



Gesellschaft für
Reaktorsicherheit (GRS) mbH

Proceedings
of the OECD/BMU-Workshop on
Special Issues of Level 1 PSA

Held in Cologne, F.R.G.
May 27 - 29, 1991



Gesellschaft für
Reaktorsicherheit (GRS) mbH

Proceedings
of the OECD/BMU-Workshop on
Special Issues of Level 1 PSA

Held in Cologne, F.R.G.
May 27 - 29, 1991

Compiled by U. Hauptmanns

GRS-86 (July 1991)
ISBN 3 - 923875 - 36 - 3

Contents

	Page
List of Participants	1
INTRODUCTORY SESSION	11
Opening Address	12
W. Ullrich, FRG	
The Activities of the OECD/NEA in Risk Assessment - An Overview -	15
P.M. Hertrich, FRG	
Objectives and Status of Work of PWG 5/Task 9, "State of the Art of Level 1 PSA Methodology"	41
R. Virolainen, Finland	
State-of-the-Art of Level 1 PSA	50
W.F. Werner, FRG	
ANALYSIS OF DEPENDENCIES	92
Issue Paper on Dependent Failures	93
U. Hauptmanns, FRG	
Why is the Markov Method not used as a Standard Technique in PSA?	97
E. Silvestri, Italy	
The Conditional Applicability of the B-Factor Method for Structural Redundancies	105
K. Lützow and L. Fuhrmann, FRG	
Evaluation Criteria of Safety System Unavailabilities for Nuclear Power Plants	123
H. Murakami, S. Oda, T. Sato, M. Matsumoto and S. Miura, Japan	

Contents

	Page
PSA Convoy-Influence and Modelling of Common Cause Failures A. Feigel and J. Wenzel, FRG	130
TIME DEPENDENT PHENOMENA, UNCERTAINTIES	142
Uncertainty Analysis - An Issue Paper U. Pulkinnen, Finland	143
Uncertainty Study in Probabilistic Risk Assessment for TVO I/II Nuclear Power Plant J. Holmsberg and R. Himanen, Finland	148
Graphical Tools for Detection and Modelling of Time Dependent Ageing Behaviour in Com- ponent Data H. Pamme, FRG	161
Draft Report for Comments: NKS/SIK - 1 Project Report: Time Dependencies in LPSA Models G. Johanson, Sweden	184
HUMAN ERROR	201
Issue Paper J. Mertens, FRG	202
A Slim - Based Approach in Analyzing Operator Cognitive Actions L. Reiman	209
An Approach to the Analysis of Operating Crew Responses Using Simulator Exercises for use in PSAs	223

III

Contents

	Page
G.W. Parry, A. Singh, A. Spurgin, P. Moieni and A. Beare, USA	
An Assessment of the Risk Significance of Human Errors in Selected PSAs and Operating Events	242
R.L. Palla, Jr., A. El-Bassioni and J. Higgins, USA	
Quantification of Human Errors in Level-1 PSA Studies in NUPEC/JINS	260
M. Hirano, M. Hirose, M. Sugawara and T. Hashiba, Japan	
Improved Main Control Board with a Better Man-Machine Interface	279
T. Oshibe, Japan	
EXTERNAL EVENTS	292
Issue paper on "External Events"	
C. Zaffiro	
External Events Assessment for an LMFBR Plant	304
K. Aizawa, R. Nakai and A. Yamaguchi, Japan	
Possibilities and Limitations of Probabilistic Fire Safety Analyses Illustrated by Analyses in the German Risk Study	318
H. Liemersdorf, FRG	
Seismic Assessment for N.P.P. According to Italian Practice	332
S. D'Offizi, L. Magri and F. Muzzi, Italy	

IV

Contents

	Page
Experience Gained in Italy on the Probabilistic Analysis of Accidents Initiated by Seismic Events A. Pugliese, A. Valeri and C. Zaffiro, Italy	340
SPECIAL TOPICS	351
Experiences with Data Collection, Retrieval and Interpretation for PSA Purposes H. Pamme and L. Seyffarth, FRG	352
Frequencies of Leaks and Breaks in Safety Related Piping of PWR-Plants as Initiating Events for LOCAs S. Beliczey, FRG	364
Evaluation of Low Power and Shutdown Events in German PWRs M. Simon, FRG	381
Living PSS Used to Support the Development of A New Generation of BWR V. Cavicchia, E. Traini, L. Matteocci and A. Valeri, Italy	391
SUMMARY OF DISCUSSION	398

