases the means of access and "parametering" is the same, namely by the use of questionnaires and a "fill-in-the-blanks technique".

An example of a questionnaire for the first type of parameter is given in figure 6. Operating is exclusively by the means of a numerical keyboard. In the case of PICTURE definitions this "parametering" can be executed at the time of the PICTURE structuring or at a later phase.

System Operating

A number of means of interactively communicating with VISCOMP during the operational phase are considered. They can be grouped into two types namely actions which come from outside VISCOMP itself and those which are possible exclusively within VISCOMP.

The first type covers actions initiated via:

- functional keyboards, e.g. picture select, acknowledge, clear screen etc.
- directly from the plant status e.g. automatic picture select, acknowledge, output reconfigure etc.

The second type covers actions initiated via:

- numerical display keyboard for "parametering" (background functions)
- by "marking" directly in display pictures
- by "marking" in displayed virtual keyboards.

The last two mentioned related to "marking" are worthy of special note since they offer the highest flexibility for the future. Predefined fields in the picture will be allocated functions in the picture planning phase e.g. select new picture, acknowledge status,

page-back, page-forward etc. These function will then be initiated by "marking" the predefined field by positioning a Cursor (blinking marker) in that field. The positioning is made by Cursor Positioning Keys (8 basic directions)

- Track-Ball, Joy-Stick (all directions)
- Touch Panel (later development)

These means are independent of fixed hardware keyboards (problem of modification and expansion).

An example is given in figures 8 and 9. In the overview picture (figure 8) a disturbance has occurred in the preheater (notified by change of colour to red). By "marking" anywhere within the outline of the preheater (previously defined) the next picture in the set will be selected on the same screen (figure 9).

The disturbance will be shown in greater detail; assuming there are further pictures in the set these can then be selected in a similar manner. A form of disturbance analysis is thereby achieved optically.

In exactly the same manner virtual keyboards can be generated i.e. marker fields are defined with descriptive texts to state the required action. The contents list type of selection can thereby be accomplished with grouped sets of picture names and facilities to page forwards and backwards through the contents.

One of the greatest impacts VISCOMP will have is in the area of savings in effort to implement a computer-based information system. Not only will the effort be greatly reduced but, the system integrity (and thereby the overall plant safety) will be greatly improved simultaneously. A number of project phase interfaces will be eliminated or simplified. This feature of VISCOMP is illustrated in figure 10.

VISCOMP is a natural progression from its predecessors. Two forerunner methods were used in the past, the list below shows their characteristics. It should also be noted that pictures in the past were also much simpler than those which are implemented with VISCOMP.

<u>Method</u>	<u>Time of Use</u>	<u>Effort/Picture</u>
Programming individual pictures	Late 60's, early 70's	2 - 4 weeks
Generating pictures based on a special display language and simple software tools	Mid 70's, late 70's	3 - 5 days
VISCOMP, complete tool	Early 80's onwards	1 - 4 hours

The system integrity obtained by elimination of too many intermediate steps and by automatic production of the end documentation is of particular importance in nuclear power plant.

5. ADVANTAGES TO THE PLANT OPERATOR

The operator benefits from VISCOMP in both the project implementation phase as well as the operational phase.

The main advantages during implementation are:

- Operators can be actively integrated into the planning phase - pictures can be generated, demonstrated, evaluated and accepted with minimum complications
- Training can begin during planning; feed-back from the operating personell can be incorporated easily at this and all subsequent phases. An "optical-simulator" can be produced
- Training and over specialisation of operators are reduced by using one tool for all man-machine interface activities.

During system operating the advantages to the operator are:

- new situations and operating procedures can be incorporated into the information system
- the system can be planned to guide the operator during disturbance analysis and for special tests.
- a wide range of operating components and philosophies are supported
- pictures consist of visible and "non-visible" information output, i.e. the operator only sees perhaps 10 - 20 active variables whereas the picture itself can be processed and influenced by many more say 100.
- the documentation always corresponds to the output presentations.

6. THE FUTURE OF THIS APPROACH

The approach adopted of developing a tool means that other computer-based application areas can also be supported by VISCOMP - by interfacing to the corresponding system. Some examples possible are as follows:

- structuring of other presentation forms via display (x-y plotter Magnetic-Tape, logs etc.)
- structuring and operating for simulations (power plant, reactor, control room, control system etc.)
- structuring and output from data analysis systems - interfacing to a historical data bank. In particular here an adaptive and interactive communication system is required.

With experience gained with the VISCOMP tool it is expected that many new areas will open up to this approach.

References

- [1] PROCONTROL Description of the PAN 2
Display System, BBC Pub.No. DKW 80914 E

K. Hillmer and M. Müller
PAN 2 Colour Display System
Brown Boveri Review 66, 1979 (10)

- [2] PROCONTROL Process Computer System
PRAUT[®] System Description, BBC Pub. No. DKW 80924 E

P. Hanbaba and F. Mötz
Control of Power Plants with the aid
of processed information
Brown Boveri Review 66, 1979 (10)

V I S C O M P

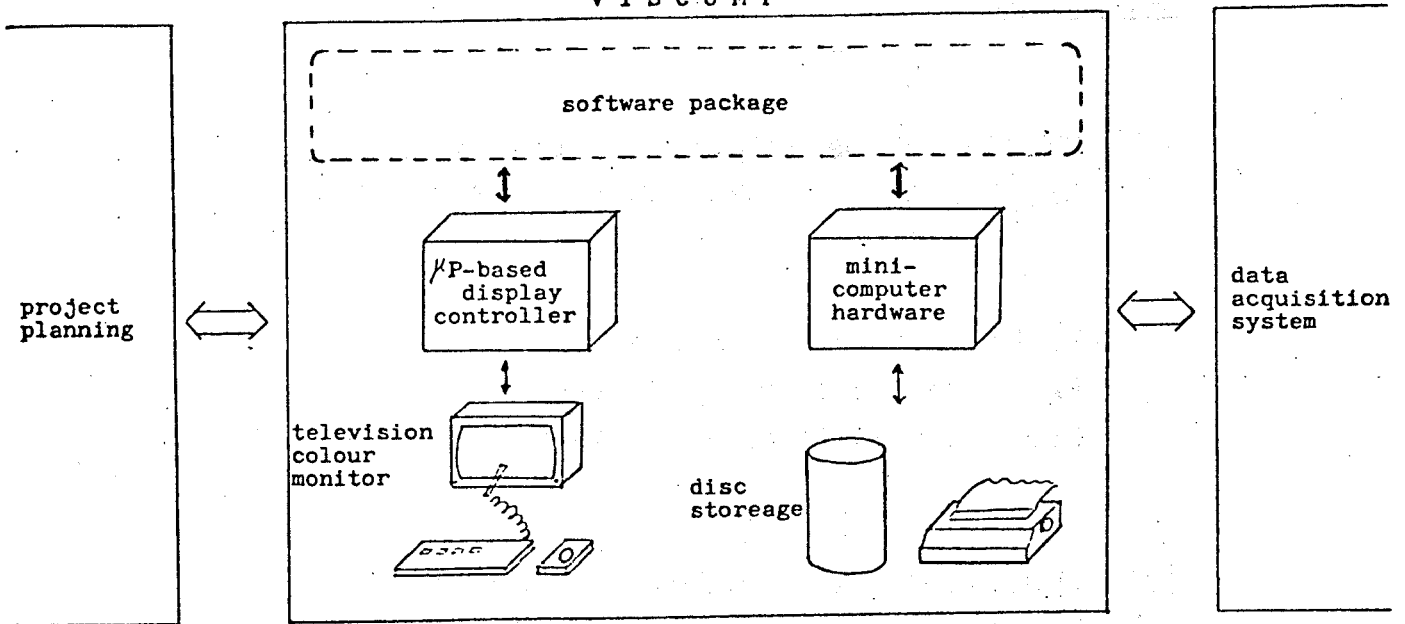
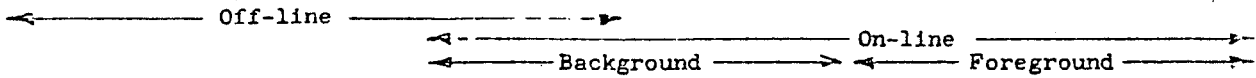


Figure 1 The major components of VISCOMP, illustrating the two external interfaces

Phases

Components	Phases					
	Design & Planning	Acceptance & Documentation	Integration & Commissioning	Parameter Correction	System Operating	Information Presentation
Off line Mini-Computer	X	X	(X)	X		(X) ¹
On-line Mini (Process) Computer			X	X	X	X
Hard Copy (Doc.)	X	X ²		X ²		X
Colour Display	X	X	X	X	X	X
α-num. Keyboard	(X)	(X)	X	X	(X)	
Functional Keyboard			X		X	
Light Pen	X	(X)	(X)			
Touch Panel	[X]				[X]	
Track-Ball, Cursor Pos-Keys	(X)	(X)	(X)		(X)	



- () = option
- [] = farther development
- 1 = optical presentation without dynamic process data
- 2 = screen image dump supported by printed logs with additional information

Table 1 The use of the individual VISCOMP components related to the project implementation phases.

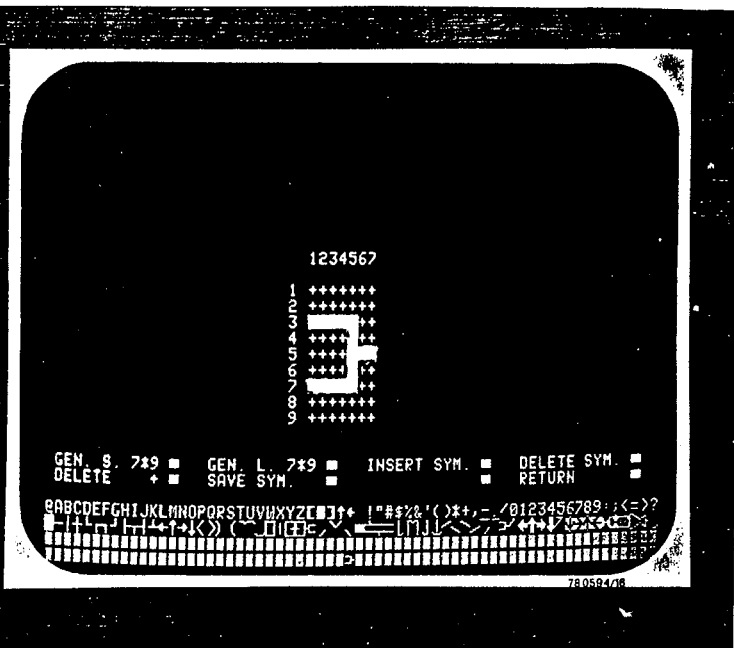
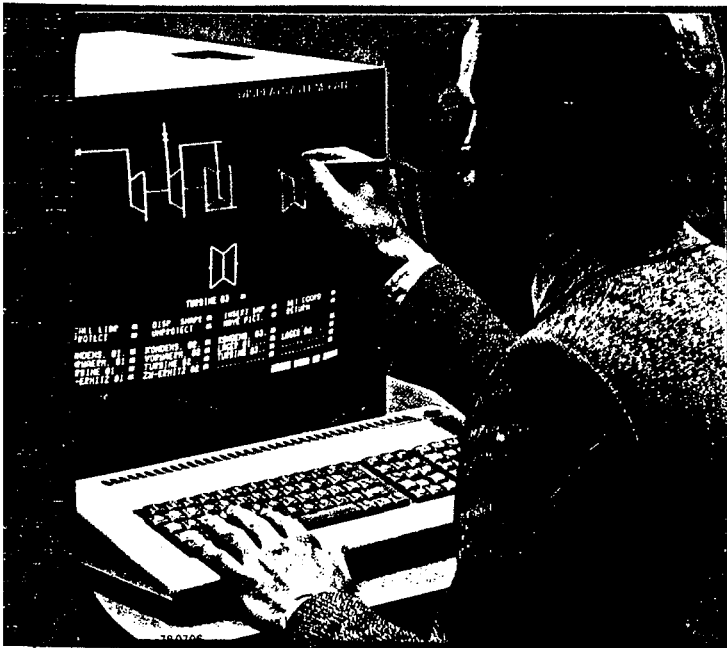


Figure 2
Interactive structuring of a PICTURE using a light-pen

Figure 3
Generation of a SYMBOL in the 7 x 9 point matrix

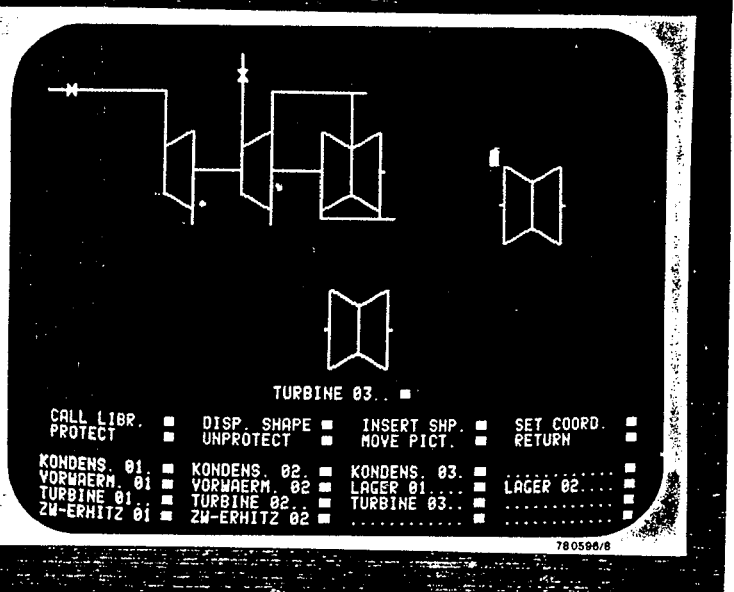
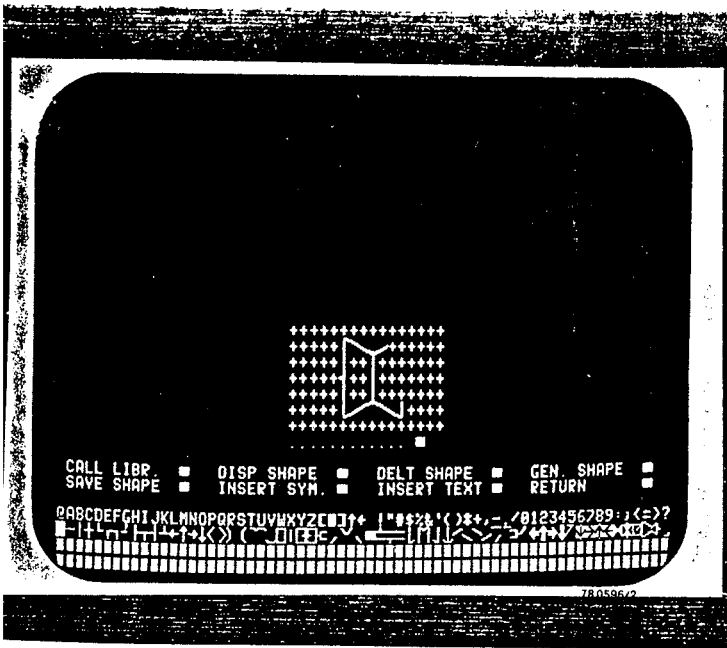


Figure 4
Generation of a SHAPE by the combination of SYMBOLS

Figure 5
Combining SHAPES to form a PICTURE

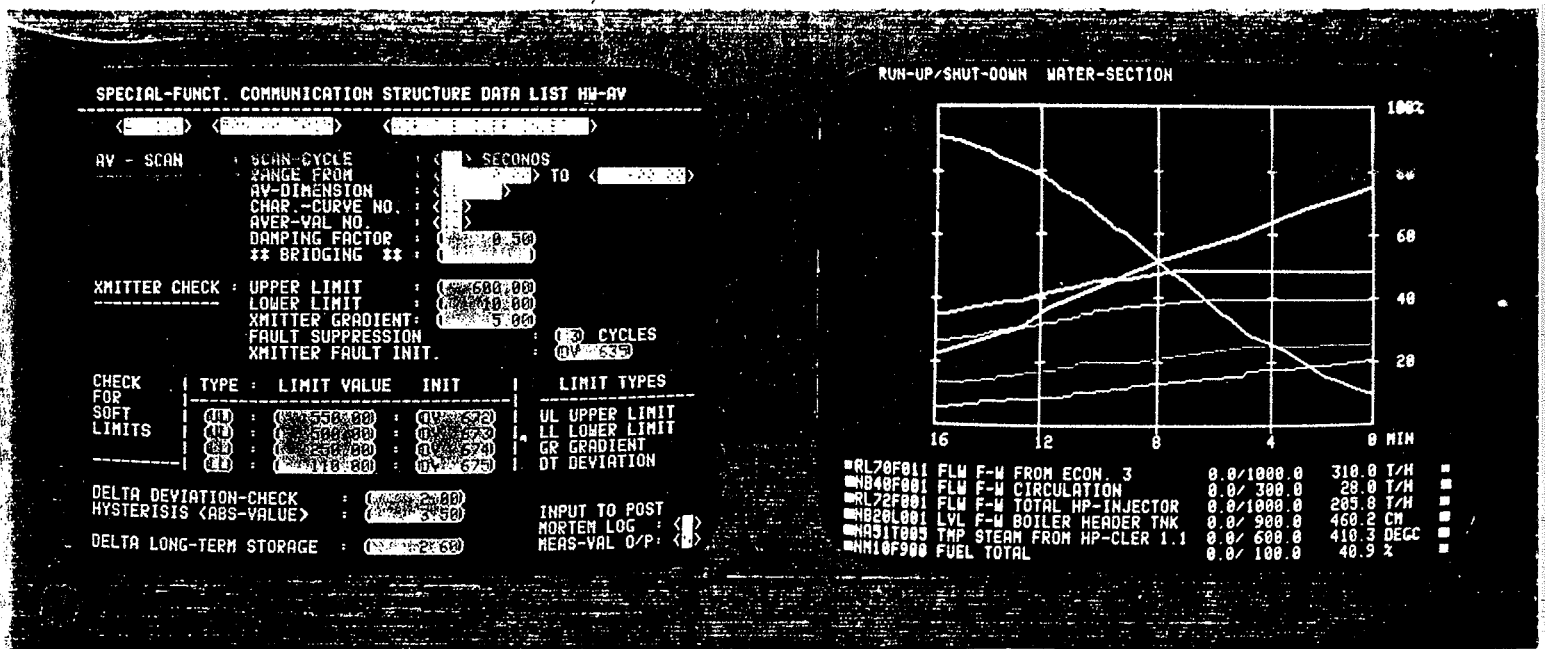


Figure 6
 Example of a questionnaire for "parametering"

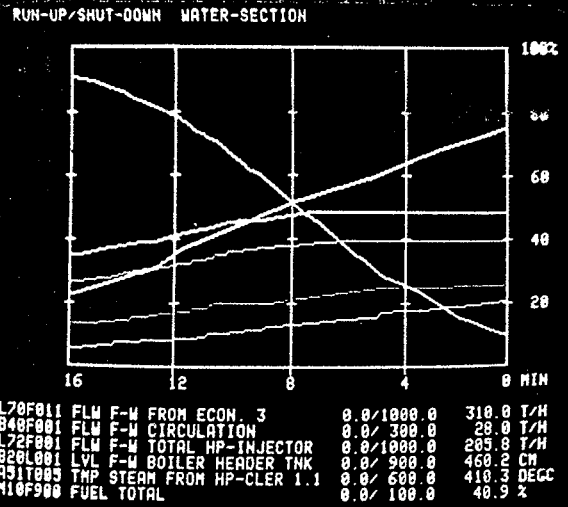


Figure 7
 Example of a PICTURE using point addressing for curves

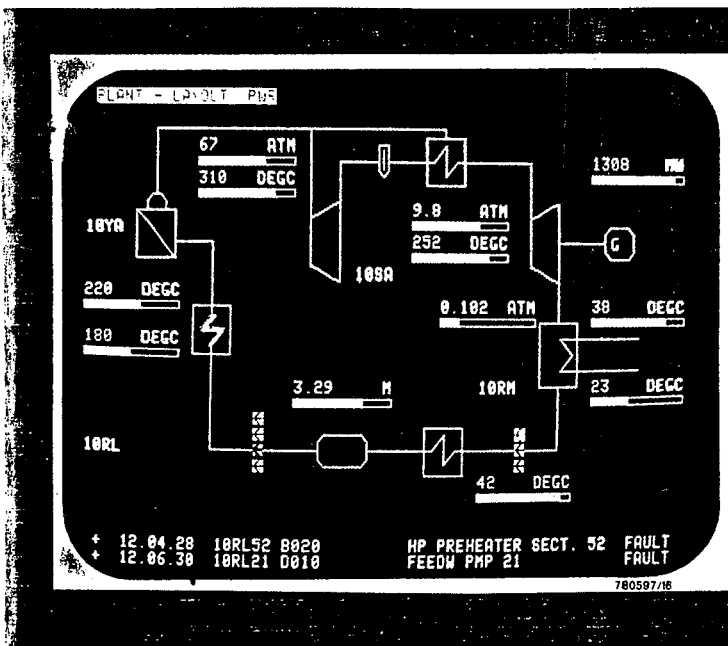


Figure 8
 Overview PICTURE for a nuclear plant

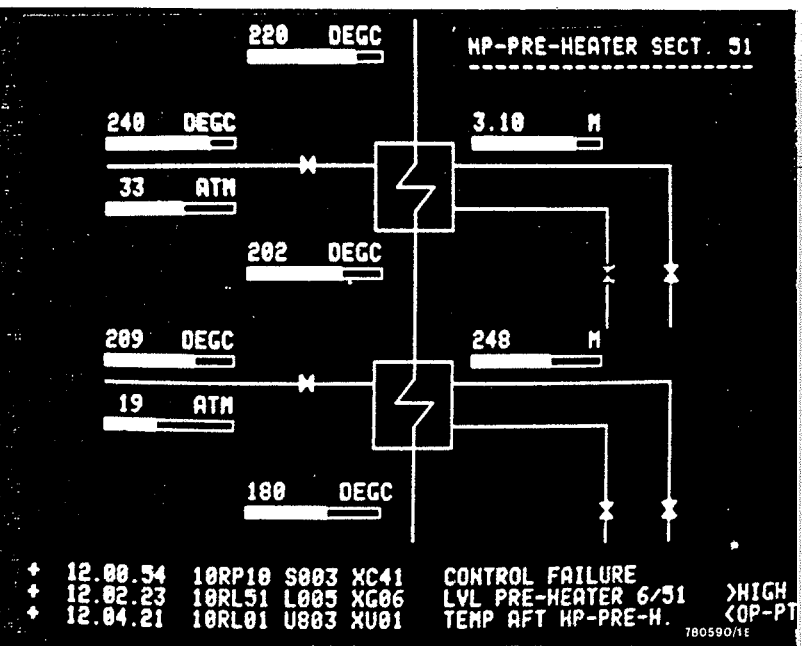


Figure 9
 Sub-PICTURE selected via the overview

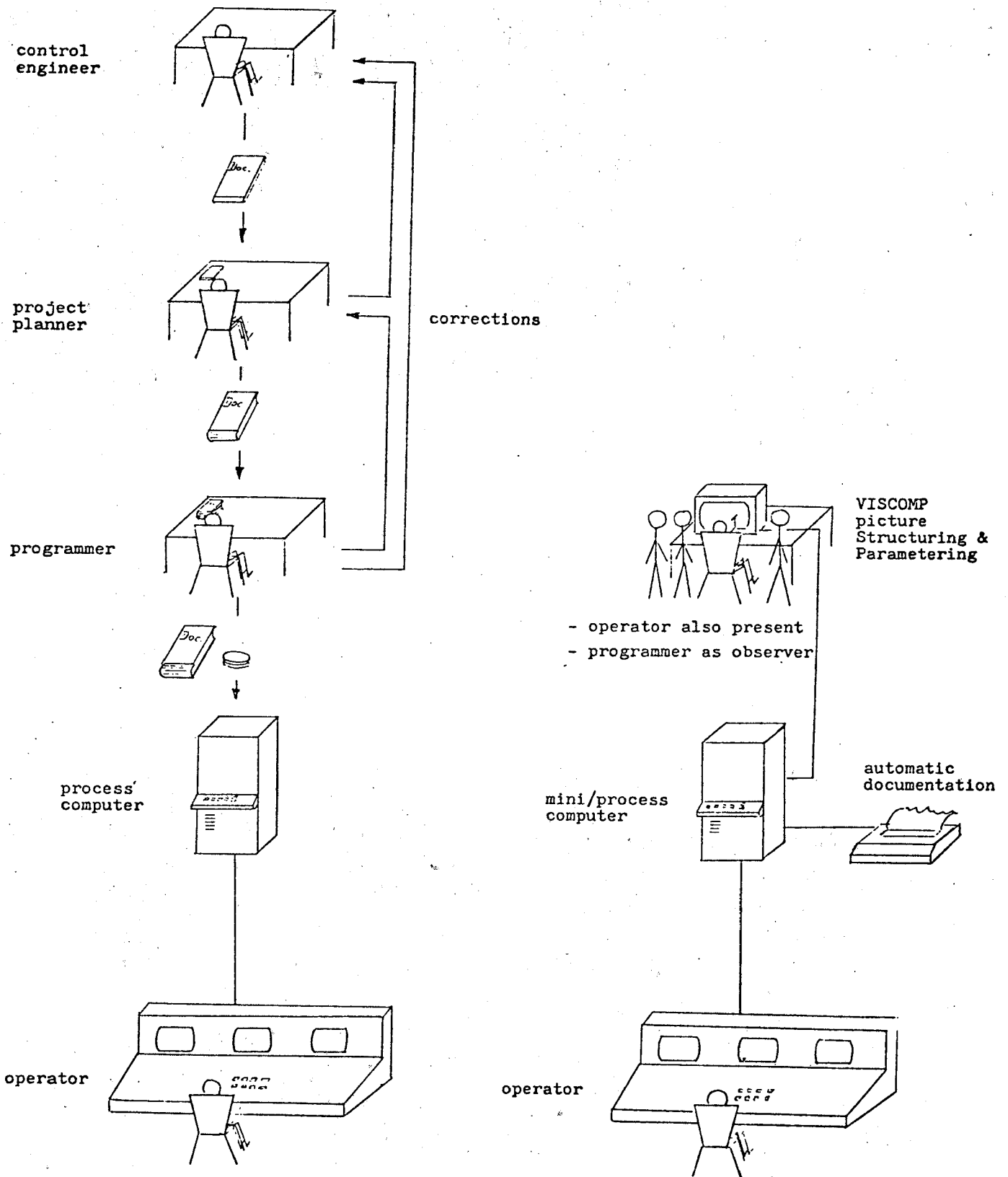


Figure 10a

Figure 10b

A comparison of the VISCOMP method (right) with the methods currently in use (left) for defining the man-machine interface in computer-based systems. Advantages in the saving of effort as well as in the system integrity can clearly be seen.

F. Frischenschlager

ANALYSIS AND PRESENTATION OF ANNUNCIATIONS IN NUCLEAR POWER
PLANTS

Specialists' Meeting on "Procedures and Systems for Assisting an Operator During Normal and Anomalous Nuclear Power Plant Operation Situations"

5. - 7. December 1979, Munich

ANALYSIS AND PRESENTATION OF ANNUNCIATIONS IN NUCLEAR POWER PLANTS

F. Frischenschlager

BROWN, BOVERI & CIE Mannheim

ABSTRACT

This paper is intended to describe an analytical method - within the overall control room conception - which ensures an evaluation of all alarms and status indications for a correspondingly selected output.

This procedure - using modern computer based output devices for process supervision - is a possibility to deal with the high quantity of relevant information, that is approximately 4 500 alarms and approximately 2 000 status indications.

Based on the activity characteristics and responsibilities of the control room personnel the process and control system data will be classified and subdivided into relevant groups.

An overview of evaluated quantities of alarms and status information for each of the defined subgroups will be given.

The paper concludes with a description of the design characteristics of the layout of the communication modules with CRT-displays.

1. INTRODUCTION

1.1 Annunciations within the Control Room Conception

The central control room area in nuclear power plants is divided into 3 functional sections (priority sections) (/1/);

These areas are:

- main operator's console: for the momentary process (constantly attended) monitoring and control for normal operation
- auxiliary control board: for the control of component systems as well as for testing and commissioning activities
- control room annex: for the technical operation control and for the documentation

The communication media are adapted to the activity characteristics and responsibilities of the control room personnel according to ergonomic viewpoints.

Some of the main functions of the main operator's console are:

- process supervision; computerized display units the main sources of information;
- manual intervention at appropriate times during the undisturbed process as well as in fault situations.

On account of frequency and the demands on reliability, the reaction to the alarms is of specific significance.

This does not exclude, however, the necessity of a high adaptability and the capability of taking fast decisions by man.

1.2 Structure of the Alarm System

Computerized Alarm System

For the computerized alarm system usually two redundant process computer units are provided with redundant peripherals for displays and printers.

The main console comprises an action desk and a separate information board. For presentation of a summary of cautionary warnings and alarms two colour CRT-displays are arranged in the middle of the information board. To enable easy readability of the information the CRT size (67 cm diagonal) is selected for a distance of two meters between the operator seated in front of the action desk and the CRT-displays.

Conventional Alarm System

In addition to computerized indication systems, a conventional alarm system with hardwired electronic devices and signal lamps is installed. Via approximately 400 signal lamps group alarms and selected individual alarms are given.

2. THE EVALUATION OF ANNUNCIATIONS

2.1 The Evaluation of Alarms

The evaluation and clarification of alarms depends on their importance which can be deduced from the criteria "safety" and "availability".

The following three influencing factors shall be pointed out in particular:

- the information volume coming in per time unit and
- the necessity of manual intervention within a certain period of time,
- to advise the operator in his search or selection of information relevant to the situation at that time.

Fig. 1 shows an overview related to the main criteria to be taken into account in the case of evaluation and classification of alarms.

2.1.1 Evaluation According to the Type of Alarm

For presentation of information about process anomalies an alpha-numeric listing technique is used. The information content of each presented alarm is covered by a single text string, containing

- the signal classification and time of occurrence
- the text for designation and
- the state indication (e.g. ">MAX, >HIGH etc.).

Additionally the annunciation text is completed with colour codes and special markers indicating the seriousness or priority of a disturbance.

To indicate the Type of an Alarm the state indication in the annunciation text is significant.

The Type of Alarm enables the following to be recognized:

- the state of the individual function of the signal source, ensuring the localization of disturbance
- the activity characteristics the operator is called up to react to.

It has to be distinguished between the following
Types of Alarms:

Cautionary Warnings:

annunciate an impending disturbance and the need for manual counteraction to eliminate the danger and to prevent interventions by the protection system.

Alarms related to Protection Criteria:

indicate inadmissible overrunning of threshold values of process parameters caused by input-signals to the protection system. This information is mainly needed in the case of fault analysis at the beginning and during the sequence operation of disturbance.

Alarms related to Protection Output-Signals:

indicate trip signals from the protection equipment to the switchgear directly or via the individual drive control unit. Related to the actual situation such alarms have to focus the operator's attention on the sequence of the protective actions to enable further measures to be taken if necessary.

Alarms related to Failures and Disturbed Functions:

are the most essential in respect to the activity characteristics and responsibilities for the momentary process monitoring.

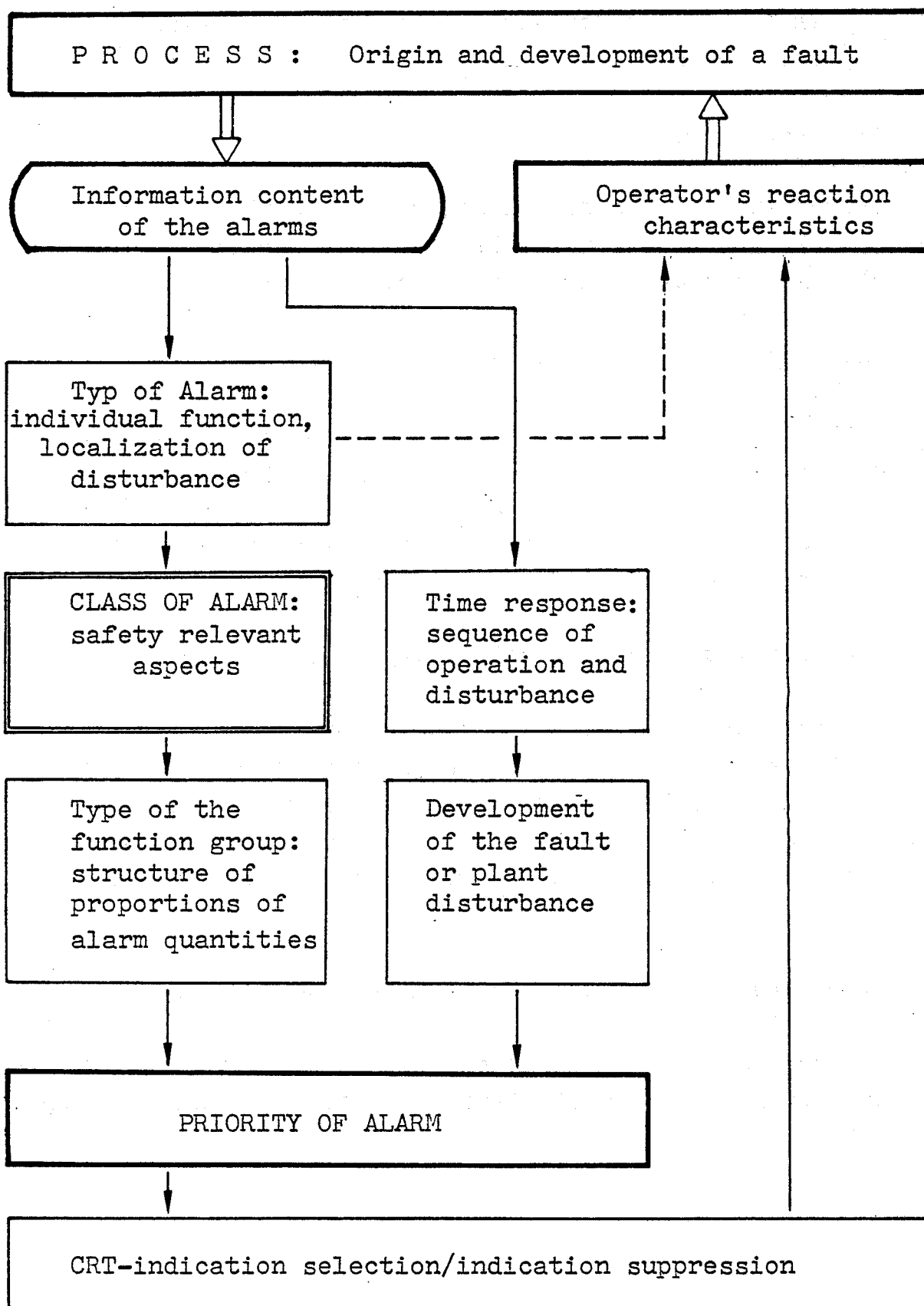


Fig.1: Overview related to the main criteria for classification alarms

2.1.2 Evaluation According to Safety Relevant Aspects:

The classification according to safety relevant aspects corresponds to the KTA standard no. 3501 and distinguishes the danger signalling classes S, I and II.

An Alarm of Class S:

(safety alarm) is the output signal of a protection subsystem. In case this alarm should occur, the responsible operating personnel has strict orders to start a protective measure within a certain period of time.

An Alarm of Class I:

indicates a fault within the safety system.

An Alarm of Class II:

indicates a fault within the operating system.

2.1.3 Evaluation in Respect of the Types of Function Groups:

The division of the process into clearly defined groups - function groups - results in a hierarchical process structure.

To provide increased transparency the high quantity of relevant information is subdivided such as to give a hierarchical structure.

Fig. 2 shows several information levels where a higher quantity of alarms with less importance are subordinated to more important levels with lower quantities.

Analysis indicates advantages in planning procedures, to define types of function groups subdividing the ranges according to the alarm classes.

The information output of each type is identified by characteristic allocations within the information levels (Fig. 2).

The evaluation of function groups and their relative importance is dependent on safety and availability criteria of the whole power plant.

Types of Function Groups:

Type "I" : safety functions
Type "II" : direct influence on availability
Type "hI"/"hII" : auxiliary functions necessary for Type "I"/"II"
Type "(II)" : No direct influence on availability
Type "kI"/"kII" : information output functions

2.1.4 Evaluation in View of Safety and Availability

To denote the urgency of an item of information enabling manual counteraction or fault elimination within a given sufficient period of time, the alarms are subdivided into the following priority groups (see Fig. 1 and Fig. 2):

Priority Group 1:

Alarms from the safety system or important operating systems which require

- strict order for manual protection actions within a given period of time;
- manual control interventions or fault elimination within a short time

in order to eliminate direct danger to safety or availability.

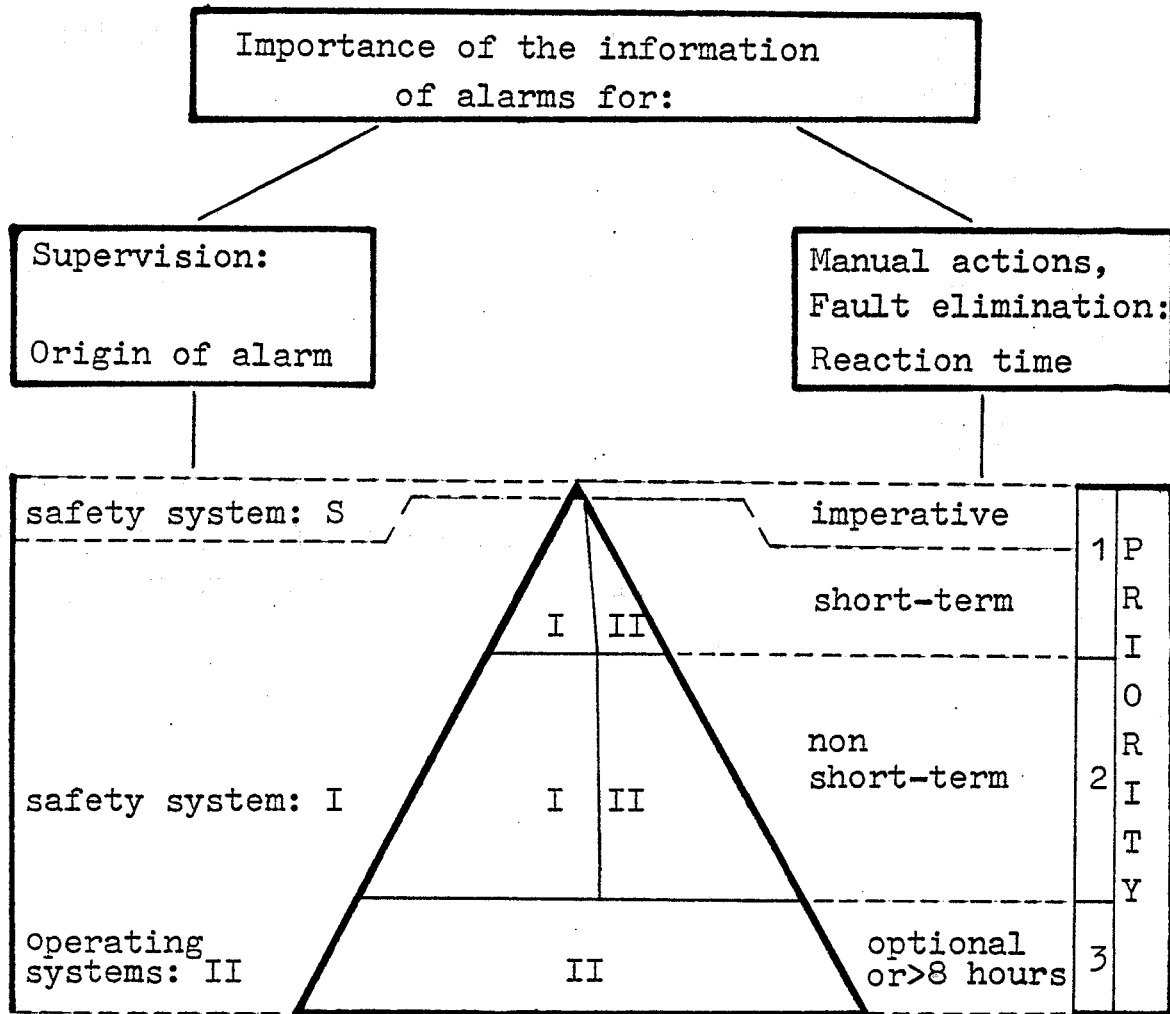
Priority Group 2:

Alarms from the safety system or important operating systems which indicate (medium urgency)

- that manual control intervention or fault elimination is not necessary within a short time
- faults endangering safety
- faults which either impair the availability or which endanger high quality plant components.

Priority Group 3:

Alarms with relatively less information content e.g. from operating systems which do not directly participate in the output generation and which result in no reduction of output or availability or in a reduction only after 8 hours.



Surfaces $\hat{=}$ alarm quantities

Fig. 2: Division of alarms in classes and priority groups and proportions of alarm quantities:
 alarm classes ... S, I, II
 priority ... 1, 2, 3

2.2 The Evaluation of Status Indications

Alarms indicate deviations of the actual state from the setpoints, whereas status indications (switching positions) indicate the actual status.

Status indications from

- aggregates and switching devices which are controlled by protection devices;
- aggregates which have a direct effect on the power generating process

suffice to evaluate the operational process.

3. INFORMATION PRESENTATION FOR ALARMS

The compression, reduction, presentation and handling of the information, the arrangement of the conventional and computerized display-units are based on the results, referred to above.

The importance of the signal information determines the type of presentation to be selected, which is characterized by gradual measures in order to alert the control room personnel and to ensure the relevant read-out-time.

Three different colours are used to indicate the priority of an alarm: red for urgent alarms (priority 1), orange for alarms of medium urgency (priority 2) and yellow for others. (priority 3).

In this solution two CRTs arranged in the information board of the main operator's console are dedicated for a chronological alarm display.

The alarms remaining active are stored and paged. The operator can reference those alarms not currently visible by selecting old pages to be displayed. In case of high alarm activity (alarm burst) it is possible that less important annunciations are filtered out from the display presentation of the alarm output in the main control room.

The logging of all annunciations, however, is independent of this annunciation selection. Actions which are not necessary within a short time can be postponed to be performed during times of less activities.

4. SUMMARY

By dividing alarms into 3 priorities as well as by the selection of the status indications important for the operating process, the control room personnel is able to react according to the importance of the annunciations coming in. For this purpose the annunciation output and especially the annunciation presentation are designed correspondingly. With the aid of appropriate form and colour as well as filtering out of less important annunciations, the control room personnel is able to have a clear survey of the entire process.

Reference:

/1/ L. Herbst: Konzeption moderner Kraftwerkswarten
BBC-Nachrichten, 1977, Heft 10, Seite 417 - 423

T.J. Bjørlo, J.K. Trengereid

COORDINATION OF OPERATOR SUPPORTING SYSTEMS AND PROCEDURES

COORDINATION OF OPERATOR SUPPORTING SYSTEMS AND PROCEDURES

by

***T.J. Bjørlo, J.K. Trengereid
OECD Halden Reactor Project***

ABSTRACT

Experience with power plant disturbance incidents has clearly indicated that adequate information on the actual operating situation is a decisive factor in the operators' ability to cope with such events. The information presented for the operator has already to a large extent been reduced and structured in the power plants which are operated at present. Despite such measures, present days' control rooms cannot be regarded as satisfactory solutions to the man-process interface problem.

During the last ten years an extensive research and development programme has been carried out at the OECD Halden Reactor Project with the aim to exploit the capabilities of modern process computer technology to ensure the safe and efficient operation of nuclear power plants. This paper presents the design philosophy which forms the basis for the work to synthesize the accumulated knowledge and results from past and current efforts into prototype solutions for operator support. Some examples of specific surveillance systems are given. The development of such systems involves both technological, methodological, and human engineering aspects. This paper has emphasized the interfaces to the users, i.e., the operator communication and the procedural aspects of such surveillance systems.

***Paper to be presented at the
IAEA-NPPCI-Meeting "Procedures and Systems for Assisting an Operator during Normal
and Anomalous Nuclear Power Plant Operation Situations"
in Munich from 5th - 7th December, 1979, Penta-Hotel, Hochstrasse 3***

December 1979

1. INTRODUCTION

The recent TMI incident demonstrated clearly the needs for systems supporting the operator in his efforts to prevent that the plant is brought into operating situations with an increased likelihood of disturbances, or that disturbances which have occurred develop towards violation of operational limits. During the last ten years a substantial research and development effort has been spent by the OECD Halden Reactor Project with the aim to exploit the capabilities of modern process computer technology to ensure the safe and efficient operation of nuclear power plants. In this work the merits of a variety of computer applications have been investigated either as a substitute for or as a complement to the functions performed by the existing control and instrumentation systems.

This paper presents the design philosophy which forms the basis for the current research and development work on systems for plant status surveillance at the Halden Project. This work seeks to synthesize the accumulated knowledge and results from past and current efforts into prototype systems for operator support. It is the declared intention of the Halden Project to have such prototype systems tested in pilot installations in nuclear power plants such that their qualities as models for future full scale systems can be evaluated under as realistic operating conditions as possible.

The development of operator supporting systems as indicated above involves both technological, methodological, and human engineering aspects. This presentation has emphasized the interfaces to the users, i.e., the operator communication and the procedural aspects of such surveillance systems.

2. INFORMATION FLOW FROM PROCESS TO OPERATOR

The complexity of present days' nuclear power plants and of the required control and instrumentation systems results in an information volume which the plant operator cannot cope with directly on a continuous basis. He must be assisted by systems which will reduce and structure the information for him. This information reduction and structuring is to a large extent already done in the power plants which are operated at present.

- Only the most important information is made available in the central control room, less important information is made available in adjacent rooms such that it will be fairly easy at hand when it is needed.
- A certain number of the indicating instruments in the control room are multifunction devices such that several measuring points can be addressed by the same device, e.g. alphanumeric cathode ray tubes, and multipoint recorders.
- A large fraction of the status indications is defined as warnings and alarms which are presented automatically, and only need to be considered by the operator when they are activated.
- The information in the control room is structured according to the plant subsystem it belongs to.

Despite such measures to reduce and structure the information which the operator will have to handle in his work, the present day control rooms cannot be regarded as satisfactory solutions to the man-process interface problem. Experience with power plant disturbance incidents has clearly demonstrated that adequate information about the actual operating situation is a decisive factor in the operators' ability to cope with such events, and that there are considerable shortcomings in this respect in most of the present nuclear power plant control rooms.

The design of a control room will always be a compromise between on one hand, simplification and information reduction to ensure a clear overview of the operating situation, and on the other, availability of detailed information to support the diagnostic work when a problem occurs in a plant subsystem. Conventional instrumentation equipment does, in our opinion, not offer the designer of a control room much flexibility in his work to find a good solution to these conflicting needs of the operator.

The conventional information presentation units are with few exceptions dedicated, single purpose devices. When such devices are used a certain piece of information must always be retrieved from the same fixed geographical point in the control room, regardless of the context in which it shall be used. During plant operation there will always be a need for different information combinations depending on the task to be performed. In each case the operator will have to go through a different pattern of data collection from different geographical locations in the control room to retrieve the information he needs. The most frequently used combination of instruments will of course be grouped together, but a really satisfactory solution can, in our opinion, hardly be found by means of conventional instrumentation equipment.

A second effect from the use of dedicated, single purpose devices for information presentation is that the control rooms, when all concessions have been given to the needs for detailed information, grow so large that the geographical problem of information collection mentioned above is strongly accentuated. As an attempt to counteract the ever growing physical size of the control rooms, efforts have been made to make each instrument smaller. Such miniature devices may reduce the distance the operator will have to walk, but the reduced demands to the operators' feet will have to be compensated with increased demands to his eyesight. Such solutions may be more cost effective but they will in no way reduce the complexity of the control room panels and will thereby hardly contribute to an improved man - process interface.

It is the essence of this paper that computers and computer based communication devices should be used to a much larger extent than at present to solve the conflict between the complexity of a nuclear plant and the normal shortcomings of the human beings which will have to operate them. By using computers to control the information flow between the process and the operator most of the problems which are indicated above may, in time be overcome.

Computers have from a technological viewpoint the capacity and the capabilities which are needed to solve the above problems. On the other hand, there is a need for more experience from practical applications of computers as modules in a power plant instrumentation system before both vendors, utilities, and licensing authorities can be expected to rely on them on a broad basis for critical functions in the operation of a nuclear power plant.

3. Computer Based Systems Using Colour Displays

The research and development efforts in the control and instrumentation systems area at the Halden Project have been concentrated on process computer application in plant control. Within this area again, the use of computers to improve the man - process interface has been given the major attention. Among the different computer driven information presentation devices which are commercially available at present, we have found that raster-scan cathode-ray tubes with colours are by far the best alternative for a flexible and at the same time precise presentation of information in the control room. This paper will thus be limited to the discussion of operator supporting systems based on the use of computers and computer driven colour displays. As already mentioned, the main emphasis will be put on the user aspects of such systems, as it is believed that just these aspects have been given too little attention as compared to the technological and methodological aspects when it comes to removing the obstacles for a more extensive use of process computers to support the control room staff at nuclear power plants.

We have at the Halden Project since many years demonstrated in experimental set-ups how a combination of computers and colour displays can be used to give significant improvements to the information flow between the process and the operator. The test reactor at Halden has for certain time periods been operated solely by means of an experimental system of this type. At the moment extensive experiments are performed (1) with an improved version of a computer-based communication system, but this time in a simulated environment such that a higher experimental flexibility can be obtained. The objectives of these experiments are to gain more insight in the operators reactions, his capabilities and limitations when dealing with such systems.

There exists however a considerable gap between what can be shown in the laboratory when running a simulator and what is actually utilized in the control rooms of nuclear power reactors. It is our intention to bridge or at least reduce this gap by developing prototype systems for selected functions, and to have such prototypes tested in pilot installations at operating power plants. It is our conviction that such pilot installations will be a very useful and may be even necessary step in the work to have computer-based solutions put in the place they deserve in a control and instrumentation system. Such installations will serve a twofold purpose, - they will demonstrate the potentials of computer-based systems for operator support, and at the same time provide a feedback which cannot be generated in the laboratory and which will help to identify the bottlenecks and shortcomings which no doubt will exist in the prototypes.

However, when embarking on an ambition as indicated above there should be a common philosophy on which the development of the different prototype systems are based such that there can hopefully be a synergetic effect when the results are analyzed. At the Halden Project we are at the moment involved on a cooperative basis in the development of four different prototype systems which all are intended for pilot installation, and which will be explained in some detail later in this paper. The ideas behind the development of these prototype systems are the following:

- a) The use of computers and colour displays will be necessary in order to find a satisfactory solution to the conflict between the need for information reduction for a clear overview of the plant status, and the need for access to detailed information for diagnostic work during disturbances.