**OECD / BMU Workshop on
"Special Issues of Level 1 PSA"**

List of Participants

ABE

Mr.
Kiyoharo Abe
Head of Risk Analysis Lab.
Japan Atomic Energy Research
Institute - JAERI
Tokai Research Establishment
Tokai-Mura, Naka-gun,
Ibaraki-ken 319-11, Japan

AIZAWA

Dr. Kiyoto Aizawa
Power Reactor and Nuclear Fuel
Development Corporation
Reactor Engineering Development
Corporation - RTDD
San-Kai-Doh Bldg.
9-13, 1-Chome, Akasaka
MINATO-KU, TOKYO-107 - Japan

BALFANZ

Herrn
Dipl.-Ing. H.-P. Balfanz
TUEV Norddeutschland e.V.
Grosse Bahnstr. 31
2000 Hamburg 54

BELICZEY

Herrn
Dipl.-Ing. Stefan Beliczey
Gesellschaft fuer Reaktorsicherheit
(GRS) mbH
Schwertnergasse 1
5000 Koeln 1

BERG

Herrn
Dr. Heinz-Peter Berg
Bundesamt fuer Strahlenschutz
Postfach 10 01 49
3320 Salzgitter

BLAESIG

Herrn
Dr. Helmut Blaesig
RWE Energie AG
HV - Abt. KK-BS
Kruppstr. 5
4300 Essen 1

BREILING

Herrn
Guenter Breiling
ABB Reaktor GmbH
Dudenstrasse 44
Postfach 10 05 63
6800 Mannheim 1

BURCHHARDT

Herrn
Dipl.-Ing. Walter Burchhardt
Energieversorgung Schwaben AG
Umspannanlage Scheibenhardt
Postfach 37 20
7500 Karlsruhe 1

CAEYMAEX

Mister Caeymaex
Nuclear Process Department
TRACTEBEL
Boulevard du Regent, 8/M7
B - 1000 Bruxelles

CALVO

Mr.
Jose I. Calvo
Consejo de Seguridad
Nuclear (CSN)
c/Justo Dorado, No. 11
E-28040 Madrid
SPAIN

CAMPBELL

Mr.
J.F. Campbell
H.M. Nuclear Installations
Inspectorate
Room 601, St. Peter's House
Bootle Merseyside L 20 3LZ
United Kingdom

CHANG

Mr.
Hong L. Chang
Nuclear Safety Division
Organisation for Economic
Co-Operation and Development
38, Boulevard Suchet
F-75016 Paris

DE GELDER

Herrn
Pieter de Gelder
Section Head
AIB - Vincotte Nuclear
Avenue du Roi 157
B-1060 Bruxelles

DEUTSCHMANN

Herrn
Herbert Deutschmann
Bundesamt fuer Energiewirtschaft
Hauptabteilung fuer die Sicherheit
der Kernanlagen (HSK)
CH-5303 Wuerenlingen

DINSMORE

Herrn
Stephen C. Dinsmore
Technischer Sicherheitsberater
Hermann-Steinhaeuser-Str. 18
6050 Offenbach

DOODT

Herrn Doodt
Gemeinschaftskernkraftwerk
Neckar GmbH
Postfach
7129 Neckarwestheim

EL-BASSIONI

Mr.
Adel El-Bassioni
Section Chief
U. S. Nuclear Regulatory Commission
Washington, D.C. 20555
USA

FABIAN

Herrn
Dr.-Ing. Hermann Fabian
Siemens AG
Unternehmensbereich KWU
U7213
Postfach 32 20
8520 Erlangen

FLODIN

B. Yngve Flodin
Swedish State Power Board
Nuclear Power / PSA
Jaemtflandsgatan 99
S-16287 Vaellingby
Sweden

GADOLA

Herrn
Angelo Gadola
Centro Progettazione e Construzione
per gli Impianti Nucleari
Viale Regina Margherita 137
I-00100 Roma

GIBSON

Herrn
Ian Kenneth Gibson
UKAEA Safety and
Reliability Directorate
Wigshaw Lane, Culcheth
Warrington
Cheshire WA3 4NE
United Kingdom

HAGSTOTZ

Herrn
Dipl.-Ing. Gerhard Hagstotz
Hochtemperatur-Reaktorbau GmbH
Dudenstr. 44
6800 Mannheim 1

HASHIBA

Mr. Takashi Hashiba
Senior Engineer
Nuclear Power Engineering Test Ctr.
Japan Institute of Nuclear Safety
Fujita Kankou Toranomon Bldg 7F
3-17-1, Toranomon
Minato-Ku, Tokyo 105
JAPAN

HAUPTMANN

Herrn
Dr. Ulrich Hauptmanns
Gesellschaft fuer Reaktorsicherheit
(GRS) mbH
Schwertnergasse 1
5000 Koeln 1