- b) The interface to the operator will be crucial for the acceptance of such aids in the control room. There must be a consistent approach to the way such computer-based systems are introduced to the plant operator both with regard to the way the information is structured, i.e., grouped together, as well as to the use of colours and symbols in the pictures. Consistency must also be required for the way such systems are operated, i.e., the same user procedures must apply independent of the functions a system performs.
- c) Simplicity must be the overriding criteria when the operating procedures are to be established, even at the expense of flexibility. The use of computers tends to be followed by fairly complex user procedures as compared to conventional equipment, and this practice must *absolutely* be avoided in systems for use in a control room environment.
- d) Experience from pilot installations at operating power plants will be needed before good solutions for full-scale systems for routine operation can be expected. The present development work should aim at solutions which can be used as complement to or substitutions for communication functions in already existing power plant control rooms.
- e) System maintenance and validation procedures must be given a very high attention. At present the maintenance and validation aspects no doubt represents a major obstacle for the acceptance of computer-based systems by the licensing authorities as well as by the end users, the utilities.

4. THE STRUCTURE OF A COMPUTER-BASED SYSTEM

When looking at the functional modules which a computer-based system for operator support must contain, one observes that the basic structure is common to most such systems, independent of the function the system is designed to perform. With reference to Figure 1, the following modules can be mentioned as examples:

- 1) Data must be collected on the current status of the process, i.e., the readings of all process sensors and/or manual observations must be made available to the system either at regular intervals or when changes occur.
- 2) A description of the operational characteristics of the plant components and their interrelations as well as the operators need for information must be available such that the data collected from the process can be properly interpreted and handled. The generation and maintenance of the data bank containing such descriptions is may be the most important task in any process computer application, and may be also one of the most neglected so far.
- 3) A data analysis module which will be specific for each application will retrieve data from 1) and 2) and produce the desired results.
- 4) Data from 1) and 3) will then be stored in a data bank which in addition to the current values also may contain historical information on the process operation according to the descriptions laid down in 2).
- 5) An operator communication module will then retrieve data from 4) and present them to the operator on colour displays with a structure and with colours and symbols which can

be defined for each separate picture. This module will allow the operator to request the information, i.e., pictures he wants and may also allow him to enter special requests to the analysis modules in 3).

- 6) Modules which support the generation and maintenance of the descriptions in 2) and the pictures in 5) will, as we have already pointed out, be a most vital part of a system to be used for routine operation.

Now, it is the message of this paper, as indicated in its title, to point out the importance of a coordinated design of the six modules, or group of modules, when computer-based operator supporting systems and procedures are to be introduced to a group of users. It is not our intention at this point in time to propose any coordination efforts between different organizations which are developing such systems, i.e., standardization, but rather to protect a group of users against being exposed to different, uncoordinated systems at the same time.

The coordination must be done in several areas. The most important will be the operator interface, i.e., the dialogue through function keyboards to address the desired information and the construction of pictures which present the information. In this context it is not only important to coordinate the different computer based systems, but until we have entirely computer based control rooms some time in the future, it will be just as important to arrive at solutions which in a natural way can be embedded in existing control rooms. This will for instance require the flexibility to use colour and symbol conventions which have already been adapted, and the ability to draw mimic diagrams which group the plant components in the same way as the existing conventional set-up.

Furthermore, the dialogue procedures should not deviate too much from the procedures the operator is already used to. For instance, extensive use of a full size alphanumeric keyboard would hardly be a success in an environment where the operator is used to simple push-button operations. In the same way extensive use of alpha-numeric text may conflict with the simple reading of dials and indicators.

It will both from a cost and a reliability point of view be desirable to try out and later use the same system solutions at several different locations. In addition to the due attention to the above aspects, it is thus important to have adequate tools available such that a system can be easily adapted to each new application. Therefore a considerable portion of the development effort at the Halden Project has been allocated to the development of such tools.

A second area where coordination will be needed is in the generation and maintenance of the data bank(s) containing the plant descriptions. The preparation and verification of such descriptive data are both time consuming and error prone. It is therefore unfortunate and not to the promotion of computer-based solutions if each system will require a different combination and a different format for the descriptive data needed to operate properly. The same argument will apply to the procedures which are needed to enter the data. Again it is our observation that computer people during the system development period have highly developed skills to handle a large volume of data with a complex structure as input to their specific system and often tend to neglect or underestimate the practical difficulties which may occur during routine operation when they as experts are not there any longer.

In the same way as for the operator interface parts, there is also a need for coordination between computer-based and conventional systems when it comes to modification and maintenance procedures.

Ideally, computer-based systems should be made such that they by means of simple procedures can accept descriptive data with the same structure and format which are used to document the conventional system solutions. For some time yet this will be more of a vision than a reality for most users. However it should be kept in mind as an ultimate goal both by system development people and by the users who buy such systems.

5. WORK PERFORMED AT THE HALDEN PROJECT

Based on the ideas presented above work has been started at the Halden Project on the synthesis of programme modules and accumulated knowledge from laboratory experiments and non-nuclear applications into prototype systems which can be tested in pilot installations in nuclear power plants. This work will be done as separate international cooperative efforts with interested organizations for each of the prototype systems. In such cooperations there will always have to be made compromises in order to arrive at workable solutions, but it will be a major aim for the work to be done at Halden to search for a coordination of the efforts along the ideas indicated above. At the moment the following research and development activities at the Halden Project can be listed in this context:

- A. The application of computer driven colour displays to provide plant status overview pictures will in itself without any extensive data digestion functions represent a significant improvement in most control rooms. We have therefore assembled a software system which contains the functional modules indicated in Figure 2. This system contains the minimum of data handling functions which should be available for a pilot installation of the type we envisage. The main emphasis in a pilot installation with this setup should be put on the use of the interactive picture editor. By means of this editor pictures with dynamic mimic diagrams, bargraphs and trends may be easily constructed and put into the picture library where they will be available for use by the operator. During the construction of such pictures information from the process can be grouped together in a multitude of combinations according to the operators' needs in the different operating situations. A systematic approach to the construction of the pictures must of course be developed since the operating strategy for the plant should in fact be embedded in the picture library once it has been properly established.

The interactive table generator will support the generation of plant data description tables. Based on these tables the limit check routines and the plant data bank will provide the current and historical status information which will be needed for the dynamic updating of the pictures.

In Figure 2 it is also indicated that the current plant data may be substituted by data from a plant simulator, such that the same setup may be used for operator training purposes, especially for handling of rare events. For the latter purpose even a primitive event sequence simulator has been developed.

By means of the above system the operator can, at the same location, by a simple request procedure have available an overview of for instance the feedwater system as indicated in Figure 3, or a detailed presentation of the status of the lubrication system of the con-

densate pump as indicated in Figure 4. In both cases all the relevant status information will be available in the picture itself indicated by numbers, colours, and symbols. For other pictures bargraphs and trend curves may also be applied.

It is our conviction that a prototype system as the one described above represents a very valuable tool which can be used to gain experience with the merits of such systems in actual power plant operation, and contacts have been established between the Halden Project and two separate utilities which both have the intention to try out the system on a cooperative basis.

- B. The warning and alarm indications in power plant control rooms are designed to convey particularly important information to the operator. Each alarm or group of alarms is presented by a separate indication, and it is the operator's responsibility to observe the patterns of warning and alarm indications and to deduce the corrective actions which are needed. With the high number of indicators and with the complex relation which may exist between them, it can be a difficult task for the operator to draw the correct conclusions about the source of a disturbance and to foresee the consequences which may result if correct counteractions are not taken in time.

For several years a collaboration between Gesellschaft für Reaktorsicherheit (GRS), Garching, and the Halden Project has been going on in the fields of disturbance analysis, control room design and operator communication (2, 3). Through this cooperation with GRS, the Halden Project has provided practical contributions to a prototype system for fast analysis of power plant disturbances developed by a German interest group. The objective of this system is to assist the operator in recognizing predefined alarm patterns and to identify the corresponding causes and consequences. By using a computer to automatically identify the expected warning and alarm patterns, the strain on the operator during critical disturbance situations can be reduced such that his performance can be enhanced during the time periods when his correct counteractions are most needed.

The cooperative efforts on this prototype system include the installation and the experimental operation of the above disturbance analysis system at the Grafenrheinfeld plant in Germany. The ability of the system to handle unexpected patterns of information from the plant, and the correctness and the contents of the sequence diagrams which represents the expected patterns, will be given special attention during this work.

The disturbance analysis system has a main structure as shown in Figure 5. In the context of this paper the system can be considered as an example where the emphasis has been put on the generation and maintenance of the descriptive data, since the quality of the results will depend entirely on the quality of the process description. It is expected that the preparation and execution of this pilot experiment will provide valuable experience on how to simplify the routines used to establish the event sequence diagrams which describe the disturbance chains, and on how to improve the corresponding verification procedures.

At a later stage, the design of the disturbance analysis system should be coordinated with a system of the type described in section A, above. Especially the use of mimic diagrams

as for instance the one shown in Figure 4, with dynamic colours and symbols to present the results should be tried out and the benefits from combining results from the analysis and directly measured data in the same diagrams should be investigated.

- C. In cooperation with Studiengesellschaft für Atomenergie Ges.m.b.H. (SGAE) in Austria the Halden Project has developed a prototype system for the surveillance of reactor protection systems which all have a large amount of redundancy in their structure in order to attain high reliability (4, 5). Because of this high redundancy, it is acceptable to operate the plant even when some components are out of operation. It is, however, important that a repair strategy is followed to ensure that the overall reliability of the protection system always remains above an acceptable threshold.

Repair strategies for various combinations of failed and non-failed components are usually documented in the operators' manuals. In this system the contents of the operators' manuals have in principle been transferred to data tables which can be entered into a computer and be handled by a data analysis programme. Through an interactive dialogue the operator can identify the components which have failed, and the system will present the status of the affected parts of the protection system on a colour display, thus giving the operator a better comprehension of the consequences of each component failure.

This system was originally planned to be tested in a pilot installation at the Zwentendorf nuclear power plant in Austria, but these plans had to be postponed due to the present nuclear moratorium in Austria. At the moment other arrangements are sought such that the concept can be tested in a real plant application.

There is no need for any direct physical connection to the plant instrumentation in order to utilize the above system. It can be seen as an example of how the combination of a computer and a colour display can be applied to improve and further coordinate the operator supporting procedures, as the tedious search in operation manuals and the interpretation of written instructions can be substituted by the same retrieval procedures and the same information presentation formats as the computer-based presentation of process status information.

- D. Detailed knowledge of core status, and the ability to predict how the core responds to specific maneuvers, will improve the safe operation of power reactors. A prototype of such a core surveillance system is being developed at the Halden Project in close cooperation with participating organizations. This system is intended as a tool for the reactor operator, giving him detailed information on the core status through the use of colour displays. In addition, a predictive mode of the system gives the operator the possibility to simulate a proposed reactor operation strategy, before the actual execution of the proposed maneuvers.

A data bank for storing the information related to the reactor core is an essential part of this system. The actual and the simulated core status information represent a large volume of data with a complex structure. The design of this data bank such that the stored information can be easily and quickly obtained by the operator, is a task which will provide valuable feedback for the construction of process data banks also in the context of other process computer applications.

The global software configuration for the core surveillance system is shown in Figure 6. The most interesting aspects in the context of this paper will be the organization of the information in the dataset library system and the strategy for the use of the dialogue and display system. The task of core surveillance involves the handling of fairly large multidimensional data sets as both space, time, and operation strategy will have to be considered for most of the interesting status parameters. Every data set will have to be searched for abnormal conditions, and the operator must be informed if such conditions occur.

There has not yet been made any definite plans for any pilot installation of the core surveillance system. However, the ongoing development work and hopefully the experience from a future experimental operation will no doubt provide valuable know-how on the handling of large, complex data sets, and on the simplification of operator procedures for complex calculations.

6. CONCLUSIONS

It is the conviction of the Halden Project that process computers with colour displays can be developed into powerful tools which will be the best means to solve the present operator - process communication problems. It is, however, realized that many problems remain to be solved before this technology will be generally accepted as practical tools for extensive use in routine operation of nuclear power plants.

This paper has explained the basic philosophy and the practical approach the Halden Project has adapted in its work to solve some of the remaining problems indicated above. A major effort has been made on development of prototypes which will provide experience and insight in the practical problems which are the real obstacles for a more extensive use of computers in the control rooms of nuclear power plants.

The development of such systems involves both technological, methodological and human engineering aspects. In this paper the interface to the users, i.e., the operator communication and the procedural aspects of such surveillance systems, has been emphasized.

ACKNOWLEDGEMENT

This paper presents results from the development work at the Halden Project on applications of process computers in nuclear plants. The authors are grateful to the Project for having been given the opportunity to present the results, appreciating the major efforts in the design and development of the prototype systems described in this paper carried jointly by the Project staff as a group.

REFERENCES

1. K. Netland: "Experimental Measurements of Operator Performance". NPPCI-Meeting, Munich, 5th - 7th December, 1979.

2. F. Øvre, L. Felkel: "Functional Description of the Disturbance Analysis System for the Grafenrheinfeld Nuclear Power Plant". Enlarged Halden Programme Group Meeting, Loen, Norway, June 1978. HPR-221.14.
3. W.E. Büttner, L. Felkel, R. Grumbach, H.G. Herdtle, F. Øvre: "Data Base Preparation and Operational Features of the Disturbance Analysis System for the Grafenrheinfeld Nuclear Power Plant". Enlarged Halden Programme Group Meeting, Loen, Norway, June 1978. HPR-221.14.
4. H. Roggenbauer: "Basic Ideas for the Development of a Computerized Operational Manual". Enlarged Halden Programme Group Meeting, Loen, Norway, June 1978. HPR-221.14.
5. R. Haubert, G. Dahll, T. Palmgren, R. Stokke: "Reactor Safety System Surveillance by Computer". Enlarged Halden Programme Group Meeting, Loen, Norway, June 1978, HPR-221.14.

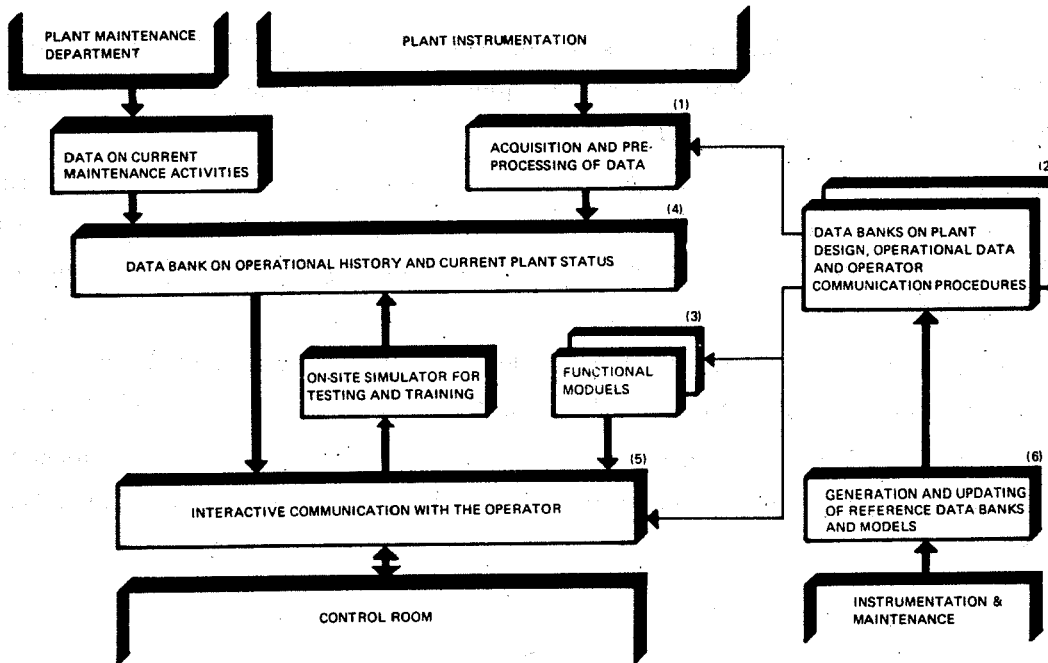


Fig. 1. Main components in a computer-based system for operator support

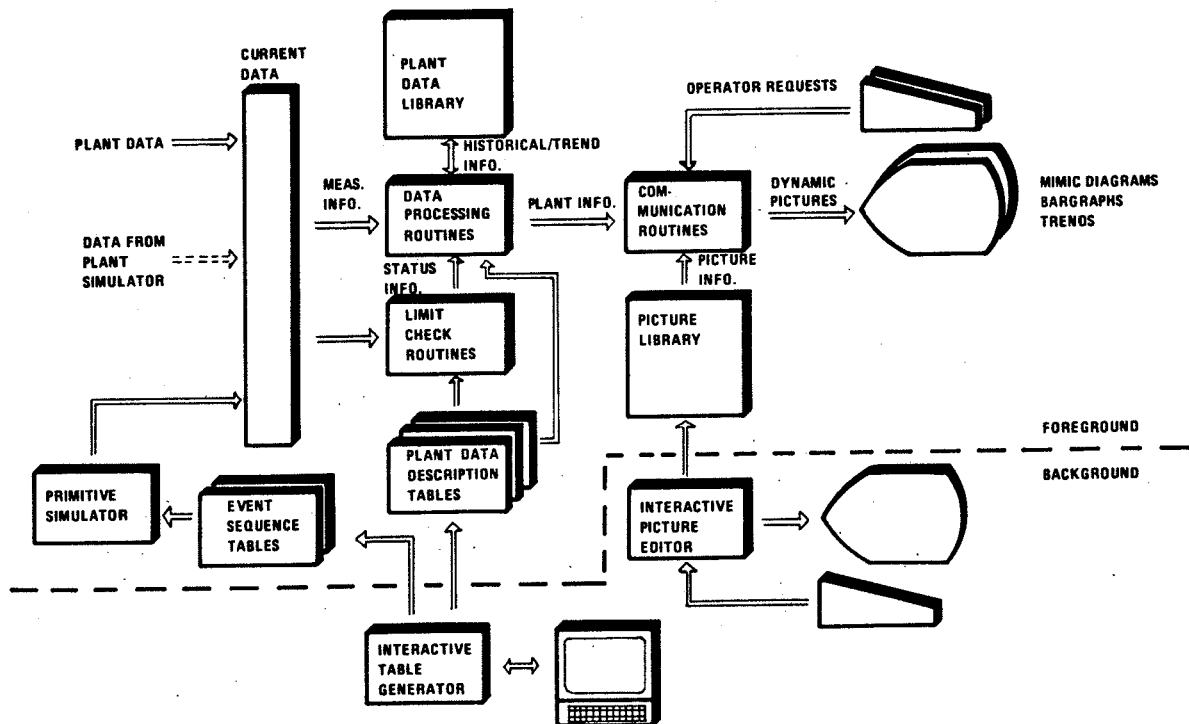


Fig. 2. Main structure of the software package to be used for development of operator communication functions

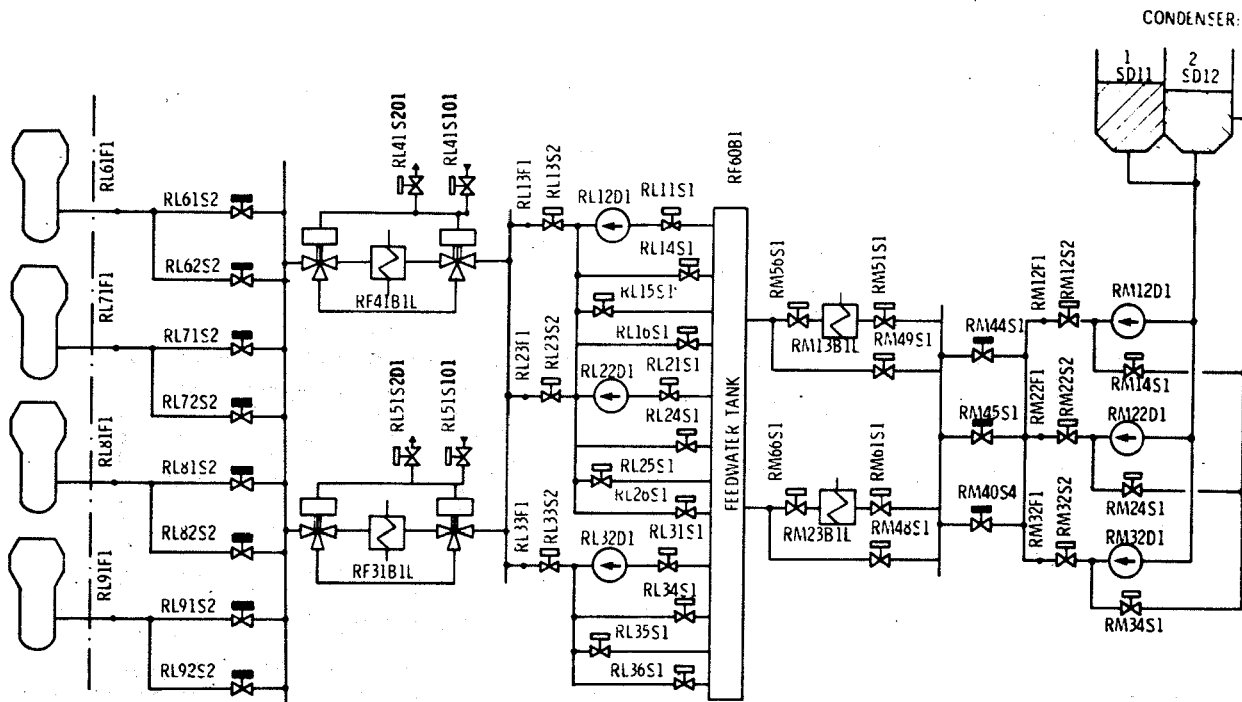


Fig. 3. Feedwater circuit, schematic diagram

MAIN CONDENSATE PUMP COOLING AND LUBRICATION

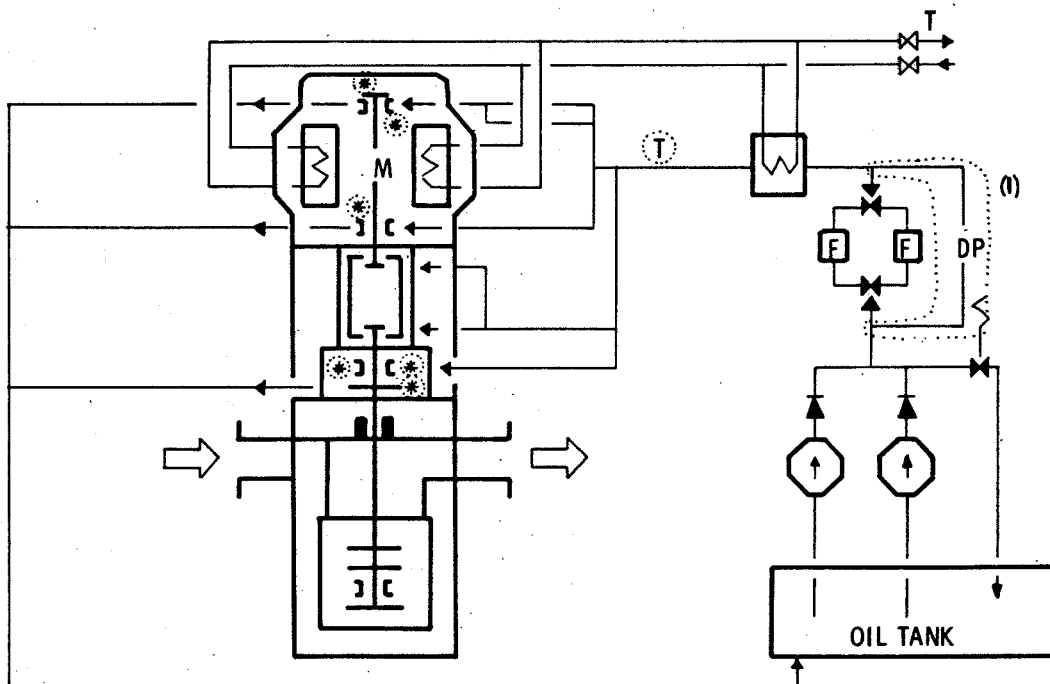


Fig. 4. Main condensate pump status visualization

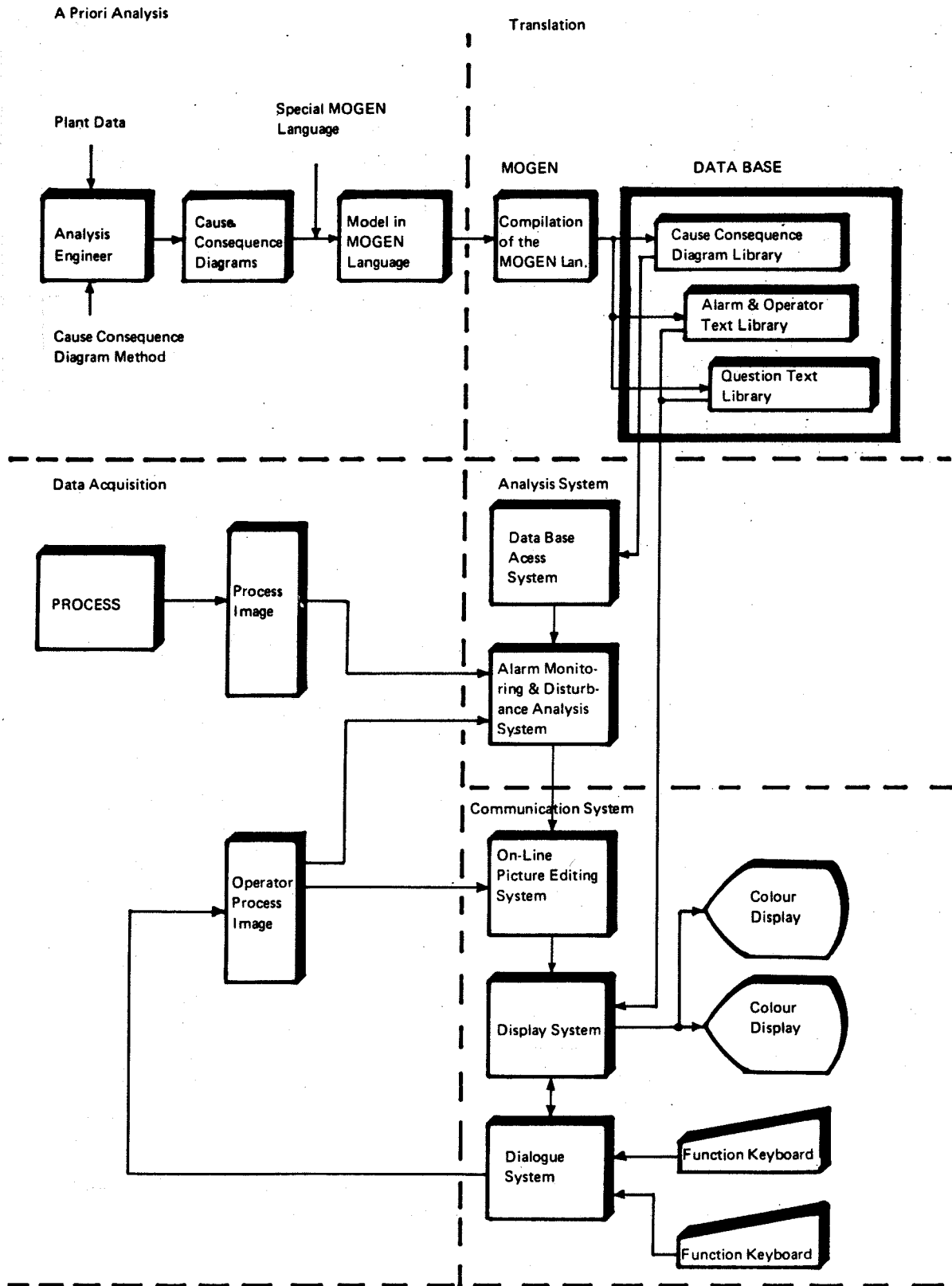


Fig. 5. Main structure of disturbance analysis system

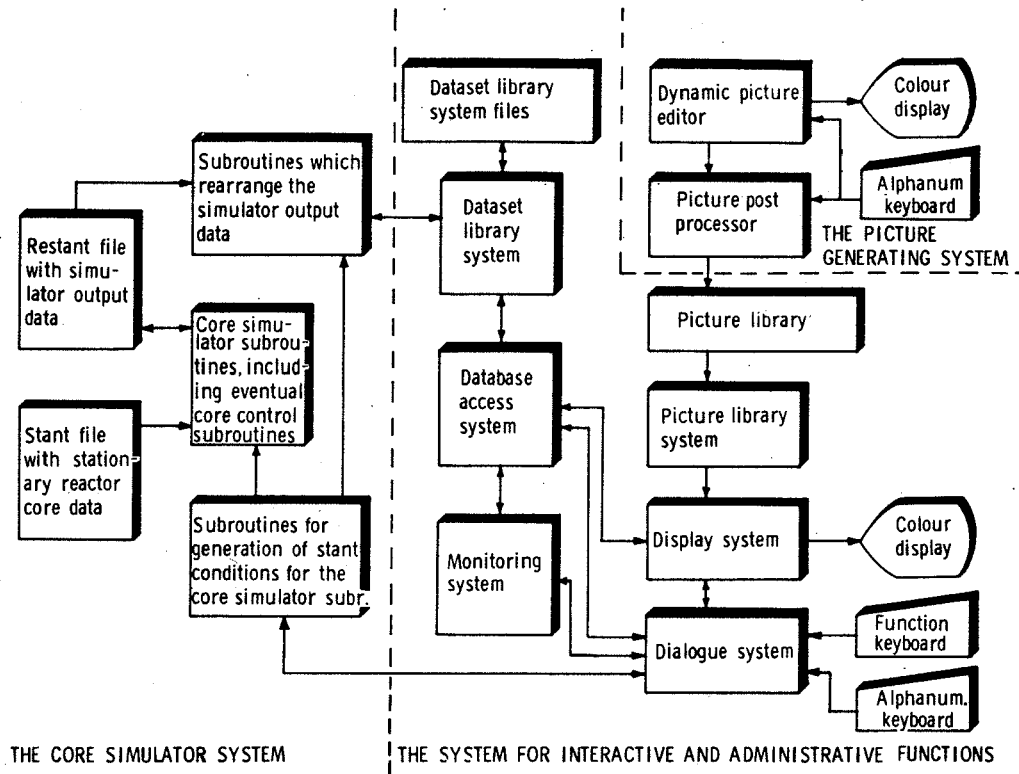


Fig. 6. Software configuration for the core surveillance system

D.M. Hunns

PSYCHOLOGY OF COMMUNICATIONS

PSYCHOLOGY
of
COMMUNICATIONS

D.M. HUNNS

National Centre of Systems
Reliability.
England.

CONTENTS

Introduction

Structuring of Mental Models

Communication

Communications Analysis

 Memory failure

 Pre-experience take-over

 Risk blindness

Conclusion

Introduction:

The human component in any technological system may be dichotomised into two distinct areas. Firstly and most obviously there is the operational, managerial team which controls, supplies, maintains and administers the day by day and year by year functioning of the system — the total 'life support' group. Then secondly, and less directly obvious, there is the original contribution from the vast human team which evolved the system through its total creative phase from concept to completion. This contribution is remembered simply in the strengths and weaknesses represented in the hardware of the system. Thus it could be claimed that the proclivity of a system to fail is always a manifestation of human fallibility, irrespective of whether failures appear to be operator or hardware associated. Indeed many would argue that if we wish to improve the human contribution to system reliability it is principally the designer with whom we should be concerned, not the operator. However, design error arises at least in part from a lack of knowledge of the true mechanisms of operator error and hence an understanding of these mechanisms remains as a fundamental requirement.

The earlier sections of this paper therefore theorise on the ways in which the mind works in an operating situation and therefrom attempt to deduce certain basic psychological mechanisms which produce human error. Measures for opposing these mechanisms are also suggested. Failures of a system due to either operator illness or an act of conscious sabotage are not considered here. While it is acknowledged that major catastrophes have originated from such causes, nevertheless accident statistics suggest that the majority of human inspired accidents derive from errors by healthy and well meaning operatives. The ideas suggested here concentrate on this latter source of system failures.

Thus, given that we are concentrating on system failures which are direct outcomes of actions or lack of actions by the operational team (operators, maintainers and their administration) and also that we assume the operatives to be medically fit and without intent to damage, then in these circumstances human inspired system failure will derive from mismatches between the system states, present and future, as perceived by each operator and the system states, present and future, which are actual — the classical misalignment of perception and actuality. If such mismatches are able to endure through an operational cycle, progressively the opportunity for recovery becomes eroded away until a point is reached where catastrophe becomes inevitable. The problem resolves down to one of communication. This paper attempts to explore a closer understanding of what do we really mean by communication and what are the elements which influence its success. The techniques of communications analysis is proposed as a systematic exploration of the alignment between an actual system state and the operator's mental model of this state. How such a technique may assist in the prediction of accident sequences is illustrated in an example analysis of a railway signalling system.

Structuring of Mental Models

Life's experience is a continuous progression of observing cause and effect. Where, in our total experience, a particular cause and effect are unexceptionally linked, for example a 10kg. mass breaks a 1kg. breaking-strain string, then we associate this as fact and use it as the basis for logical deduction in future situations. However, even if this example were inviolate, other cause and effect associations are less straight forward. For instance, consider the cause and effect sequence of turning the ignition key and starting the car engine. Here, for most of us, a number of effects will have been experienced, the principal two being that the engine either does or does not start. If asked to predict the outcome of a given attempt we would immediately request supplementary information, for example, has the car just been running previously, if not is it a cold, damp, morning, etc. Clearly the mental model carried by those who have had any dealings with cars is a complex one. But even having established a detailed scenario the cause and effect relationship will not be clear. A judgment must be made involving a laboursome recall effort of previous experiences. In other words the mental model carried relating cause and effect in a car starting sequence is a probabilistic one. In fact the same could be argued in relationship to the first example of the mass and string, only in this case no evidence had arisen to suggest that the "effect" probability was less than unity.

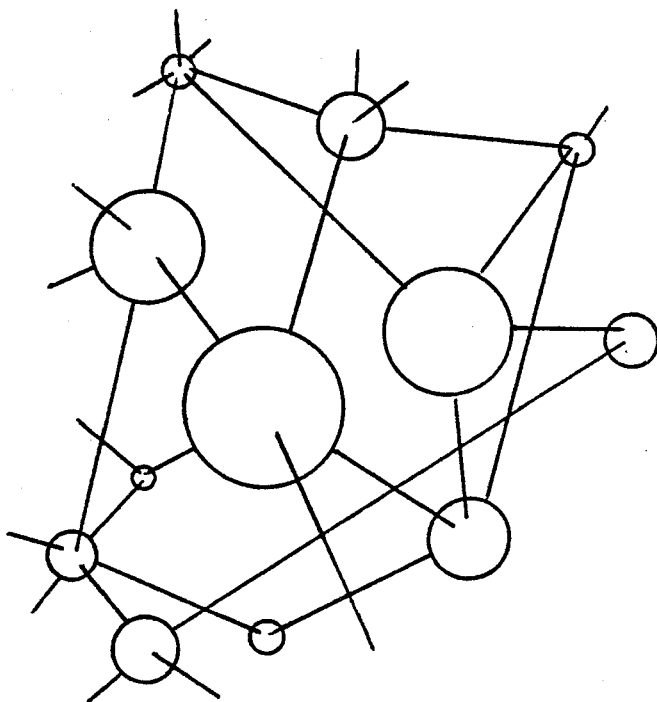


Figure 1. The Associative Mind

So it would seem reasonable to suppose that for each one of us our deductive capability is based on a vast complex of personal "cause and effect" associations which are probabilistic in nature and which are experiencing continuous updating. We might picture this complex of associations as a massive multidimensional net where the knots are the "units of recognition", the independent ideas, and the strings represent the associative links between these ideas. The principle is illustrated in Figure 1.

The multidimensional concept opens up the possibility for there to be many different association routes linking

two units of recognition (uor's). The conscious mind appears to move freely over this net like a travelling frame, centring itself over each successive uor as the associative linking permits. Where a given uor has a number of

alternative association links, for example where a "cause" has several possible "effects", the frame must expand to bring in the various possibilities and consider their relative likelihoods. The concept is illustrated in Figure 2 where the frame has centred on uor A and expanded to review the associated uor's B,C,D and E. Their relative likelihoods,

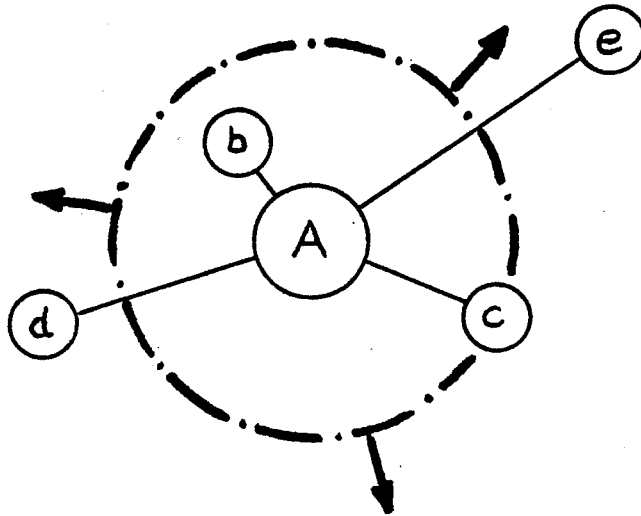


Figure 2. The Process of Thought.

as experienced by the mind depicted in this example, are represented in terms of distance from A. So as the frame progressively expands the less frequently experienced, and therefore more weakly associated uor's come into view. The process of expanding the frame is both time consuming and energy consuming and the more intently it is pursued the more is the mind aware of the exercise of a conscious thought process. The ultimate expansion of the frame is almost certainly a fundamental requisite of controlled lateral thinking, is extremely fatiguing and can be sustained only in short intervals. How-

ever, normally this so called "viewing frame" of the conscious mind will not require excessive expansion in order to proceed purposefully through the multidimensional field of uor's. That is to say, the normal process of thought is relatively rapid and effortless.

Where a particular "cause" uor has only one possible associative link to an "effect" uor the conscious viewing frame transports between the two involuntarily and, in thinking terms, instantaneously. This instantaneous transition is, in effect, reflex thought and because of the absence of a decision-operation does not incite conscious awareness of its process. It is the ultimate in learnt response and undoubtedly forms the basis of our high speed processes like speech, reading, writing and even vision itself. It is quite possible that the majority of uor's in the brain are of this single transition type; however, it is only those which have multiple transition possibilities which incite conscious awareness by inducing the decision-process of thought.

The process of learning occurs when through the senses the mind can experience and link uor's. However, it is apparent that the experience must be repeated many times before the reflex response is achieved. Figure 3. shows an analogous illustration of the growth of association links. Units of recognition, A and B, are introduced to the mind as associatively linked. A and B carry a large number of potential links and each time the association

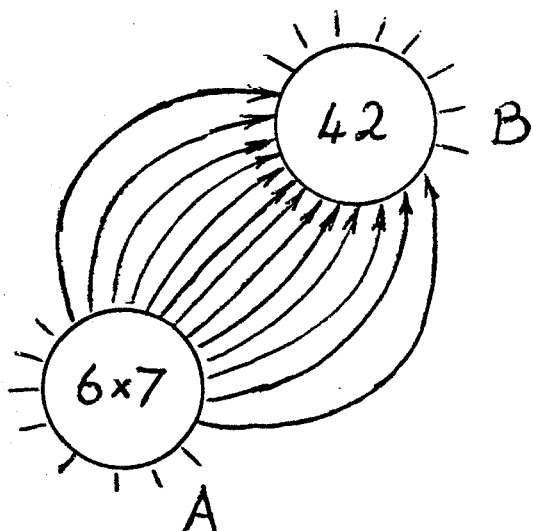


Figure 3. The Strength of Associations

is re-experienced (this could be simulated by conscious internal repetition) so a further link is established. With each further attachment the associative transition speed between A and B is increased until finally, with the commitment of the last available link, reflex speed is achieved. In the same process the possibility of linking associatively elsewhere becomes progressively reduced until finally A is totally eclipsed by B. For all intents and purposes the two have become one. A child learns its "times tables" by dint of this repetitive process. $6 \times 7 = 42$; there is no other possibility.

Given the validity of the proposition that we learn by observing associative relationships it does not follow that in the same process we understand the mechanisms of these observed associations. The utter conviction a person may have that glass, as a material, forms an impervious barrier to water is merely the outcome of repeated observation of this phenomenon. The observer's mastery of the fact in no way enables him to explain the mechanism by which it comes about. The cause and effect basis of knowledge, if it is to be a firm foundation for deductive reasoning requires that each associative link should be conditioned by all those factors which determine its certainty. In practice of course these conditioning factors are only partially observed and consequently it is found that one cause may call up in the mind one of several possible effects; in any given instance it is not possible to say with certainty which one it will be. However, a given person will have his own conviction as to which outcome is the most likely. Figure 4 illustrates the process. Suppose the "cause" is A with associative links to alternative "effect" nodes B and C. Suppose also, in this person's experience, B has occurred twice as often as C. Thus there will be twice as many associative links between A and B as between A and C; B therefore will register a stronger associative experience than C. It is by this means that the mind generates conviction as to the most likely outcome. It is important to note that the absolute strength of the association between, say A and B is not a factor which has meaning in the mind — it is the relative strengths of the links AB and AC which register consciously. This is clearly demonstrated by the fact that we judge in the comparison domain with ease but are generally poor when it comes to judgment in the absolute domain. In fact it is almost certain that an ability to judge absolute quantities is accomplished by firstly learning a register of calibrated factors so that the exercise in effect continues to operate in the comparison domain.

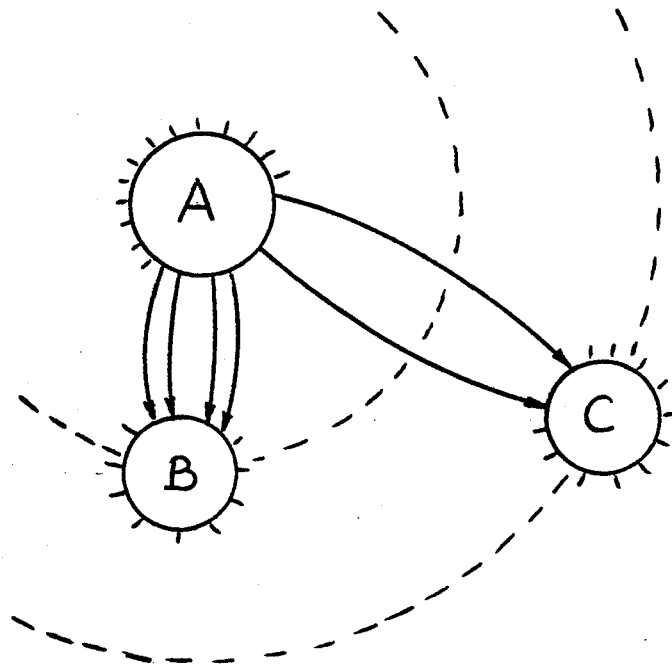


Figure 4. The Process of Judgment

The multidimensional structure of associated "units of recognition" which represents the total register of a person's accumulated experience is, of course, that person's memory. The foregoing postulations have suggested that this structure is also the foundation and mechanism of a person's deductive and conscious thought processes. The conscious mind has been depicted as a viewing frame which traverses this structure, resolving and pursuing the routes of strongest association, back and forth, until a required answer is resolved. It would seem that, the "viewing frame" retains a short term (typically, in the order of 10 seconds) image of its

immediately previous whereabouts to enable a retracing of the steps should a particular pursuit prove fruitless — the feature which we would consciously describe as our short term memory.

The total associative structure acts in co-operation with the senses to establish an inner picture of the world which is outside. We live not with reality itself but with our individual and internally constructed images of reality.

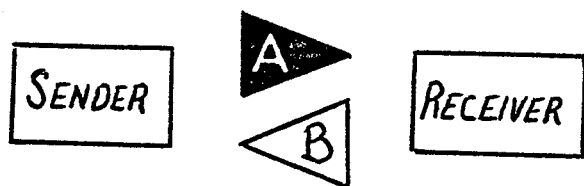
Communication

It is perhaps more than obvious to say that without the senses the brain, from the human point of view, would be simply a piece of vegetation. The associative structure which is the core of our awareness is entirely dependent on, and at the same time limited by, the powers of our senses. From the moment that as an embryo we come into being, the senses act on the brain to supply the associative links which build up our patterns of recognition. The task of building up the associative structure of the mind is inconceivably enormous. It is not surprising that several years of contact are required before a consistent and workable model of the environment about us is developed in the mind. Perhaps the accomplishment of this stage is signified by the commencement of conscious memory.

Communication therefore is an old friend. It is the life blood of the senses and the food of the mind. It originally provided the brain with the mental models of its environment and it unceasingly continues to update this information to provide a dynamic awareness of each moment's existential state.

Communication comes in many forms, covering the full spectrum from being forced irresistably upon us to that which is casually observed or consciously sought. But however it impinges upon the brain, if the communication is to be comprehensible it must accord with our repertoire of understanding. A regularly flashing light in the darkness is observable, it is communication but, of itself, it has no meaning. However, if the observer is on a ship at sea the communication is at once of the utmost significance. Therefore our mental models are essential to interpret communication but, by the same token, will also limit the interpretation which we can make. In effect the mental model enables an assumption to be made about the intelligence being conveyed. The assumption may be in fact a set of possible assumptions, each weighted in terms of likelihood, but whatever form it takes it will serve as the basis for updating the current mental model of our perceived environment, the surrounding system.

An analyst, studying the sequence of operations on a process plant, if he is to predict the action which a particular communication incites in a process operator, firstly must have a close knowledge of the general mental model carried by the operator and secondly he must trace the current state of updating immediately before the communication arrives. This would appear to be the only basis on which meaningful predictive analysis can be carried out. If in the course of a systematic study of this type the analyst can show that the associative "cause and effect" response in the operator produces "effects" which are decisively wrong or are simply indecisive then he must conclude either that improvements must be made in the base mental model of the system as carried by the operator or that the communication scenario itself has proved inadequate. Experience tells us that inadequacies in both areas become paramount whenever the "normal" system develops an abnormality. Designers do not always recognise the need to make special provision for communicating abnormalities to the operatives. The training of operatives is not always geared to registering, and from time to time reinforcing, the necessary cause and effect models associated with such abnormalities.



- A: Receiver registers and understands sent information
- B: Sender knows that receiver has registered and understands sent information.

Figure 5. The Ideal Communication Cycle.

Having discussed the essential role of the mental model for correctly interpreting communication from the receiver's point of view it is as well to consider also the situation with respect to the sender. The sender attempts to register information with the receiver, indicated by the forward transmission 'A' in Figure 5. If he is successful the state of mind of the receiver is thereby updated. But in his turn the receiver should feed back to the sender (return transmission 'B') that the information has been fully

received and understood. Without this feed back the sender will not know the state of mind of the receiver and therefore to this extent his mental model of the total system about him will have become uncertain. The requirement is fundamental. In practice the feed back tends to be circumstantial. If we say to a man who is running, "Carry on running!", the fact that he continues to run may tempt us to assume that he is complying with a communication successfully received. Such an assumption, based on observation, however is groundless. If, on the other hand, we say "Stop!" and he does immediately stop we are convinced, and with good reason, that the communication was successfully received. The assumption could still be wrong but we now have a substantial weight of probability on our side in favour. Nevertheless it would be dangerous to use this as an axiom; however, the corollary can be stated without risk,

'Continuation of this present state of existence by the receiver cannot be taken as confirmation of information received if that same information did not command an immediate and evident change of state.'

The analyst, in tracing the sequence of communication states which occur in an operating cycle, must identify not only what the receivers know at each succeeding system state but also what the senders perceive the receivers to know. Once again the exercise is at its most fruitful when considered in the context of existant system abnormalities. There is little doubt that the establishment of positive feed back confirmation is the aspect of communication which is most vulnerable to neglect by system designers. An ideal example of where this has not been neglected is the telex system where the message typed onto the keyboard of the sending machine is reproduced on the 'sending' platon as a return copy from the receiving machine.

From the sender's point of view communication may be divided into the following general categories,

- (1) A command requiring current action.
- (2) A command requiring action at a specified occasion in the future.
- (3) Information to be used as the receiver decides.
- (4) A question.

The "question" form of category (4) effectively reverses the roles between sender and receiver, the receiver of the question thereafter taking the part of the sender — he may become a sender in any one of the categories (1) to (3). Category (1) communications aim to alter system states in present time while category (2) and category (3) communications prime the receiver for future alterations of system state. Of particular interest is how the ideal communication cycle (Figure 5) can be achieved in the case of communications which relate to future action: Category (2) and category (3) communications, if of a transient form, are susceptible to being forgotten by a human receiver. It is therefore frequent practice for the

sender to employ some inanimate device which continuously displays the information until either the receiver acts upon it or the information is no longer applicable. Ideally the receiver would himself cancel the display by executing the action which it communicates, this, in turn, feeding back to the sender. The London underground railways make extensive use of this principle in their aspect light signalling systems. Normally a signal light shows the danger colour "red" which means "stop". When the signalman perceives that the line is clear for an expected train he alters the signal light to "green", this then becoming a category (2) communication. On passing the signal the train automatically returns the signal light to "red", this action being observable by the signalman.

This use of an inanimate "message carrier" is not without its shortcomings. First of all the receiver loses positive identification of the original sender — in this respect he must make an assumption. Secondly should circumstances alter the validity of a "set" communication the sender must take positive action to cancel — he may well forget. Thirdly, the receiver himself may omit to cancel the communication, thereby creating a contradiction between actual state and indicated state. Enterprising design can do much to alleviate these possibilities.

The foregoing discussions have concerned themselves principally with the interpretation and feedback of information. However, fully interpretable information may be originated, perfectly transmitted and yet fail to be received. To be taken into account here is the receptiveness of the receiver — broadly speaking this can be split into three categories (given the collective acronym CUE).

- C — Consciously seeking the communication
(a driver looking for a road sign).
- U — Unprepared - the communication would be a surprise
(a driver finding a tree across the road).
- E — Expectant - the communication is awaited but not sought
(a driver reaching a set of traffic lights).

The mental model which the receiver currently carries will determine the CUE level of receptivity which he offers to a given communication. Broadly speaking, to improve the probability of successful reception the U-category receiver requires the information to be sent with high conspicuity and with extended time for assimilation. These requirements may be progressively de-rated for the E and C category receivers. Since it is the occurrence of abnormal operating states in a system which will tend to find the operators in the U-category of receptivity it is obviously important that strong and distinguishing means should be provided for communicating these states. Perhaps it is the systems analyst who can identify the abnormal states which should be communicated; it is certainly the system designer who must provide the means.

Thus a prerequisite for effective communication is that its form and information content should fall within the repertoire of understanding of the receiver. This repertoire of understanding is defined by the existant system models carried in the mind. The communication, as interpreted within the constraints of these models, is used to update the receiver's perception of system state. The importance of feeding back a "communications receipt"

to the sender has also been highlighted as essential to correctly update his, the sender's, perception of system state. Categories of immediate and delayed communication have been defined and in the latter context the pros and cons of the "inanimate messenger" have been discussed. Finally mention has been made of the CUE receptivity levels of the receiver and the implications these have on the forms of communications which are required.