HENNINGS

Herrn
Dipl.-Ing. Wilfried Hennings
Forschungszentrum Juelich GmbH
Institut fuer Nukleare
Sicherheitsforschung
Postfach 19 13
5170 Juelich 1

HERTTRICH

Herrn Regierungsdirektor
Dr. Michael Herttrich
Bundesministerium fuer Umwelt,
Naturschutz und Reaktorsicherheit
RS I 2 (G)
Husarenstrasse 30
5300 Bonn 1

HIRANO

Mr. Mitsumasa Hirano
Head, Reactor Design Analysis Div.
Nuclear Power Engineering Test Ctr.
Japan Institute of Nuclear Safety
Fujita Kankou Toranomom Bldg 7F
3-17-1, Toranomom
Minato-Ku, Tokyo 105
JAPAN

HIROSE

Mr. Masao Hirose
Principle Engineer
Nuclear Power Engineering Test Ctr.
Japan Institute of Nuclear Safety
Fujita Kankou Toranomom Bldg 7F
3-17-1, Toranomom
Minato-Ku, Tokyo 105
JAPAN

HOEMKE

Herrn
Paul Hoemke
Gesellschaft fuer Reaktorsicherheit
(GRS) mbH
Schwertnergasse 1
5000 Koeln 1

HOLMBERG

Mr.
Jan Holmberg
Technical Research Centre of Finland
Laboratory of Electrical Engineering
and Automation Technology
Otakaari 7 B
SF-01250 Espoo

KALFSBEEK

Herrn
Henk Kalfsbeek
Commission of the
European Communities
D.G. XII/D/1 - ARTS LUX 2/52
Rue de la Loi 200
B-1049 B r u s s e l s

KOJIMA

Shigeo Kojima
Mitsubishi Atomic Power
Industries, Inc.
4-1 Shibakouen 2-Chome
Minato-ku, Tokyo 105
JAPAN

KUNITZ

Herrn
Dr. Harald Kunitz
Gesellschaft fuer Reaktorsicherheit
(GRS) mbH
Schwertnergasse 1
5000 Koeln 1

LIEMERSDORF

Herrn
Heinz Liemersdorf
Gesellschaft fuer Reaktorsicherheit
(GRS) mbH
Schwertnergasse 1
5000 Koeln 1

LIWAANG

Mr.
Bo Liwaang
Swedish Nuclear Power Inspectorate
(S K I)
Division for Reliability Analysis
Sehlstedtsgatan 11
Box 27106
S-102 52 Stockholm

LUETZOW

Herrn Professor
Dr.-Ing. Klaus Luetzow
Technische Hochschule Zittau
Theodor-Koerner-Allee 16
O-8800 Zittau

MAGRI

Herrn
L. Magri
ISMES
Via dei Crociferi 44
I-00187 Rom
Italien

MERTENS

Herrn
Dr. J. Mertens
Institut fuer Sicherheitsforschung
und Reaktortechnik ISR
Forschungszentrum Juelich GmbH
Postfach 19 13
5170 Juelich

MOESER

Herrn
Dipl.-Ing. Andreas Moeser
Bayernwerk AG
Postfach 20 03 40
Nymphenburger Str. 39
8000 Muenchen 2

MUELLER-ECKER

Herrn
Dieter Mueller-Ecker
Gesellschaft fuer Reaktorsicherheit
(GRS) mbH
Schwertnergasse 1
5000 Koeln 1

MURAKAMI

Mr. Hideaki Murakami
Manager Nucl. Power Plant Div.
Tokyo Electric Power Company
1-3 Uchisaiwai-cho, 1-Chome
Chiyoda-ku, Tokyo
Zip code 100
Japan

ODA

Mr.
Shingo Oda
Safety Engineering Section
Hitachi Engineering Co. Ltd.
2-1 Saiwaicho 3-chome
Hitachi-Shi
Ibaraki-Ken
317 Japan

OHLMEYER

Herrn
Dipl.-Ing. Hermann Ohlmeyer
Hamburgische
Electricitaets-Werke AG
Ueberseering 12
2000 Hamburg 60

OSHIBE

Mr.
Toshihiro Oshibe
Nuclear Power Engineering Section
The KANSAI Electric Power Co., Inc.
3 - 22, 3-chome, Nakanoshima,
Kita-ku, Osaka 530
JAPAN

PAMME

Herrn
Dipl.-Ing. Hartmut Pamme
RWE Energie AG
KK - BS
Kruppstr. 5
4300 Essen 1

PARRY

Mr.
Gareth Parry
Senior Executive Engineer
NUS Corporation
910 Clopper Road
Gaithersburg, Maryland 20878
U S A