Communications Analysis

Communications analysis is a step by step tracing of the alignment between actual system state and the system state as perceived at any time by the operators. In effect it is an analysis of the communication links which preserve this alignment. The analyst must discipline the study by the assumed mental models he attributes to the members of the operating team; most importantly he must deduce at each stage not only what each operator knows or assumes (the "probability" model) about the system state but also what each operator believes to be the states of knowledge of the other operators.

The technique is best illustrated by reference to an actual system analysis. The system chosen for this example is a British railways signalling system, a system which was in use in the middle of the last century. By taking a system from the past we have the advantage of knowing something of its performance history.

The essential components of the system are illustrated in Figure 6. Essentially it constituted an information system designed to prevent the possibility of a rear end collision between two trains in a tunnel. The idea was simply to permit only one train at a time to occupy the tunnel in

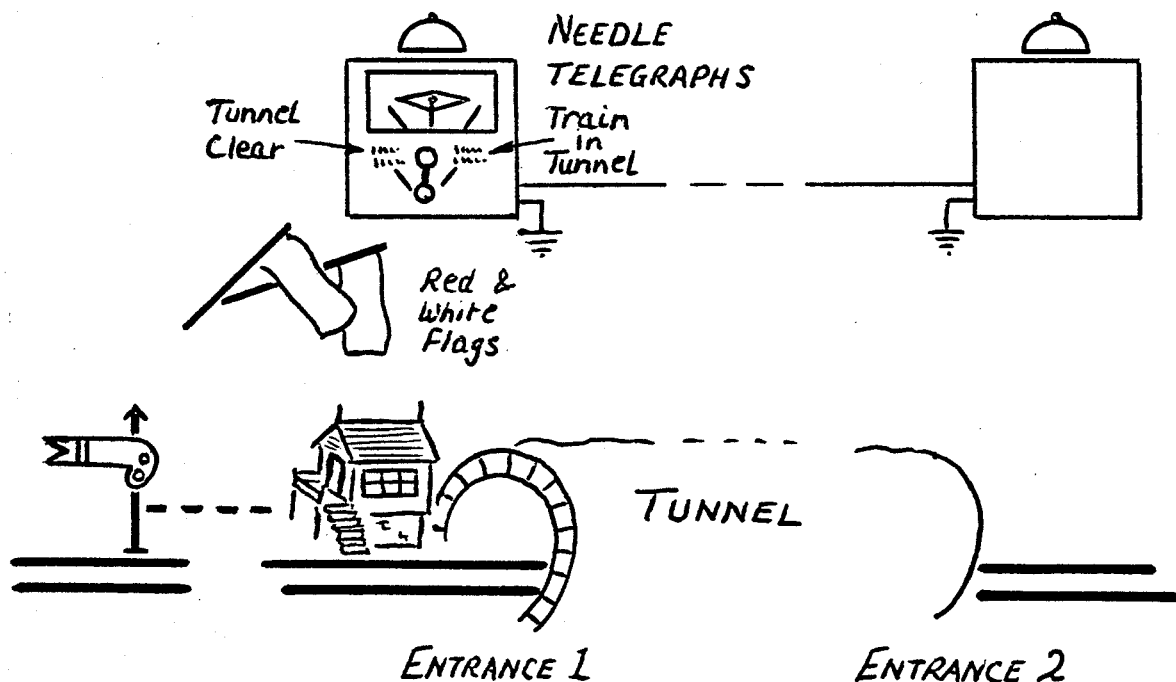


Figure 6. Signalling Arrangements for Rear End Collision Prevention

COMMUNICATIONS ANALYSIS

ACTUAL SYSTEM STATE		COMMUNICATION SEQUENCE	PERCEIVED SYSTEM STATE																		
			S ₁	S ₂	d ₁	d ₂	i ₁	i ₂	d ₁	d ₂	i ₁	i ₂	d ₁	d ₂	i ₁	i ₂	d ₁	d ₂	i ₁	i ₂	
A	TUNNEL CLEAR		A	A																	
	Train (D ₁) approaches	* ▷ D ₁																			
	S ₁ observes D ₁	D ₁ ▷ S ₁																			
	S ₁ sends "clear" to I ₁	S ₁ ▲ I ₁																			
	S ₁ observes I ₁ respond	I ₁ ▷ S ₁																			
	I ₁ sends "clear" to D ₁	I ₁ ▲ D ₁																			
	D ₁ sends "danger" to I ₁	D ₁ ▲ I ₁																			
	S ₁ observes I ₁ at "danger"	I ₁ ▷ S ₁																			
	D ₁ passes S ₁ & enters tunnel	D ₁ ▷ S ₁																			
	D ₁ observes he is in tunnel	* ▷ D ₁																			
B	TRAIN IN TUNNEL		B	B																	
	S ₁ sends t-t-t to I ₁	S ₁ ▲ I ₁																			
	I ₁ sends t-t-t to S ₂	I ₁ ▲ S ₂																			
	S ₂ sends "acknowledge" to I ₁	S ₂ ▲ I ₁																			
	I ₁ sends "acknowledge" to S ₁	I ₁ ▲ S ₁																			
	PAUSE: 1 1/2 to 2 minutes.																				
	D ₁ leaves tunnel & passes S ₂	* ▷ D ₁																			
	TUNNEL CLEAR																				
	S ₂ observes D ₁	D ₁ ▷ S ₂																			
	S ₂ sends t-c to I ₁	S ₂ ▲ I ₁																			
I ₁ sends t-c to S ₁	I ₁ ▲ S ₁																				
S ₁ sends "acknowledge" to I ₁	S ₁ ▲ I ₁																				
I ₁ sends "acknowledge" to S ₂	I ₁ ▲ S ₂																				
A			A	A																	

FIGURE 7. NORMAL SEQUENCE FOR TUNNEL SIGNALLING SYSTEM

any one direction. Trains travelling in opposite directions would be permitted to pass in the tunnel. A signalman, in his cabin, was situated at each end of the tunnel. A train entering either end of the tunnel would be observed by the signalman there who would immediately notify the signalman at the other end. This second signalman would watch for the emerging train and then immediately notify the first signalman. Meantime it was the first signalman's responsibility to prevent a second train from entering the tunnel until he received the 'tunnel clear' information. Each signalman communicated with an approaching train by means of a semaphore signal situated some 300 metres from his box and the tunnel entrance. Normally these signals displayed the "danger" indication (semaphore arm horizontal). When the tunnel was clear and he saw a train approaching the signalman would clear his semaphore signal (semaphore arm raised) thereby signalling the right of way to the driver. On passing the signal the train operated a treadle on the rail which automatically reset the signal to the "danger" position. Should the tunnel not be clear on the approach of a train the signal would be left at danger and the driver, observing this, would stop at the signal box until permitted to proceed. Each signalman was supplied with a white and a red flag for direct communication with the drivers. In addition, should the treadle fail to reset the semaphore signal to danger on the passing of a train a warning bell would ring in the signalman's cabin.

The two signalman communicated with each other by means of a pair of electrically connected "needle telegraph" instruments. The normal position for lever and needle was central. Operating the lever to the right or left gave the "train in tunnel" or "tunnel clear" signal, the needles in both instruments inclining to the right or left accordingly. In addition, the single-beat bell at the receiving instrument would respond. By use of bell codes a limited set of additional communications between the signalmen was possible. Finally, each signalman possessed a set of time-tables and a clock.

Figure 7. is the communication diagram which traces the sequential communication states as a train is worked through the tunnel. The two system states, designated A and B, are respectively "tunnel clear" and "train in tunnel". The communication stages are symbolised by arrowheads: a black arrowhead indicates a positive and specific act of communication, a white arrowhead indicates that the communication is an act of observation by the receiver. When a signalman communicates with a driver via the semaphore signal (this is a category (2) communication as defined in the previous section of this paper) the communication act is split into two phases, (i) between signalman and signal, (ii) between signal and driver. The same principle is applied to the needle telegraph instruments. Thus the train driver on observing the semaphore signal to be raised, concludes that the tunnel is clear, state "A", concludes that the semaphore signal knows this fact, state "A", and assumes that the signalman also knows this fact, state "a". The assumption is made on the basis that the driver's mental model of the system tells him that it is the signalman who is deputed to put the signal to "clear". The use of capital and small letters for the operators' knowledge of system states differentiates between directly communicated knowledge and that which is assumed. The perceived system states are systematically listed for all the operators.

S1 : Signalman at entrance 1
S2 : Signalman at entrance 2
D1 : driver of first train
D2 : driver of second train
D3 : driver of third train

Indicators Is : semaphore signal
It : needle telegraph system

The operators' designated symbols are given opposite.

FIGURE 8 - ACCIDENT SEQUENCE

ACTUAL SYSTEM STATE	COMMUNICATION SEQUENCE	PERCEIVED SYSTEM STATE	SYSTEM STATE	
A TUNNEL CLEAR D1 PASSES IS D1 SENDS 'danger' to IS IS indicates failure to S1 D1 enters tunnel	6 IS S1 D1	A a	A a	
	7 IS S1 D1	A a	A a	
	8 IS S1 D1	A a	A a	
	9 IS S1 D1	A a	A a	
	10 IS S1 D1	A a	A a	
	B TRAIN IN TUNNEL S1 → S2 (Train in tunnel) Train D2 approaches IS sends 'clear' to D2 D2 sends 'danger' to IS IS sends 'failed' to S1 D2 passes S1 S1 flags E-t to D2 D2 enters tunnel D2 in tunnel D2 stops & reverses (45 minutes)	11 S1 Ib S2 Ib *	B b a	B b
		12 S1 Ib S2 Ib *	B b a	B b
		13 S1 Ib S2 Ib *	B b a	B b
		14 S1 Ib S2 Ib *	B b a	B b
		15 S1 Ib S2 Ib *	B b a	B b
16 S1 Ib S2 Ib *		B b a	B b	
17 S1 Ib S2 Ib *		B b a	B b	
18 S1 Ib S2 Ib *		B b a	B b	
C (TWO) TRAINS IN TUNNEL S1 ← S2 (Train in tunnel) D1 PASSES S2 B (ONE) TRAIN IN TUNNEL S2 → S1 (tunnel clear)	19 S1 Ib S2 Ib *	B b a	B b	
	20 S1 Ib S2 Ib *	B b a	B b	
	21 S1 Ib S2 Ib *	B b a	B b	
	22 S1 Ib S2 Ib *	B b a	B b	
	23 S1 Ib S2 Ib *	B b a	B b	
	24 S1 Ib S2 Ib *	B b a	B b	
	25 S1 Ib S2 Ib *	B b a	B b	
	26 S1 Ib S2 Ib *	B b a	B b	
	27 S1 Ib S2 Ib *	B b a	B b	
	28 S1 Ib S2 Ib *	B b a	B b	
	29 S1 Ib S2 Ib *	B b a	B b	
30 S1 Ib S2 Ib *	B b a	B b		

SYSTEM IS NOW PRIMED FOR DISASTER WHICH WILL OCCUR IF D3 ARRIVES BEFORE D2 EMERGES FROM TUNNEL.

The use of capitals and small letters in the case of these symbols serves to discriminate between, for example, the system state perceived by S1 and the system state which S1 believes S2 perceives.

In building up the diagram the perceived state changes are noted as they occur. At any position, however, a total inventory of the operators' perceptions can be summarised merely by calling down each last recorded state. In Figure 7 perception-summaries have been made at each switching of actual system state. The 'dash' symbol indicates the 'neutral' state of mind, the symbol 'o' indicates 'out of the control area of the system' and the * symbol represents this same control area. Thus, * ▷ D1 means that the driver of train 1 observes that he is approaching the tunnel control area. The use of a question mark symbolises the "question" category of communication. (Category (4) in the previous section of this paper).

The normal system operating cycle is systematically traced and proved in Figure 7 where it can be seen that stage 1 and stage 20 in the communication sequence are identical. The communication diagram may also be used to check whether there are similar or identical intermediary stages within the perception of each operator. These present potential opportunities for sequence skip errors, liable to arise following some interruption or distraction.

However, the principle use of the diagram is to trace the developments following some system state abnormality. Figure 8 illustrates a possible sequence following a failure of the first train to successfully reset the semaphore signal to "danger" — stage 7 in the communication sequence. The sequence of Figure 8 is pursued using a logical application of the operators' mental models of the system with which they are dealing. This particular sequence is given as it was one which actually occurred in Clayton tunnel on the Brighton to London line. On Sunday, 25th August, 1861, a violent rear end collision caused 23 deaths and 176 serious injuries. It is ironic to note that without the signalling system the particular accident would not have occurred.

The sequence, briefly, was this. Train 1 approached a clear tunnel and was signalled to proceed by signalman 1. However, the passing train failed to reset the semaphore signal to danger and immediately the warning bell rang in signalman 1's cabin. Before dealing with this, signalman 1 sent the "train-in-tunnel" signal to signalman 2 who acknowledged. Then signalman 1 turned his attention to the semaphore signal only to find that train 2 already had passed the signal and was about to pass his cabin. In great hurry he displayed his red flag as the train entered the tunnel. He then had no means of knowing whether or not the driver of train 2 had seen his danger flag. He again sent the "train-in-tunnel" signal to signalman 2 who again acknowledged. Signalman 1 hoped that signalman 2 had registered "two trains in tunnel". Signalman 2 apparently concluded that his first acknowledgment had not been received and so the signal had been repeated. In due course train 1 emerged from the tunnel and signalman 2 sent the "tunnel clear" signal. Signalman 1 concluded that both trains had passed through and permitted the entry of a third train which had now approached. The driver of train 2 however had seen the red flag, had stopped in the tunnel and was in the process of reversing back out

Psychological Error Mechanisms

At first sight the numbers of ways in which we can make errors in our minute by minute progression through life would appear to be enormous; and yet, in various guises, certain basic mechanisms occur again and again. One has already received considerable attention in previous sections of this paper — namely, the problem of communication — and no more need be said here. However, three other mechanisms are worth mention since every-one of us will have regularly experienced at least two of these and the third is a recurring factor in many accident situations.

(i) Memory failure: A pan of milk is placed on the stove and heated. In many households the chances are barely less than one in three that the milk will boil over before the heat is removed. It appears to be a regularly occurring situation of memory failure. With very much more severe results railway signalmen have temporarily routed a goods train onto a main line, have then forgotten the fact and have subsequently signalled an express through on the same line. It became a well known hazard and led to a variety of safe guards to prevent its occurrence. Recent analysis of American Licencee Event Reports (LER's) for nuclear plants have revealed the same mechanism as the human error (the so called unrelated task error) which most frequently occurs.

In the section of this paper which discusses the structuring of mental models the mind is described as a vast multidimensional associative structure, like a string net where the knots are ideas (units of recognition) and the strings are the associative links between them. The conscious mind, like a viewing frame tracks from idea to idea, as the associative links dictate, and in its tracking process preserves only a short-lived image of where it has been. Thus, if we pursue a task to a certain stage and then for one or other reason break off to undertake another task, if this second task requires a new train of thought and also endures for more than, say 10-15 seconds, the memory of the first task will have completely gone. We are then dependent upon the presence of an effective external cue (one which can communicate with a U-category receiver, as defined in the section headed 'Communication) to re-associate with this first task. The boiling over of milk is one such cue. Normally these cues are present in our daily actions, and we are recalled to tasks without being aware of the means by which this occurred. We simply assume that we "remembered". In certain cases the necessary cue may arise in the internal mental processes without external prompting but it is a chance affair.

Given that the foregoing explanations are correct the likelihood of memory failure will be greatly reduced if in situations where parallel operational tasks are identified, the designer ensures the presence of cues which are both relevant and boldly conspicuous.

(ii) Pre-experience take-over. This phenomenon has been known to occur at times of heightened relaxation on the part of the operative. However, it is more frequently associated with instances of heavy time stress when the operative is attempting to respond rapidly to an emergency situation. In Figure 2 there is depicted the process of thought in which the viewing frame of the conscious mind expands to take in the less and less strongly associated 'units of recognition'. It is suggested that this expansion process consumes time and energy; neither of which are willingly spared at the instant of a perceived emergency. It is perhaps a fair analogy to

suggest that where fast mental response is demanded the conscious mind viewing frame is extremely reluctant to expand and therefore follows the route of strongest association. If the strength of an earlier response pattern has not become superceded the stage is set for pre-experience take-over.

One mitigating approach which designers could adopt is to attempt to standardise on emergency response patterns, particularly in the layouts and handling of emergency controls and indicators. Alternatively, the frequent exercising of such responses in regularly repeating sessions will work to obliterate this phenomenon.

(iii) Risk blindness. In the event chain of many accidents can be detected an action or lack of action which flew in the face of required safe practice. It is the psychology which causes operators to run machines without safeguards, to take a host of short-cuts in the avoidance of inconvenience. It is the logical outcome of a weighing of the hard fact of inconvenience on one hand against some nebulous theory of risk on the other. In many cases the operatives will not even know why a particular facet of safe practice is specified. We do not easily foresee many moves ahead in the developing pattern of events. Few operators will appreciate the significance of freely sacrificing one link in the potential hazard chain.

Two positive steps can be taken to combat the mechanism of risk blindness. Firstly, the reason for safe practice should be clearly advertised in each application; secondly, specific attention should be given to ways of reducing the inconvenience of applying it.

Conclusions

A theory has been proposed relating to the structuring of mental models and this theory used to account for a number of human error mechanisms. Communications amongst operators and the systems around them is seen as a vital factor in the area of human error and a technique, communications analysis, is proposed as one approach to systematically predicting the ways in which actual system state and the operators' perceptions of that state can get out of step and lead to catastrophe. To be most effective it is expected that the analyst would apply communications analyst with an interactive computer system. Of particular importance is the ability to trace the operator-system communication scenarios in various abnormal system configurations.

K. Netland

MEASUREMENT OF OPERATOR PERFORMANCE - AN EXPERIMENTAL SETUP

MEASUREMENT OF OPERATOR PERFORMANCE

- AN EXPERIMENTAL SETUP

by

K. Netland

OECD Halden Reactor Project

ABSTRACT

Without doubt, the human has to be considered as an important element in a process control system, even if the degree of automation is extremely high. Other elements, e.g. computer, displays, etc., can to a large extent be described and quantified. The human (operator), however, is difficult to describe in a precise way, and it is just as difficult to predict his thinking and acting in a control room environment. Many factors influence his performance, such as: experience, motivation, level of knowledge, training, control environment, job organization, etc. These factors with many others have to a certain degree to be described before guidelines for design of the man-process interfaces and the control room layout can be developed. For decades, the psychological science has obtained knowledge of the human mind and behaviour. This knowledge should have the potential of a positive input on our effort to describe the factors influencing the operator performance. Even if the human is complex, a better understanding of his thinking and acting, and a more precise description of the factors influencing his performance can be obtained.

At OECD Halden Reactor Project an experimental set-up for such studies has been developed and implemented in the computer laboratory. The present set-up includes elements as a computer- and display-based control room, a simulator representing a nuclear power plant, training programme for the subjects, and methods for the experiments. Set-up modules allow reconfiguration of experiments.

Paper to be presented at the Specialists' Meeting on
"Procedures and Systems for Assisting an Operator during
Normal and Anomalous Nuclear Power Plant Operation Situations".

Münich, Germany, 5th - 7th December, 1979.

INTRODUCTION

The use of computer driven colour displays as information carrier in control of complex processes has shown an increasing trend in the last years. The background for introducing such devices into the control room either as a supplement to an already existing conventional instrumentation or as the sole man-process interface is both of an economical character and a desire for a better and more safe control. The safe control, however, is also dependent on many factors that relate to the performance of the control room operator and of the other personnel that support the production. These factors are more or less easy to measure or describe.

This paper describes some work that are in progress or being planned at the OECD Halden Reactor Project for experimentally measurement of factors that influence the operator's performance in control of complex processes. The ultimate aim of the experiments is to develop guidelines for design of colour display based man-process interfaces that minimize human failures in supervision and control of such processes. Even if these studies of operator's performance are based on extended use of computers and colour monitors, the knowledge gained of the human thinking and acting should be of interest also for the design of other types of interfaces.

To develop guidelines for design of colour displays, much effort has still to be done, i.e. to evaluate the various hypotheses developed. These evaluations have to be done experimentally in the most realistic environments available, since testing directly on plants in operation can be too risky and costly. The simulation studies will to a large extent be based on scenarios where relevant operational problems can be investigated.

FACTORS INFLUENCING OPERATOR PERFORMANCE

It is difficult to describe in a precise way the human as an element of a control system, and just as difficult to predict his thinking and acting in all the diverse situations that can come up in a control environment. However, to be able to describe and design his role as a part of the production process, and to design a proper information system, it is a necessity to have knowledge of the human behaviour. For decades the psychological science has obtained knowledge of the human mind and behaviour. By merging the experience and knowledge of psychologists and process engineers we will obviously gain positive results in our efforts to design a more proper control room.

Figure 1 indicates some of the factors that influence the human performance in controlling complex processes. Some of these are easy to control, while others are more difficult to get hold of.

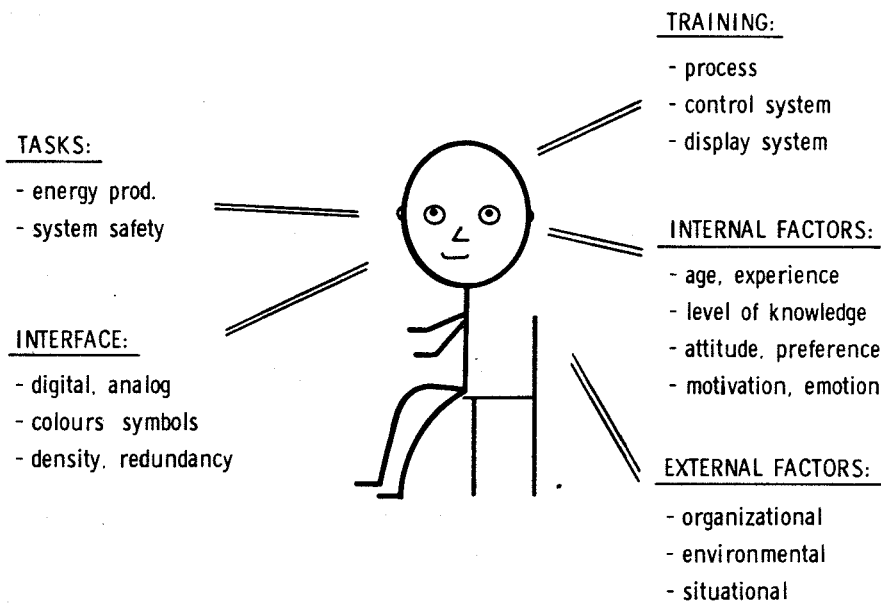


Fig. 1. Factors Influencing Operator Performance

Internal Factors

This group contains factors such as emotion, experience and level of knowledge of the relevant sciences. Regarded independently, these factors are to a certain degree controllable, but specific combinations may be impossible to obtain, e.g. young people with long experience or older people with keen colour perception. Experience is normally a positive element, but can be of negative influence when misunderstandings have been allowed to develop during years of veiled malpractices caused by lack of retraining and refreshment of process knowledge. Habit may be a negative factor in retraining operators for a completely new type of control room. Perhaps recruitment of new, unbiased personnel is more beneficial. The level of knowledge (formal education) can be controlled through selection in recruitment, but higher level of education may be contaminated by factors such as motivation and preferences.

The operator's type of education and background influences his way of "abstract thinking" and preferences for different displays. Information of plant

status presented in mass-balance or energy-balance diagrammes giving a direct and pointed information, or in the traditional circuit diagrammes is such an example of different "levels of abstraction".

Factors as attitude, preference, motivation and emotion are rather difficult to control. They should therefore be considered having a certain variance when designing control systems.

External Factors

Factors within this group are such as the physical environment (light, temperature, etc.), the organization model and the situational factors in the control room. The physical environment can for normal operation be given a neutral influence on the operator's performance. The organizational aspect can to a certain degree be given a positive form, but is obviously more complex since elements such as the operator's role, status and position in the overall organization has an impact. His position in the organization will also be dependent to some degree on his level of education. In regard to the situational factor: How is the operator's actions influenced by disturbance of others present in the control room, or what about his thinking and acting while in serious plant anomalous situations?

The Influence of Training

This includes both the pre-operator training and the operator retraining in control and supervision of the process in question. The training content and how it is exercised is again dependent on other factors like the level of knowledge, the degree of automation of the control system and hence the operator's role in the whole production process. Coarsely, the operator performs his tasks within three overlapping modes:

- rule based (according to procedures)
- knowledge based (his process knowledge)
- skill based (his experience)

The performance level of rule and knowledge based actions can be increased by the amount and quality of training. The performance level of skill based actions, on the other hand, depends mainly on the experience from the actual or similar control room situations. Most of the tasks in supervision and control of complex processes is rule based, which should give little room for the probability of

mal-operations. This is true, however, only for pre-conceived situations. When unforeseen situations occur, rule based actions may render unsafe or undesired actions in contrast to knowledge based actions. Process knowledge is also a prerequisite for rule based actions in that it should at all times be known which procedure to follow.

Another performance influencing factor is the understanding of the control system and the particular display system, e.g. to distinguish between abnormal and normal functioning of the automatic control system.

The Influence of Man-Process Interface

When driven by computers, colour displays as information carrier gives a huge amount of possibilities in information presentation. However, bad display design and wrong use of colours and symbols can lead to misinterpretation of the displayed information. Relative to a conventional control room, bad design of a computer and display based information system can easily lead to grave consequences. This assumption originates from the nature of the two types of information presentation. A conventional control room has the nature of parallel information presentation, i.e. the particular information is "somewhere" ever-present in the control room. In a computer driven display based control room the information presentation is more based on operator requests on a few display units; therefore a bad display design can "hide" relevant information.

To give the operator the tool for improved plant availability - and safe operation of the plant, which such a computer and display based system have the potential to, many new problems have to be solved. Such problems are for instance information presentation in digital, analogue or functional form, or any combination of these. The additional dimension of using colours dynamically has to be correctly applied. Further, the objective information density - or display load- depends on various factors like frequency of use and task load. Redundant information, i.e. different variables indicating the same process state, is possibly necessary for the operator for verification before he is willing to decide a corrective action.

An autonomous problem area is how to present the current alarm situation not only on a dedicated display unit, but also to reflect it through all process information. In a conventional control room a huge amount of "alarms" are always present on the annunciators. The operator has to analyse by himself

which of these "alarms" are real or relevant. Application of computer programmes that analyses the "alarm pattern" can filter out the relevant alarms for display. This can be one of the main advantages of computers in process applications.

ELEMENTS OF AN EXPERIMENTAL SET-UP

An experimental set-up has been designed and implemented in the computer laboratory at the Halden Reactor Project to study some of the factors that influence the operator's performance. In Figure 2 is indicated the main elements included in the design, which can be summarized to:

- computer and display based control room
- digital simulator representing a nuclear pressurized water reactor
- selection of subjects to act as operators, and design of their training
- system for control and supervision of each particular experiment
- development and implementation of hardware and software that are specific for each particular experiment

Any redesign of the various elements is obviously limited due to cost and work capacity. Still many of the factors influencing operator's performance can be varied; the flexibility of the set-up should be reflected in the discussion of some of the main elements below.

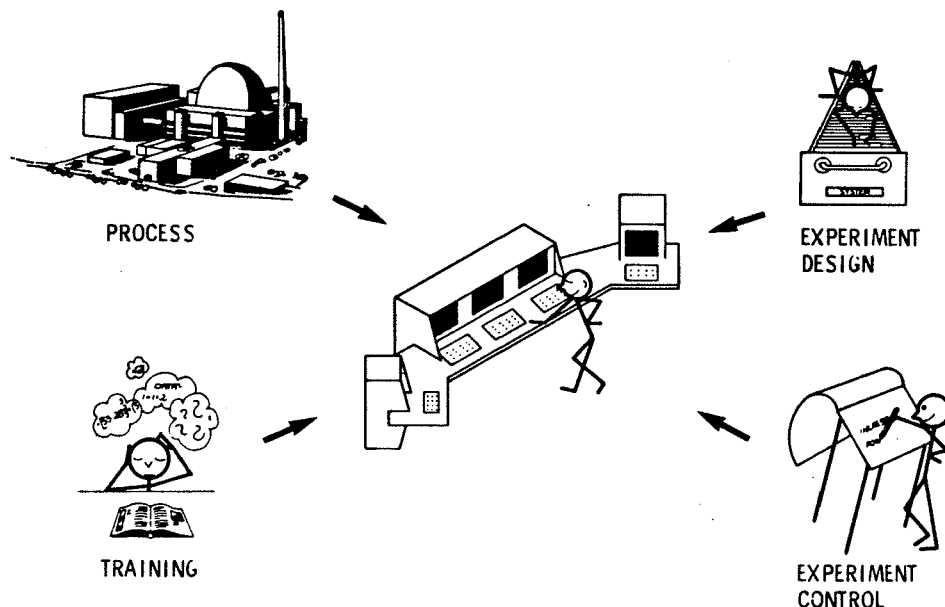


Fig. 2. Elements in Experiment Set-Up

Colour Display Based Control Room

The design of the experimental control room is based on long time experience at the Institute. However, as seen from either the user (operator) or from a pure technical point of view (designer), the design has obviously changed during this period. The present control room architecture and the display and keyboard design reflect years of research in this field, see Figure 3.

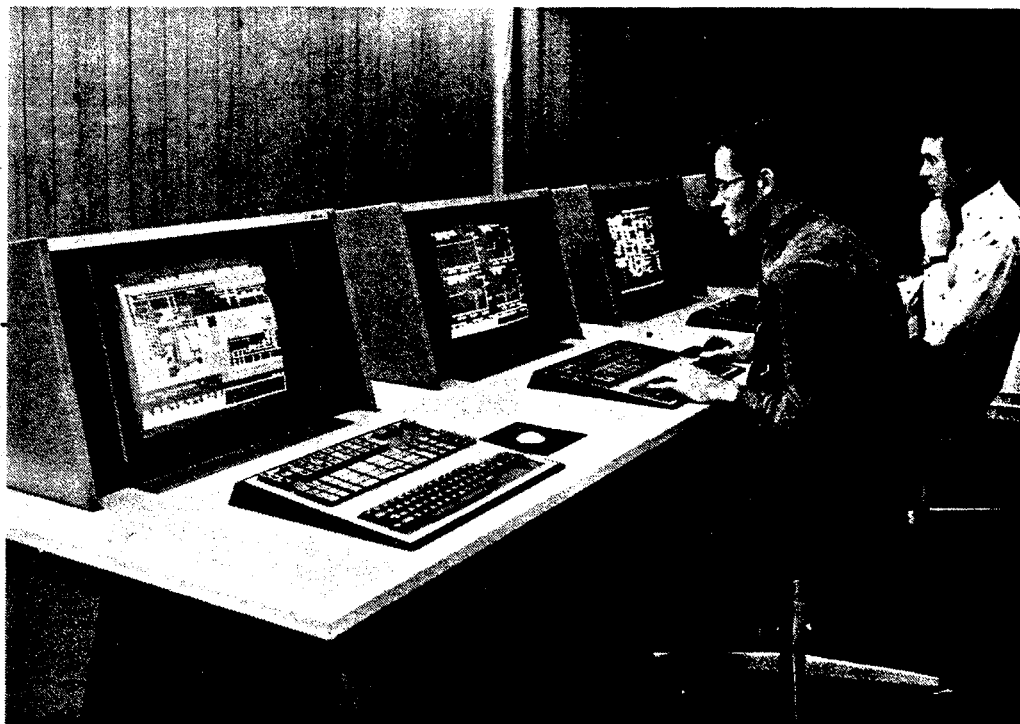


Fig. 3. Colour Display Based Control Room

In the main control desk one module comprises a standard colour monitor, a function keyboard, an alphanumeric keyboard, a pointing device (tracker ball), a controller that supplies the monitor with colours and symbols; and finally a computer that controls all these devices and communicate with all the computers involved in the set-up.

The colour monitors installed are of a professional type with high quality characteristics on parameters like focusing and convergence. In order to verify some of the technical data supplied by the manufacturer, the brightness level and the spectral colour distribution has been measured physically. Thus, valuable data about the characteristics of the most frequently used colour monitors exist at the Institute.

The design of the function- and alphanumeric keyboards is based on experimentation and on industrial applications. The buttons on the function keyboard can be randomly grouped within a matrix of 8 by 20 buttons, the group geometry can thus be adapted to any user requirement. The alphanumeric keyboard has a standard layout. As a pointing device the tracker ball has proved itself very effective for addressing purposes in the picture, for manoeuvring of valves, pumps and so on.

A semigraphic display controller is included in the communication module. Semigraphic means that graphic displays are produced by combining element symbols to a whole; e.g. a valve on a pipe-line is made of adjacent element symbols, one for the valve and a number for the pipe-line. The screen is arranged in a 48 by 64 matrix for element symbols; the controller can generate 16 foreground and 8 background colours simultaneously, while a much higher number of colours is programmable.

The arguments for having a separate computer in each of the modules are based on design principles of a highly reliable computer structure. If one of the modules fails, the operator can switch to an adjacent module without restrictions in the man-process communication. Another main argument is to minimize the response time on operator's request.

Pressurized Water Reactor Simulator

The simulation of the process, as it is seen by the operator, is done to a rather realistically detailed level. The implemented simulator is based on a development work done in Studsvik, Sweden, augmented with a detailed feedwater system and an advanced playback system.

Included in the simulator are:

- reactor core
- primary cooling
- three steam generators with feed water system
- two turbines with generators and two condensors
- chemical and volume control system

The system control includes automatic control of core, borating and dilution, the feedwater system and turbine, the steam dump system and of the reactor protection system.

The reactor core is simulated in the axial dimension only and includes the neutronics and the fuel and coolant dynamics. The main pumps of the primary coolant system will always be in operation, resulting in a constant flow in all three main loops. The volume and pressure dynamics as well as the boron concentration of the primary coolant are simulated. Each of the steam generators has its own feedwater control system. Steam generator and hot well levels are maintained either automatically, or manually through operator control of valves and pumps. Each of the two turbines are controlled by separate control systems. The reactor protection system can induce reactor trip and turbine runback, and can block control rod withdrawal.

The dynamic simulation is initiated from a separate terminal. It can be freezed at any time and for any period to allow procedural or operational discussions. The playback facility renders the possibility to recall any situation or event. All data included in a complete experimental run, both process history and man-process communication, is stored continuously on a disk file. This facility is of special interest when the so-called "confrontation method" is applied (described later in this paper).

Malfunctions can be initiated by the experimental supervisor from a separate terminal. The following malfunctions are presently simulated:

- turbine trip
- load rejection
- condensor fault
- illegal opening of dump valve
- electrical grid disturbance
- fault in feedwater controller
- primary system leakage
- control rod droppage
- faulty automatic rod control
- faulty pumps and valves (pump stoppage, stuck valves, etc.)

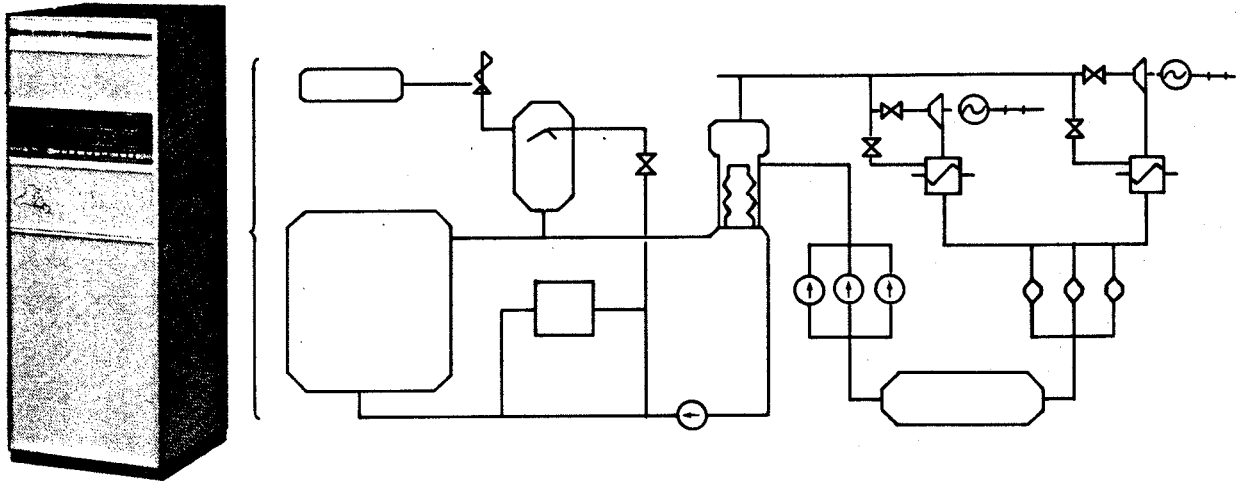


Fig. 4. Pressurized Water Reactor Simulator

Selection and Training of Subjects

As stated above, the man-process interface design depends on various factors. To be able to study the influence of each of these factors on the operator performance, groups of subjects with different background and experience will act as operators. The Institute is in contact with different organizations in the vicinity that may offer a range of subjects, e.g. a college for process engineers, a computer science college and the operators of the reactor plant.

Prior to the actual experimentation the subjects are trained sufficiently for the necessary understanding of the process and for the familiarity with the existing man-process interface. A training programme has been developed to prepare the subjects as reactor operators for particular experimental designs. The theoretical part of the training intends to give a basic process understanding up to a level where elementary operating tasks and plant disturbances can be handled. Dependent upon the subjects' background and level of process knowledge, this training may span from the fundamentals of the functioning of various plant components in the circuits to a global comprehension of the relation between the sub-circuits and the resultant final output.

The practical part concentrates on the man-process communication so that the process control system and execution of manual control is conceived, the various possibilities for information flow such as status information and alarm pattern is highlighted.

The main items of the developed training programme are:

- a general orientation and background survey for the current experiment and description of the existing set-up characteristics
- nuclear physics, from the nature of the nucleus and the phenomenon of fission, via reactivity and criticality concepts to the conditions for maintaining a chain reaction
- description of the various process systems and the plant components, their identification and symbolic representation in displays; the alarm philosophy and presentation
- an outline of safety philosophies and the use of procedures and manuals
- practical training in man-process communication in the current control room

EXPERIMENTS BASED ON "CONFRONTATION METHOD"

During the past years a cooperation between organizations within the Nordic countries has resulted in a data accumulation of control room operator functioning. These data have led to the formation, planning and design of a series of experiments in order to study the factors of human performance and reliability related to computer based control rooms with colour displays.

In some experiments already performed the method used may be identified as the so-called "Confrontation Method". In this particular set-up (see Fig. 5) is implied that a subject performs a predefined operational task. While doing so, the experimental supervisor may introduce a plant malfunctioning that should be seen, identified and corrected by the subject. All process data and the subject's actions are logged on file. A number of plant parameters and all actions are additionally logged on-line on hard-copy units.

From the filed data the process history and the subject's actions can be replayed. Thus, the experimental supervisors (a psychologist and a process engineer) can confront the subject with every action done and the subsequent consequences, and inquire why so and so was done in the various situations.

It is hypothesized that in this way the subject will reveal the structure of his mental model of the process, and his way of handling the task situation based on the current displays.

As indicated above and shown in Fig. 5 the experimental run is followed by a replay. The subject is active during the first part and passive during the replay where any influence on the process history is inhibited. The replay of a particular experimental run can be repeated anytime and for an unlimited number of times.

An initial series of experiments with a group of computer science students acting as operators has already been run through (see photo below). The resulting data are currently under study. The design of a new series of experiments has been initiated, this time with operators of the Halden Reactor acting as subjects. These series are scheduled to take place early next year.

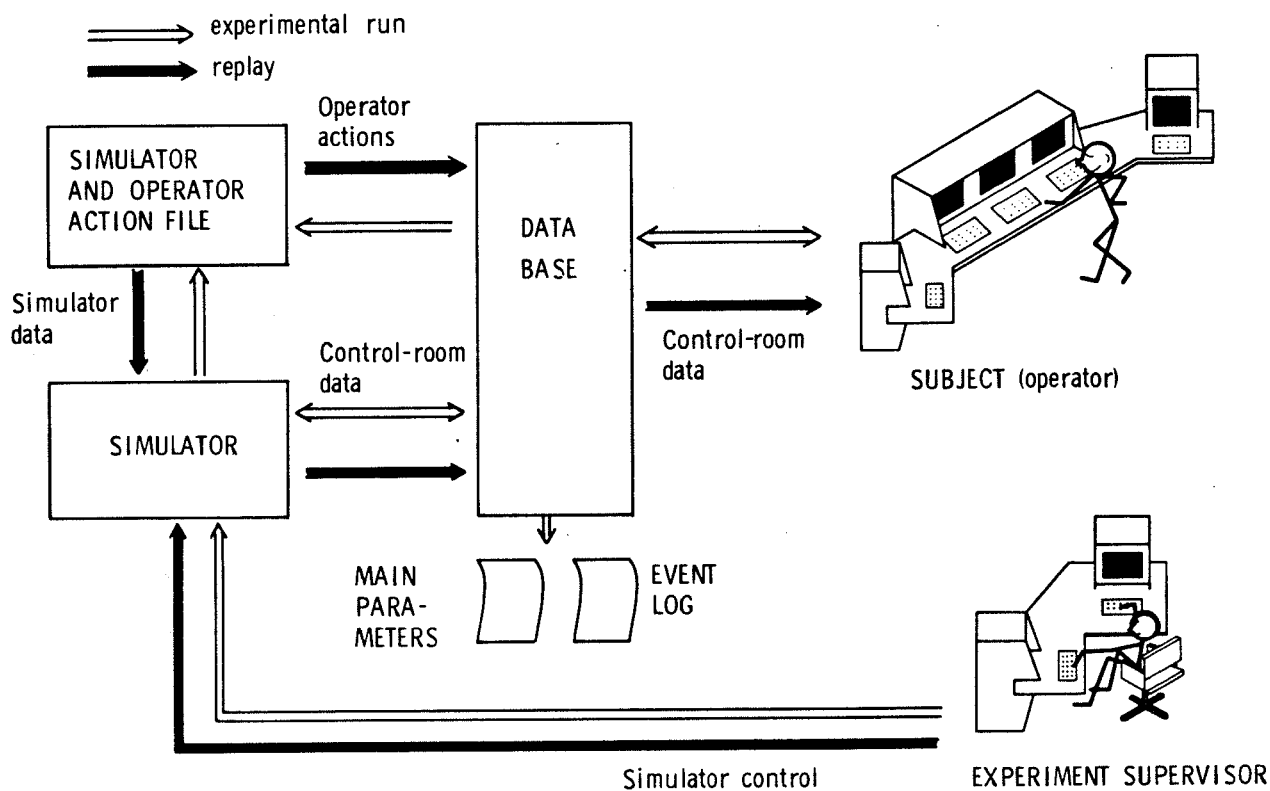


Fig. 5. Structure of the "Confrontation Method" Set-Up

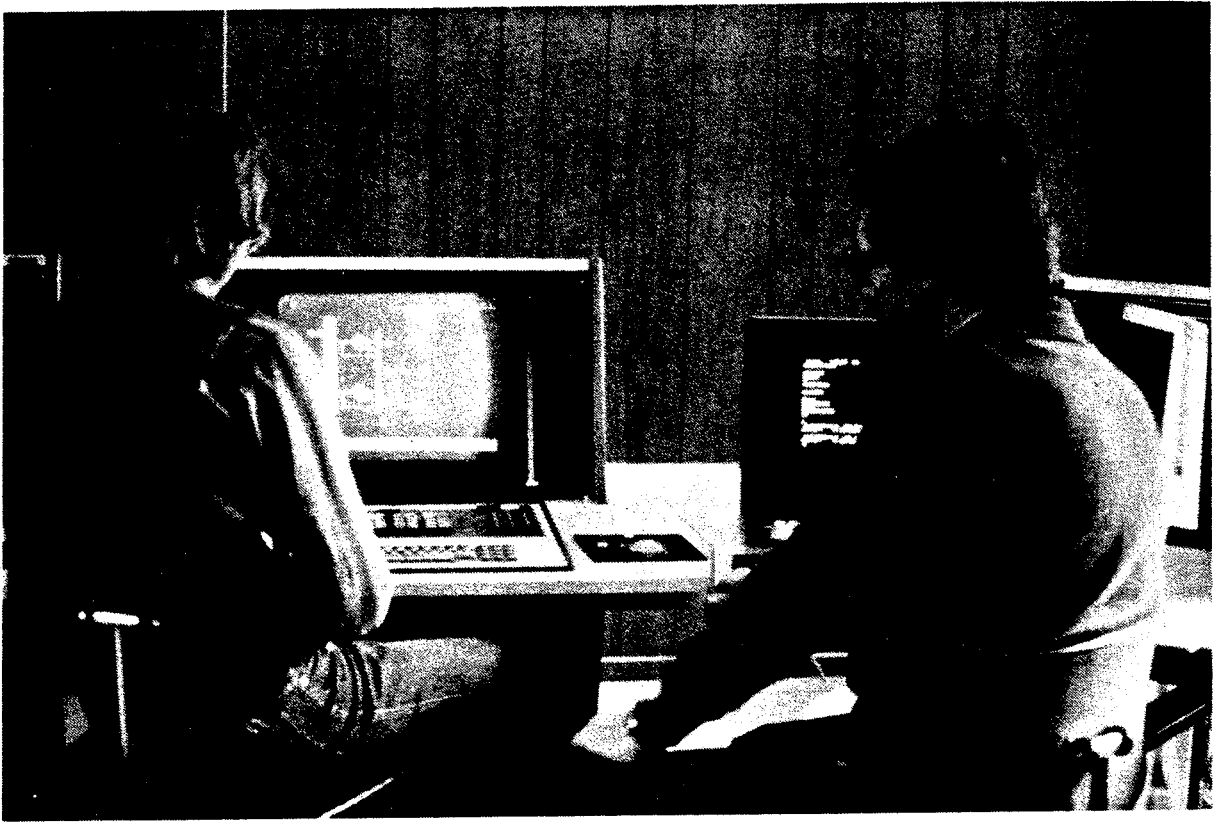


Fig. 6. Subject and Experimenter discussing the Event

LIST OF REFERENCES

1. K. Netland and J. Ø. Hol: "Development of a Computer and Colour Display based Control Room for Experimental Operation of the Halden Reactor". Halden Project Report 202-1977.
2. J. Rasmussen: "Notes on Diagnostic Strategies in Process Plant Environment". Risø National Laboratory Report, Denmark, 1978.
3. K. Netland, J. Ø. Hol and G. Øhra: "Operator-Process Communication in a Computer-Based Control Environment". Symposium on Process Supervision and Control in Nuclear Power Plants, Enlarged HPG Meeting, Fredrikstad, Norway, 1977.
4. F. Pettersen, T. Olsen: "Considerations for Design of a Modular Operator Communication Console". Enlarged HPG Meeting, Fredrikstad, Norway, 1977.
5. J. Wirstad: "On the Allocation of Functions between Human and Machine". Ergonområd, Sweden Report - 1979.
6. R. Stokke, B. Fagerstrøm: "STUDS - A Simulator Tool for Control Development". Enlarged HPG Meeting, Fredrikstad, Norway, 1977.
7. J. Ø. Hol, G. Øhra and K. Netland: "Design of Pictures and Use of Colours and Symbols for a CRT based Supervision System". Enlarged Halden Programme Group Meeting, Loen, Norway, 1978.
8. P. G. Sjølin, B. Wahlstrøm, J. Wirstad: "A Task Analysis for the Planning and Operator Training in Nuclear Power Plants". Enlarged HPG Meeting, Loen, Norway, 1978.
9. P. E. Blomberg, R. Josefsson, F. Åkerhielm: "Simulators for Training of Nuclear Power Plant Operators and Technical Staff". IAEA/NPPCI Specialists' Meeting, Studsvik, Sweden, 1976.
10. M. Holmgren, J. Ø. Hol: "Information Presentation in Computer Based Control Rooms - An Experimental Design". Internal Working Paper, OECD Halden Reactor Project, 1978.
11. E. Hollnagel: "Design Criteria for Experiments on Reference Situations". Risø National Laboratory Internal Report, Denmark, 1979.

L.P. Goodstein

PROCEDURES FOR THE OPERATOR, THEIR ROLE AND SUPPORT

PROCEDURES FOR THE OPERATOR
THEIR ROLE AND SUPPORT

L.P. GOODSTEIN

IWG/NPPCI SPECIALISTS' MEETING ON PROCEDURES
AND SYSTEMS FOR ASSISTING AN OPERATOR DURING
NORMAL AND ANOMALOUS NUCLEAR POWER PLANT OPE-
RATION SITUATIONS.

5-7 December 1979 - Garching, Federal Repub-
lic of Germany

PROCEDURES FOR THE OPERATOR - THEIR ROLE AND SUPPORT

L.P. Goodstein
Risø National Laboratory
DK 4000 Roskilde, Denmark

INTRODUCTION

Written procedures play an important role in the control by management and regulatory authorities of costly and potentially hazardous facilities. For example, in the United States nuclear field, there exists the legal requirement that "activities affecting quality shall be prescribed by documented instructions, procedures or drawings (These) shall include appropriate quantitative or qualitative acceptance criteria for determining that important activities have been satisfactorily accomplished"

(1). This requirement is reflected in working specifications such as ANSI N18.7(1976) covering "Administrative Controls and Quality Assurance for the Operational Phase of Nuclear Power Plants" which, among other things, covers the preparation of instructions and procedures. Applicable types of procedures include:

- systems procedures (energizing, filling, draining...)
- general plant procedures (startup, shutdown, power operation and load changing, fuel handling, process monitoring)
- maintenance
- radiation control
- calibration and test

- chemical-radiochemical control
- emergency
- test and inspection

In the eyes of its designer or regulatory auditor, a procedure is, by definition (2),

"a manner of proceeding in any action or process and implies a formal set method of conducting affairs. Properly prepared, tested, and used, written procedures standardize the conduct of operations, eliminating, to a great degree, the influence of "personal preference" by applying emphasis on the order in which operations are to be performed, thus accomplishing the task the same way every time, in accordance with an approved method. Written procedures provide qualitative and quantitative guides by which the satisfactory accomplishment of the task can be measured, items requiring increased cognizance are flagged, and expected responses or results are indicated, thus allowing operators to rely less on memory and to concentrate on evolutions in progress".

In practise, of course, there often arise conflicts between, on the one hand, the desire for a "formal set method of conducting affairs" and, on the other hand,

- (a) the involvement of humans in carrying out procedures
- (b) the dynamic environment which characterizes a typical modern industrial process plant.

Analyses of event reports will readily substantiate the existence of these conflicts in the form of so-called "procedural errors" and the like. The situation in the U.S. was characterized by NRC as follows (3):

1. A significant fraction of the event reports reported to NRC for the past several years is attributed to operator error. We believe that deficiencies in procedures are one of the major contributing causes.

2. Our inspectors find it necessary to do far too much "jaw boning" about procedures in the field.
3. A significant portion of the items of noncompliance found during inspections involves procedures.
4. The development of procedures is relegated to nearly last place in preoperational preparations of most licensees..... NRC must then mount a tremendous last-minute review effort prior to finding a facility complete. In several cases; startup delays have resulted. We are sensitive in this area and cannot consider a facility ready for operation without a sound procedural base.
5. We find instances where personnel have failed to follow procedures.

In the light of this experience, it can be useful to take a fresh look at procedures by first examining the operator's work situation, his behavioral characteristics and then at his need for suitable support, for example, in the form of procedures - and all of this in light of his responsibilities for monitoring and controlling a dynamic, complex and occasionally unpredictable process. An added impetus for doing this exists in the form of the process computer and the possibilities which it offers for providing support for procedures. This paper concludes with a brief description of such an application.

THE OPERATOR'S WORK SITUATION AND THE ROLE OF PROCEDURES

In our studies of the human operator (see, for example (4) - (7)), we have treated the human as an information processing system and have sought to describe his possible behavior in terms of concepts such as:

- operator models or representations of plant properties
- operator-utilized data categories
- operator strategies for utilization of these data in the light of his knowledge and skills and his goal.

One result of this work has been a framework for studying the operator's interaction with the plant in the performance of a diagnostic task. This ladder representation taken from (5) and shown in simplified form on Fig. 1 locates and connects the various elements which comprise the complete cycle of diagnosis.

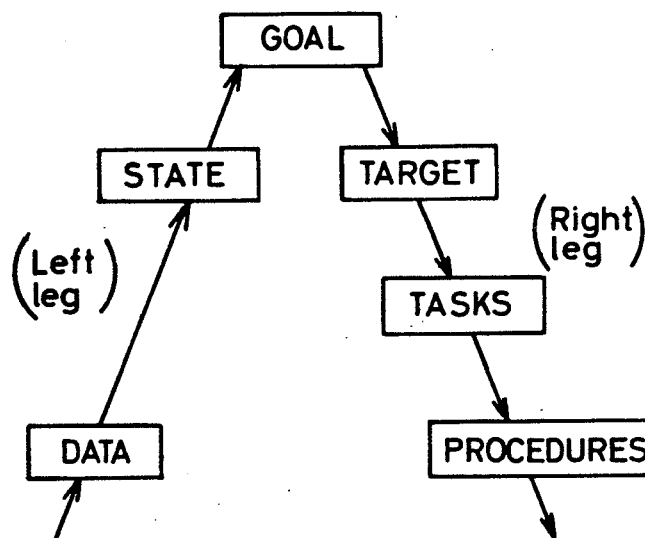


FIG. 1.

Thus, in response to an "alert" in the form of an alarm or from normal monitoring, the operator essentially traverses the left leg of the ladder in an upwards direction as he observes the available data, identifies the plant state and, on the basis of current goals, standard operational practice, etc. selects the appropriate target state (shutdown, setback,..) for averting/correcting the identified situation. Then the right leg is traversed in a downward direction as the operator plans the necess-

ary set of tasks and thereafter executes the sequences of actions required to achieve the target state. Traversing the two legs of the ladder reflects different forms for activity. Coming down the right leg, the operator's data processing proceeds from the general to the specific. That is, the present state is....; conditions are; what sequence of operations on the plant is necessary in order to reach the target state. Thus the operator is concerned with the planning and carrying out of a set of tactical maneuvers structured on the basis of operational procedures made up of operator-independent sets of rules for proceeding from a given state to another given state by means of a series of prescribed actions and manipulations with respect to the plant.

This stressing of on the plant is to emphasize a primary difference between, on the one hand, right leg tactics for plant control and, on the other, left leg strategies which underlie the operator's own internal speculations about possible plant state(s) which could account for the perceived data. Left leg processing can thus be said to be operator-centered - as opposed to the plant - and comprises elements of observing, weighing, inferring, testing and evaluating which, especially in non-stereotyped situations, (should) reflect a conscious, goal-controlled activity drawing heavily on a solid base of plant knowledge. Being highly operator-dependent, the very nature of this type of data processing makes it quite incompatible with the idea of proceduralization as defined, for example, in (2).

Humans are flexible, adaptive and subject to considerable variability. They are adept at improvising but, as a result, their

behavior is not always predictable. Depending on one's viewpoint, therefore, operators are usually employed because of (or in spite of) these characteristics - firstly, to co-function with the automatic control system in carrying out the normal daily routines and for dealing with foreseen disturbances and, secondly, to cope with the rare and possibly critical situations which the designer did not consider. Besides giving rise to potential problems with regard to the sharing of responsibility between operator and designer, the above spectrum of activities can have other disadvantages. For example, the skills attained in connection with daily operations and minor disturbances may not be applicable or indeed can conflict with those required for dealing with rare and unfamiliar events. This state of affairs has led to the description of the operator/pilot's job as consisting of 99% boredom and 1% sheer terror (12).

Analyses of event reports (8) tend to verify this in that, in everyday tasks, errors are concentrated by far on planning, recall and execution of procedures - i.e., in connection with right leg activities. For example, if a procedure is repeated often enough, its execution will become automatic and efficient with the danger that occasional deviations from normal which might affect either the selection or the execution of the procedure may not be responded to. In addition, interference among similar procedures can occur. Reliance on memory can be disastrous. On the other hand, problems with identification do not appear to be prevalent.

However, errors in connection with major accidents (rare events) can often be referred back to left leg activities in that oper-

ators are unable to utilize the available information collectively in a functional context to make inferences about system state. Instead, they rely heavily on individual indicators which, with experience and training, have become the principal signs of familiar operational states.

These results demonstrate that there are at least two areas with an obvious need for improvement:

- better procedural support for right-leg activities
- better and more integrated displays of plant state and properties for left-leg activities.

The rest of this paper will deal with the first of these. For a discussion of the second, see (9) where a suitable set of design criteria for man-machine systems are introduced and discussed within the context of a control room interface design.

COMPUTER-BASED PROCEDURAL SUPPORT

A transformation from conventional paper-based procedures to a computer-based implementation with VDU's opens up a vast spectrum of possibilities. The most obvious are connected with the facilities which become available for on-line preparation, editing, storing or retrieval of procedural material. A second advantage is connected with the possibilities for administrative

control which can be incorporated - for example, in recording the usage of procedures. The third important feature is the direct availability of the process data base which can be accessed during the actual execution of procedures, checklists, etc.

Other possibilities for procedural support can best be discussed by means of an example and we have selected the startup of a (PWR) reactor in order to illustrate:

- how long sequences can be structured.
- how a good overview of status can be maintained - even in the (usual) case of unexpected interruptions and holds along the way.
- how appropriate information can be made available.

The model procedure used as a basis for the following embodies approximately 50 major steps to move the system from cold shutdown to 5-10% power and takes about 48 hours. A useful representation for structuring this evolution - based on earlier work with time-line analyses by Pedersen (10) - is shown in Fig. 2 as a two-dimensional format in which the various sub-tasks or sub-procedures are arranged vertically with respect to time or order. Horizontally they can be located in different ways - for example, depending on the startup phase. In Fig. 2, they are distributed according to the sub-system to which they are most closely connected. Another related possibility is to distribute them by task category - i.e., monitoring of reactivity balance; monitoring of heatup, cooling, temperature, gradients, or rod maneuvering; etc. In either case, one obtains

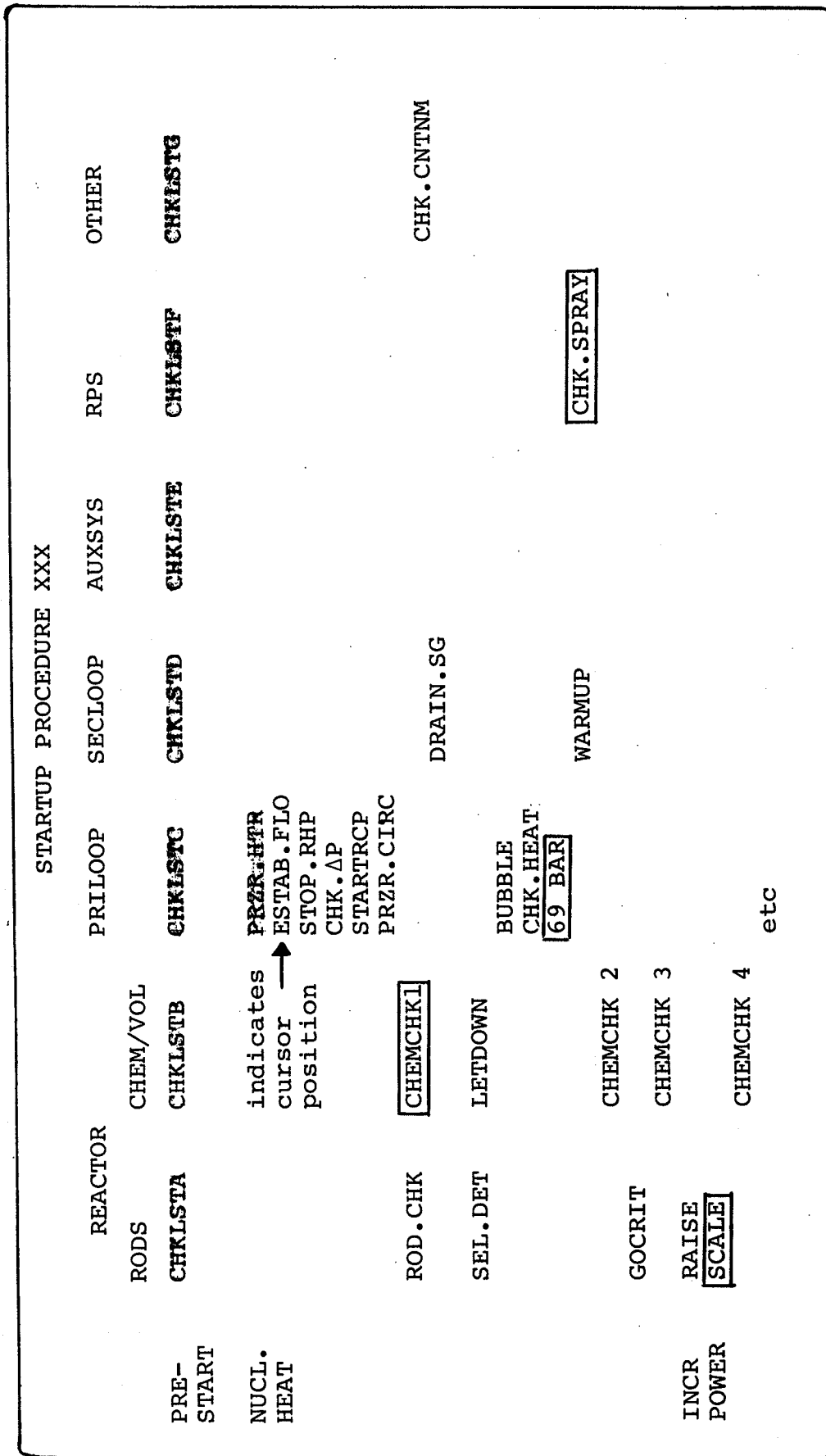
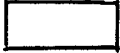


Fig. 2. SURVEY DISPLAY

a kind of high-level representation of the ordered set of sub-procedures (defined by short textual descriptors) required to take the system from one state to another under normal, prescribed circumstances.

The use of color displays makes it possible to code the text identifiers in order to emphasize and clarify status. Thus background colors could be used to indicate such things as sub-procedure complete, in process, on "hold", has problem. In addition, analyses of typical procedures indicate that sub-processes in the system often are plant-paced; i.e., the operator initiates a change via a sub-procedure which, after five minutes or three hours requires that another sub-procedure be started. These plant-paced sub-procedures can be coded, for example as shown on Fig. 2 with a  to serve as reminders to the operator.

The potential for a certain amount of flexibility is implicit in the two-dimensional layout which could be interpreted to indicate that sub-procedures along the same horizontal could be performed in any order. The computer could assist as time-keeper, status monitor and discrete constraint checker.

It is intended that this overall survey would be displayed on one VDU. Through some form for operator selection (trackerball, cursor...) of a particular sub-procedure, the appropriate body of text (or at least the first section of it) would appear on a second VDU as illustrated in Fig. 3. While no claims are made here for optimized ergonomic layout, any (sub)procedures should have the generic structure shown in Fig. 4.

VDU 2

PROCEDURE XXX - ENERGIZE PRESSURIZER HEATERS

PREREQUISITES: - N.G. SEE CHECKLIST C

(OR)

PREREQUISITES: OK

ACTIONS	LOCATION		FEEDBACK FROM
	PANEL	NO.	
SET A-H SELECTOR ON: H	X	X	VDU DISPLAY ABC
ENERGIZE HEATERS	X	X	VDU DISPLAY CDE
	X	X	
	X	X	
PLOT PRESSURIZER TEMPERATURE	X	X	PLOTTER ZZ

PRECAUTIONS: WHEN RC TEMP REACHES 70°C,
START RC PUMP (SEE PROCEDURE ZZZ)

REMINDERS

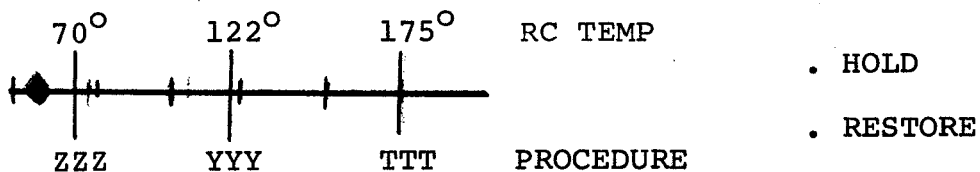


Fig. 3. PROCEDURE DETAILS

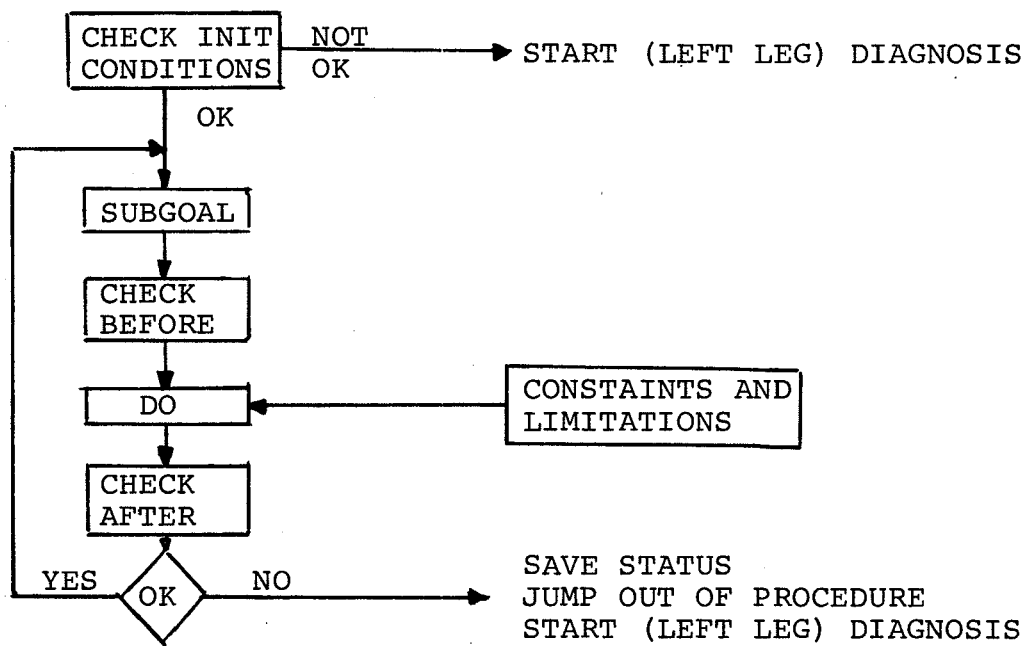


Fig. 4.

In essence, this structure requires that every procedure start with an interface specification with regard to the plant, the operational environment, personnel, etc. in the form of conditions, states, etc. which must be present in order for the procedure to be carried out without undesirable and/or unforeseen side effects, latent influences and the like. This implies that the first statement says something to the effect that "this procedure is intended to under the conditions that". This leads to suitable checklists which operator and computer together will "fill in" with the help of suitable displays. Only then can the body of the procedure be carried out. If the conditions are not satisfied, then a diagnostic situation exists. These "checkpoints" represent good opportunities for clarifying responsibility. For example if the actual conditions match those specified by the writer of the pro-

cedure, then he takes responsibility for the results of its subsequent (correct) execution. If not, then the operator has a clear mandate to identify and correct the deviation.

The actions carried out in the body of the (sub)procedure should consistently give rise to some form for feedback about the results of the operation with respect to the specified criteria. A third VDU is for extra support - to check conditions, monitor operations, give feedback via suitable displays of the plant. Reference to these displays can be made on VDU No. 2 as shown in connection with the particular procedural step(s). See (11) on an earlier proposal for a paper-based procedure.

As mentioned earlier, "reminders" can be handled in various ways. The example in Fig. 3 indicates that the reactor coolant temperature will start to rise now that startup is underway and that, according to the plot at the bottom of the display, there exist three tasks to be performed in connection with three levels of temperature. Blink or other attention-getting means could be incorporated for alerting the operator when these temperatures are approached.

Thus the three VDU's function as an integrated set of displays (see Fig. 5) indicating, in the example chosen, the overall status of start-up, details on the current (sub)procedure together with feedback information on the results of checks, maneuvers, etc. In the case of inappropriate or incorrect responses to any of the steps, the procedural system could be placed in HOLD while the required diagnosis was carried out using the same set of VDU's with (other) suitable displays to assist in identifying the problem and determining the proper

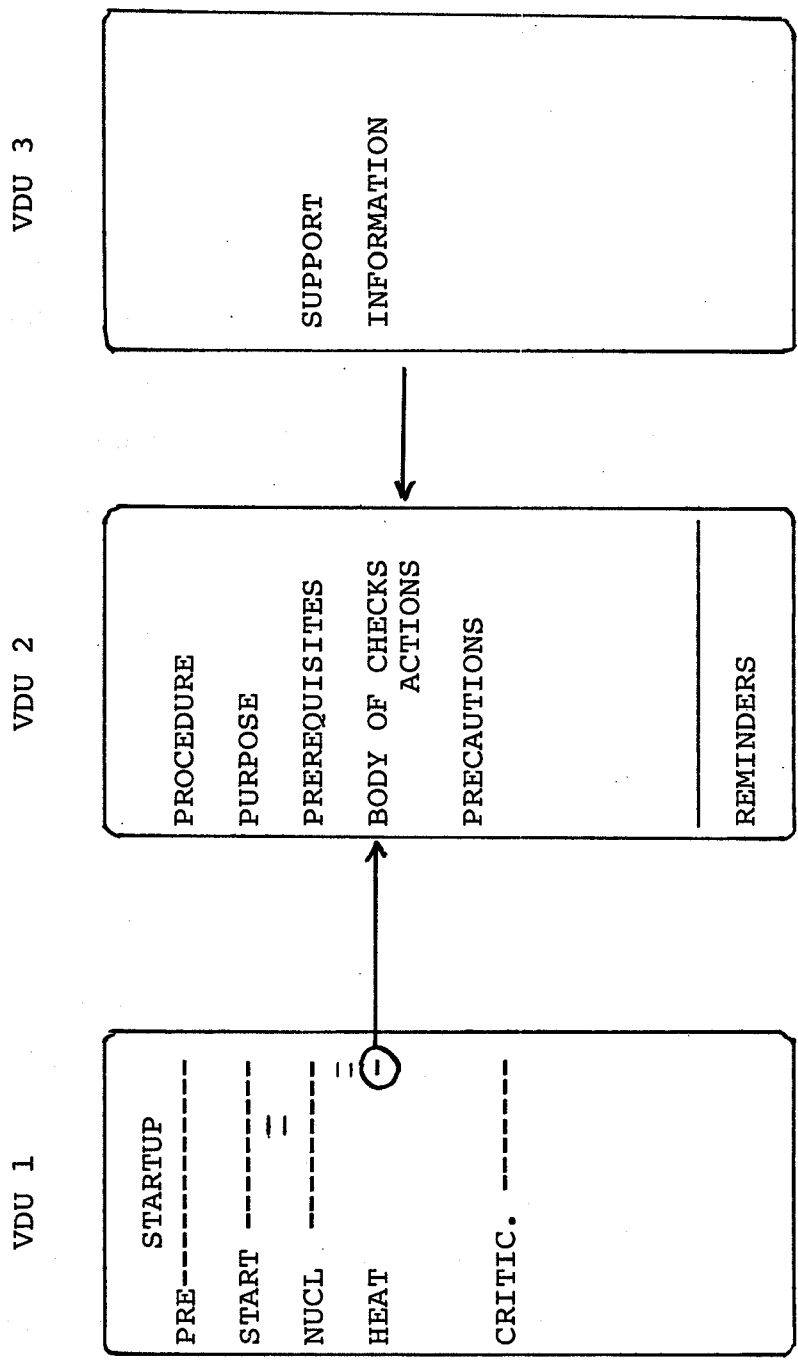


Fig. 5.

corrections. These, in turn, would be linked to appropriate procedures for carrying out the corrections and these would be retrieved, supported and executed in the same way as the original sequence. Upon their completion, the HOLD could be released and the original procedure resumed.

Implicit in all of this is an adherence in the design to a suitable set of criteria relating operator interactions with the plant to requirements for safety and reliability. Among other things, these include the concepts of error tolerance and reversibility so that, in the case of errors in critical sequences, recovery can be assured. As a last resort, the incorporation of suitable interlocks and barriers will be required.

CONCLUDING REMARKS

Since a procedure is a kind of script to an author-created situation, it would seem natural to require that its "performance" be checked out by means of a dress rehearsal in the control room. Even a "talk-through" or "hands-off" approach should be able to pinpoint obvious discrepancies between procedure and equipment, omissions, ambiguities, excessive demands, lack of feedback, etc.

ACKNOWLEDGEMENTS

I thank Jens Rasmussen for his suggestions on improving this paper. For a complementary paper on the systematic design of procedures, see (13).

REFERENCES

- (1) Office of Federal Register - 10 CFR 0.735-1 Part 50 App B pg 29.
- (2) AHERN, P.: Written procedures - blueprints for safe operation - Trans ANS Aug. 1975.
- (3) THORNBURG, H.: Procedures - the necessary instrument for management control - Trans ANS Aug. 1975.
- (4) RASMUSSEN, Jens: The Human Data Processor as a System Component, Bits and Pieces of a Model. Risø-M-1722, 1974, 51 pp.
- (5) RASMUSSEN, Jens: Outlines of a Hybrid Model of the Process Plant Operator. (I: Monitoring Behaviour and Supervisory Control. Edited by T.B. Sheridan and G. Johannsen. (Plenum Press, New York, 1976) 371-384.
- (6) RASMUSSEN, Jens: Reflections on the Concept of Operator Workload. In: Moray, N. (Ed.): Mental Workload (Plenum

Publishing Corporation, 1979). Proceedings from NATO Workshop on Mental Workload Theory. Athens, 1977.

- (7) RASMUSSEN, Jens: Man as a System Component. To be published in "Man-Computer Research" H. Smith and T. Green (Eds.), Academic Press.
- (8) RASMUSSEN, Jens: What Can be Learned From Human Error Reports. In: Duncan, K., Gruneberg, M., and Wallis, D., (Eds.): Changes in Working Life. John Wiley & Sons. (Proceedings of the NATO International Conference on Changes in the Nature and Quality of Working Life, Thessaloniki, Greece, 1979).
- (9) GOODSTEIN, L.P. and Jens RASMUSSEN, - The Use of Man-Machine System Design Criteria. - Risø-M-2196 - (to be published).
- (10) PEDERSEN, O.P.: An Analysis of Operators' Information and Display Requirements during Power Plant Boiler Start - Risø-M-1738 - Dec. 1974.
- (11) DOWLING, E.P. and J.A. CASTANES: - Efficient plant operation through condensed information display - Proceedings of Specialists' Meeting on Control Room Design 1975 IEEE Pub 75CH11065-2 (1975).
- (12) BIBBY, K.S., F. MARGULIES, J.E. RIJNSDOFF and R.M.J. WITHERS, (1975). Man's Role in Control Systems. IFAC Congress Boston, 1975.
- (13) LIND, M.: The Use of Flow Models in Design of Plant Operating Procedures - IAEA IWG/NPPCl Specialists' Meeting on Procedures and Systems for Assisting an Operator during Normal and Anomalous Nuclear Power Plant Operator Situations - Garching 1979.

J. Decuyper, S. Reynaud, A. Hoepner, Rolland

A GOOD OPERATOR-PROCESS RELATION RESEARCH IN CREYS-MALVILLE
PROJECT

"A GOOD OPERATOR-PROCESS RELATION RESEARCH
IN CREYS-MALVILLE PROJECT"

To be presented at the

"International Atomic Energy Agency specialists meeting
on Procedures and Systems for assisting an operator
during normal and anomalous nuclear power plant operation
situations

5 - 7 December 1979, Munich (R.F.A.)"

by Mr DECUYPER, REYNAUD, HOEPNER (NERSA), ROLLAND (EDF-CRPT)

1. INTRODUCTION

This paper deals with the approaches undertaken by NERSA in order to get an optimal man-machine interface design, both in normal and in abnormal operation conditions.

The main features followed are :

- adoption of a control system allowing the easiest process control and operating (this aspect has been presented recently in a paper at a previous meeting, see ref. 1, and will therefore not be exposed),
- design of the control room according to the operational simulation data and the control and instrumentation devices which are to be installed,
- research of optimal operating procedures, mainly during load variations and during abnormal operating conditions,
- operator's training.

Before discussing about a few examples of the items seen below, let us remember the main features of the plant.

2. SUMMARIZED DESCRIPTION OF THE PLANT

2.1. Main characteristics

The plant of Creys-Malville has already been described in previous papers (see ref. 1 and 2). This paper will therefore be restricted to present the main features which have influenced the design conception of the control room and, more generally, instrumentation and control :

- the power evacuation during normal operation is provided by two turbine groups, working in parallel (the symmetrical order is 2 for the conventional part of the plant),
- the power removal from primary circuit is assured by four secondary sodium loops (the symmetrical order is 4).

...

- the connexion of the steam-generators to the feedwater and live steam pipes establishes a pressure equalization both at the inlet and at the outlet,
- the sodium masses bring enormous thermal inertias (approximately 5600 MJ/°C for the primary circuit and 400 MJ/°C for each secondary loop),
- the physical separation of electric supplies in the control room.

2.2. Main options of operating

Here we shall also discuss only the options that have an incidence on the design of the control room :

- the control rods should be controlled manually by the operator,
- the four primary pumps should be at the same speed ; they should also have a group speed set point ; the speed should always be set manually.

These two options are safety-related.

- normal (steady load) operation can be accomplished by only one operator,
- an objective for the plant is to be able to assure a 10 % range of load follow.

3. CONTROL ROOM DESIGN

3.1. General design

Fig. 1 shows the lay-out of the control room of Creys-Malville plant.

The first design basis criterion is to have a master control board (BP : bloc principal) and a secondary control board (BS : bloc secondaire). The two boards are face to face located : such a lay-out complies with the option of operating with only one operator ; it also minimizes his movements and allows him a complete view of the boards, wherever he might be in relation to them.

...

The incorporation of a control device on the BP or the BS is made merely with a functional concept :

- instrumentation required for normal operating (steady state and daily load variations) is located at BP,
- instrumentation required for normal operating (start-up and shut-down procedures) and abnormal operating is located at BS.

Both on BP and BS, the panels begin with reactor instrumentation and progress through the heat transport systems to the turbine and electrical generator system (see fig. 1 again).

3.2. Detailed design

The detailed lay-out of the instrumentation on the control boards is issued from :

- the elementary systems related functional studies (not yet completed),
- the plant simulation data : they are related to steady state, load variations, start-up and shut-down procedures, and accidental transients.

We should like to expose to you a few examples of the considerations issued from this second point.

The plant simulation data which influenced the design of the control room are :

- the real time hybrid simulation data, accomplished with the plant simulator (see ref. 2),
- the accidental transient numerical simulation (see ref. 3).

3.2.1. The plant simulator mainly consists of two components :

- the hybrid computer,
- the on-line control board.

The advantage of disposing of an on-line control board is that the arrangement of instrumentation may easily be modified and adapted to conclusions drawn from the simulation. The control board being of modular conception, a quick modification is made possible.

We can say today that such a simulation has allowed us to define more precisely the master control board of the control room. It has also indicated some principal information and its optimal location needed from the operator which we did not expect at the beginning of the project :

- A continuous pen recorder for the live steam outlet generator temperature (TsV) located closely near the modules of the control rods. This recorded measurement is required because the operator must keep the steam temperature as constant as possible while handling the control rods and such an operation is somewhat difficult owing to the high thermal inertias.
- A digital indicator for the optimal sodium core outlet temperature according to the load : it lets the operator know the speed with which the control rods must be manipulated. It is mainly important during load variations or consequently an automatic load runback.
- A digital indicator for the optimal primary sodium pump speed (as seen above, it is always manually controlled by the operator). The mode of operating in steady state of the Creys-Malville plant establishes a law between primary and secondary pump speed as a function of the load, in order to operate with a core inlet temperature approximately constant. This information is also very important in case of automatic load runback.

The real-time simulation also lends support to the utilization of the following devices : (whose installation is being studied at present)

- an indication giving the position of the three control rods regulating the core sodium outlet temperature,
- a display (by monitor) of the position of each control rod (this information is already given to the operator by digital indicators).

...

- 3.2.2. The accidental transient simulation data let us draw the conclusion that it is not necessary, for a sodium cooled fast reactor plant, to provide for an area of the control room reserved for safeguard system and equipment.

This is a consequence of the high thermal inertia of sodium which affords the operator sufficient time before beginning protective procedures.

Furthermore, we shall note that the systems allowing to maintain the unit in safe condition during hot shutdown after an accidental condition and especially the decay heat removal systems, are in service during normal operation conditions (like the primary tank well cooling circuit, always in service, or the Na-Air exchanger on secondary circuits in service during every cold shutdown).

These considerations lead us to conceive of a very simple emergency control board outside the control room ; in case the latter is not available, on it there are no actuator switched devices, but only some indicators or alarm displays. The manual operation and protective actions on the actuators are carried out from the switchgear room located in the two electrical equipment buildings.

The functional analysis of the safety related systems has further corroborated this choice.

3.3. Operator-process interface design consideration

The interface between the operator and the plant in the control room will be designed according to :

- the computer generated visual displays,
- the traditional control equipment.

3.3.1. Computers

Two computers have a colour display monitors as interface with the operator :

- The "TCI" computer (Complementary Data Acquisition System : Traitement Complémentaire de l'Information) : this provides a major portion of the information needed by the operator during normal and accidental operation :

- . the status of each system of the unit,
 - . the alarm (not safety-related) display,
 - . some synoptical diagrams of the main systems, with associated analogical and digital information displayed. A blowup of the diagram is also possible.
- The "DDDC" computer (Detection and Diagnosis of Core Malfunctions : "Détection et Diagnostic des Défauts du Coeur) : it gives to the operator the core status (thermal and nuclear flux maps, control rod diagram).

3.3.2. Alarm Display Devices

As an example of the research of a good interface between the operator and the plant processes, let us discuss the approach we have had about the alarm display criteria.

The alarm display devices in the control room are :

- the CRT, located both in the BP and in BS panels, associated with the computers,
- the conventional alarm annunciator windows,
- the lamps located on the actuator switch modules.

The alarms or information are classed in four annunciation categories, related both to the delay required and the kind of protective action. (Cf. Table I).

The information to the operator must comply with :

- simplicity and ease of understanding, in order to increase the probability of the operator's taking the correct action,
- reliability, related to the importance of the information.

So, the following measures are provided :

- Alarms shall be presented only once to the operator, in order to avoid multiple acknowledgements ; this option affects also the category 1 alarms.

- Alarms shall be presented to the operator on the control panel where he must begin the protective action and where he disposes of all useful information to take correct action,
- Alarms shall be presented consistently with the real condition of the plant and if it has not been delivered in a previous display (e.g. low oil pressure must not be presented when the pump is not operating).

Table 1 presents the synthesis of the previous considerations.

3.3.3. Synoptical integrated panels

The arrangements of the switches on panels (horizontal part) are provided with a modular conception ; each module is 24 x 28 mm.

This conception allows for a functional grouping of both switch modules and indicators, in order to improve the operator's ability for protective action, both in delay and in efficacy.

The study for a good arrangement of the modules is carried out by means of a full scale wooden model of the control room ; the grouping of control devices may be easily conceived by the use of stickers or magnetized models of the devices.

The safety requirement of physical separation and the choice of a control hierarchy limited to elementary systems, suggest that in practice synoptics be related to one elementary system.

4. RESEARCH OF OPERATING PROCEDURES

The research of operating procedures has been accomplished, as previously mentioned, with the real time plant simulator, in order to be able to take into account the operator's behaviour and his reactions.

A special effort has been made about the load variation procedures, because keeping the steam temperature constant at 490° C is the main difficulty in normal operating.

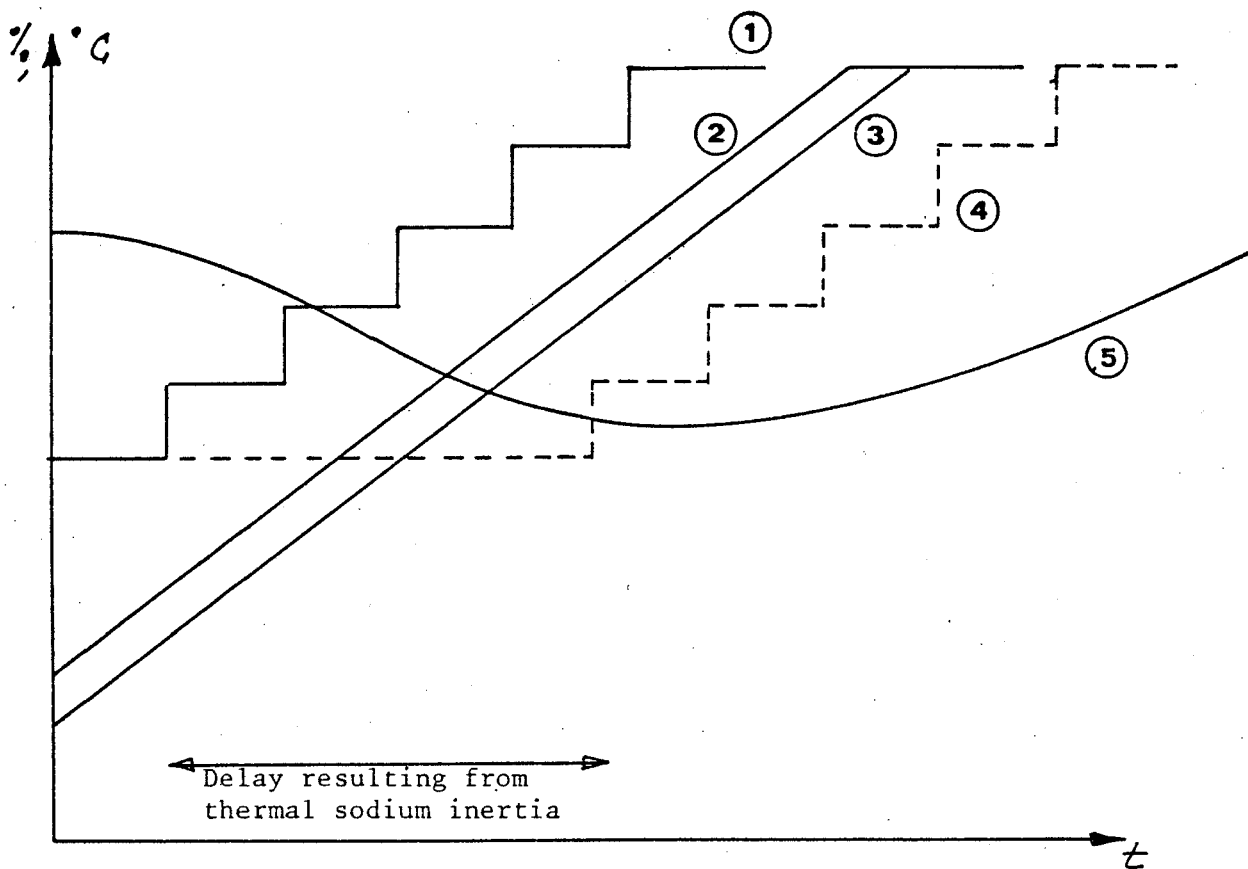
In fact, during this transient, the operator has to handle (see page 2).

- the 21 control rods, individually,
- the primary pumps, group controlled,
- the secondary pumps, group controlled (if they are not automatically controlled).

Furthermore, a few considerations to be taken in account are :

- As a consequence of sodium's thermal inertia, the effect of the control rod initiated power variation is "seen" in the steam generator only after a relatively long delay.
- The secondary pumps (automatically or manually controlled) and the feed-water pumps (automatically controlled), vary the sodium and water flows according to the load set point and therefore they cannot take into account the inertia of the sodium.

The following schematic diagram shows the essential of these considerations in the case of a load increasing (qualitative scales) :



- ① Increasing of thermal power (control rod initiated)
- ② Sodium flow in steam generator
- ③ Feedwater to steam generator
- ④ Increasing of thermal power in the steam generator
- ⑤ Live steam temperature

The higher the load change rate, the greater the problem (hence the fall in steam temperature). There are not many difficulties at a rate of 1,5 %/mn, but at 5 %/mn they are important.

As a result of the simulation, quite simple operating criteria could be given, assuring good plant characteristics :

- individual control rod action of only about 1 cm,
- power increasing anticipation in relation to the load set point,
- limited primary flows step ($\approx 2,5$ %).

The simulation has also shown the core burn-up effects on the operator's possibilities and, so, on operating instructions. In fact the efficiency of control rods at the end of the core's life is a lot less than at the beginning (a factor 3 is expected) and so the operator has to control them much more often.

5. OPERATOR TRAINING

The operator training program will start in 1980 ; this training program is one of a three phases complex including :

- 1st phase : selecting of the operators which is based on minimal knowledge criteria ; the desired characteristics for this kind of candidate are : being a technician with several years experience in a nuclear plant operating shift or possibly in a thermal plant.
- 2nd phase : operator training, comprises a basic program which is necessary for everybody and a variable program depending on the initial knowledge level of each of the operator under training as well as improving for particular subjects.
- 3rd phase : qualification which is the normal issue of the initial selection and training program, the decision is based on continuous assessment during all the training sessions.

These three phases are shown on the table number 2.

In the following, we give some comments on two essential parts of the basic training program :

...

- Training on the plant simulator : initial program includes two sessions :

- . the first session treats the normal operating conditions (start-up, shut-down, operating with only one turbo-alternator...)
- . the second session treats the incidental or accidental situations (acceleration or run-down of primary or secondary sodium pumps, trip of main feedwater pump...)

The preparation of these sessions has to allow for the inexact reproduction by the simulator of the real operator-process interface.

- On-site training for a detailed knowledge of the plant :

This training comprises the detailed study of components, circuits and automatic systems as well as all the written instructions and procedures. This on-site training represents the longest part of the basic training program ; it is essentially directed by the team of engineers operating team of the plant. The possible creation of a computer assisted learning system is now being considered for initial and in service operating training.

REFERENCES

- Ref. 1 - The Control System adopted for Super-Phenix reasons for choice and evaluation of performance by MM. DECUYPER/SKULL/HERY/HENNEBICQ/CKET - I.A.E.A. Meeting on "Nuclear Power Plant Control and Instrumentation - WIEN, 1978.
- Ref. 2 - "Incidence du suivi réseau sur le coeur et les composants des circuits sodium de Super-Phenix" by MM. DECUYPER/REYNAUD/QUINTON/CKET - I.A.E.A. Meeting on Nuclear Power Plant Control problems Associated with load following an network transients, CADARACHE, 1977

TABLE I
Assignment of Annunciation Category

Annunciation Category	Definition	Type	Location of Required Protective Action	Location		
				Hardwired window	CRT Display	Type writer
1 (red)	Annunciation requiring an immediate reaction of the operator	single	BP BS	BP BS		
		group	BP BS	BP (detail) BS (detail)		
2 (yellow) or 3 (white)	Annunciation allowing a major delay for the operator's reaction Annunciation only informing the operator (no action required)	single	BP BS	BP BS	BP BS	
		group	BP BS	BP (detail) BS (detail)		
4 (green)	Annunciation of faults initiating automatic reactor shutdown or power runback (which are to be supervised by the operator)	single group	- -	BP BP	BP (detail)	

BP : Master control board

BS : Secondary control board

OPERATOR TRAINING PROGRAM

Table 2

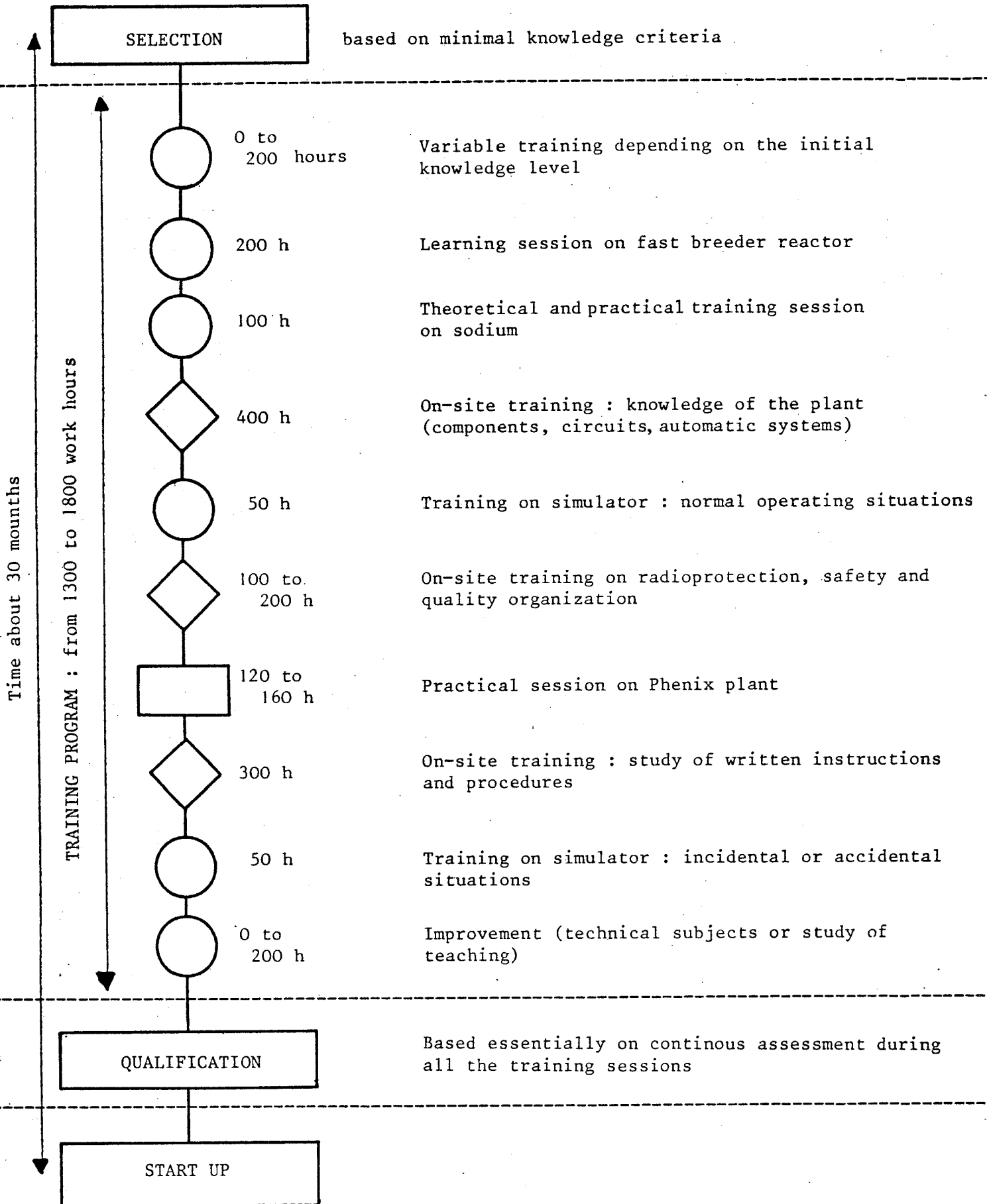
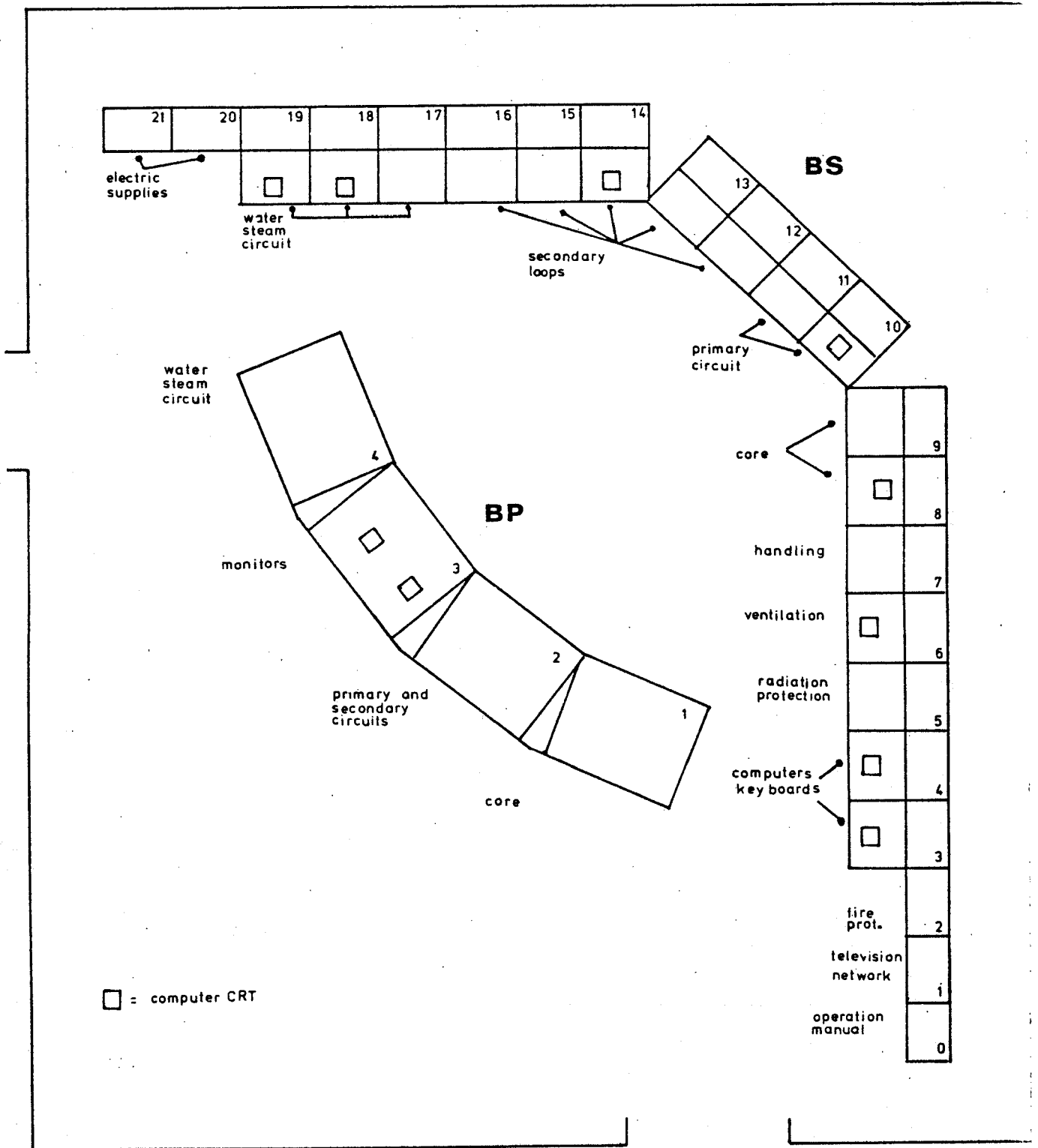


FIG. 1 CONTROL ROOM GENERAL LAY-OUT



E.S. Patterson

OUTLOOK FOR THE USE OF COMPUTERS FOR PROTECTION SYSTEMS AND
AUTOMATIC CONTROL IN NUCLEAR POWER PLANTS

OUTLOOK FOR THE USE OF COMPUTERS
FOR PROTECTION SYSTEMS AND AUTOMATIC
CONTROL IN NUCLEAR POWER PLANTS

by

E. S. PATTERSON
BABCOCK & WILCOX, CO.
LYNCHBURG, VA., USA

Presented to the IAEA/NPPCI Specialists Meeting,
Session 6, December 7, 1979, Munich

SUMMARY

The technological power of computers has rapidly increased since 1976; however, the issues of 1976 centering upon the detection of software errors are still with us. Virtually no progress has been made in proving that software errors absolutely do or do not exist. The rapidly rising demand for the reduction in the probability for human error cannot be met without extensive use of computers for control and safety related functions. The software error issues of 1976 must be resolved if we are to significantly reduce human error..

COMMENTS

The state of computer technology has rapidly moved forward since the May 1976 IAEA/NPPCI Specialists' Meeting on the Application of Computers in Protection and Control with an increase in the power of computers and computer-type devices. The technology is continuing to be very attractive to designers although there has been a broader recognition that the cost of program development is a major cost consideration that has made a number of proposed applications unattractive.

New applications of computers to safety and control problems have been slowed or virtually halted since 1976 for the following reasons:

- 1) There have been no pressing safety issues that computer technology would solve better than other more cost effective technique.
- 2) Licensing computer systems for safety or safety related functions has been a most difficult task.
- 3) There has been no visible demand in the nuclear plant market for computerized safety related functions.

The work on computer applications to safety related functions has continued in a few research organizations principally in areas that were under development prior to 1976. But, in spite of the attractiveness of some of these programs, there has been little or no interest shown in implementing these developments in operating plants.

The future outlook for computerized safety and control functions in the USA may be determined by the requirements coming out of the TMI-2 incident. The general belief is that the emerging demands for human factors accountability, the human engineering of control rooms and the use of complex systems to direct the operator and control the plant will continue into the future.

The belief also exists that these demands, all directed toward eliminating human error, cannot be satisfied without the extensive utilization of computer technology. The functions that must be computerized will, in many cases, be considered safety related which will raise the old issues of 1976, computer and software reliability.

The investigations into techniques for verifying that absolutely no errors exist in a software program have not been encouraging. I understand that Halden has recently concluded an investigation into software error detection with disappointing results. The Electric Power Research Institute also has a validation study underway but it is too early to draw any conclusions about their work. Worldwide, little or no progress has been made in the development of software error detection techniques or methods since 1976.

Structured programming, the organization and control of all the programming activities during the software development process, was proposed by Halden and others by 1976. This approach, assuring a low probability of software errors, is now widely accepted as the best way of assuring reliable software. It is my opinion that if we are to meet the near term and future demands for reducing human error we must increase our dependence and confidence in computer technology and this requires that we quickly arrive at a resolution of the software error issue.

I suggest that the regulatory authorities may have fallen into the trap of looking too much at the possible effects of software errors instead of the probable existence of software errors and their probable effects.

I suggest that the entire matter should be reviewed specifically for human error reduction applications. In such a review, the probability of human error and its consequences should be weighed against the probability of computer errors and their consequences in the proposed application. If the two risks are judged in the proper context it is entirely possible that we will be released to move rapidly ahead with safety related computer applications directed toward the reduction of human error.

/dww