PUGLIESE

Mr.
Dr. Antonio Pugliese
Direzione Sicurezza Nucleare e
Protezione Sanitaria (DISP)
E N E A
Via Vitaliano Brancati 48
I-00144 Roma

PULKKINEN

Mr.
Urho Pulkkinen
Technical Research Centre of Finland
Laboratory of Electrical Engineering
and Automation Technology
Otakaari 7 B
SF-01250 Espoo

REIMANN

Mr.
Lasse Reimann
Department of Nuclear Safety
Finnish Centre for Radiation
and Nuclear Safety
P. O. Box 268
SF-00101 Helsinki 10

RIEHN

Herrn
Dr. Peter Riehn
Hessisches Ministerium fuer Umwelt,
Energie und Bundesangelegenheiten
Mainzer Strasse 80
6200 Wiesbaden

ROEWKAMP

Frau
Dr. Marina Roewekamp
Gesellschaft fuer Reaktorsicherheit
(GRS) mbH
Schwertnergasse 1
5000 Koeln 1

SATO

Mr. Takashi Sato
TOSHIBA Co.
ISOGO Engineering Centre
8 Shinsugita - Cho
ISOGO-KU
J-Jokohama 235
Japan

SCHNEIDER

Herrn
Peter Schneider
Elektrowatt Ingenieur-
unternehmung GmbH
Zweigniederlassung Mannheim
Alois Senefelderstrasse 1-3
6800 Mannheim 1

SCHUBERT

Herrn
Dr. Bernd Schubert
Hamburgische Electricitaets-Werke AG
Postfach 60 09 60
Ueberseering 12
2000 Hamburg 60

SEYFFARTH

Herrn
Dipl.-Ing. Lothar Seyffarth
RWE Energie AG
Kruppstr. 5
4300 Essen 1

SILVESTRI

Herrn
Dr. Enrico Silvestri
Ansaldo S.p.A.
Corso Perrone 25
I-16161 Genova
Italy

SIMON

Herrn
Manfred Simon
Gesellschaft fuer Reaktorsicherheit
(GRS) mbH
Schwertnergasse 1
5000 Koeln 1

STUECK

Herrn
Dr. Reinhard Stueck
Gesellschaft fuer Reaktorsicherheit
(GRS) mbH
Schwertnergasse 1
5000 Koeln 1

TUERSCHMANN

Herrn
Michael Tuerschmann
Gesellschaft fuer Reaktorsicherheit
(GRS) mbH
Buero Berlin
Kurfuerstendamm 200
1000 Berlin 15

VALERI

Mr. A. Valeri
Direzione Centrale della Sicurezza
Nucleare e della Protezione
Sanitaria
Ente nazionale Energie Alternative
Viale Regina Margherita 125
I-00198 - Rom

VERSTEEG

Mr. M.F. Versteeg
The Nuclear Safety Department
of the Ministry of
Social Affairs and Employment
Nuclear Safety Department
P.O. Box 90804
2509 LV Den Haag
The Netherlands

VIROLAINEN

Mr. Reino Virolainen
Finnish Centre for Radiation
and Nuclear Safety
P. O. Box 268
SF-00101 Helsinki 10

WEND

Herrn
Wend
TUEV Rheinland e.V
Postfach 10 17 50
500 Koeln 1

WENZEL

Herrn
J. Wenzel
Siemens Aktiengesellschaft
Unternehmensbereich KWU
E 422
Postfach 32 20
8520 Erlangen

WERNER

Herrn
Dr. Wolfgang Werner
Gesellschaft fuer Reaktorsicherheit
(GRS) mbH
Forschungsgelaende
8046 Garching

ZAFFIRO

Mr.
Carlo Zaffiro
Direzione Sicurezza Nucleare e
Protezione Sanitaria (DISP)
E N E A
Via Vitaliano Brancati 48
I-00144 Roma

ZIMMER

Herrn
Dr. Hans-Josef Zimmer
Badenwerk AG
Abteilung MK
Badenwerkstr. 2
Postfach 16 80
7500 Karlsruhe 1

ZIMMERMANN

Herrn
Markus Zimmermann
Gesellschaft fuer Reaktorsicherheit
(GRS) mbH
Forschungsgelaende
8046 Garching

Introductory Session

... ..

... ..

... ..

... ..

... ..

... ..

Opening Address

W. Ullrich

Gesellschaft für Reaktorsicherheit (GRS) mbH, Cologne, FRG

Ladies and Gentlemen,

it is a pleasure for me to welcome you on behalf of GRS to the OECD/BMU-Workshop on "Special Issues of Level-1 PSA".

With the increasing use of complex technologies there is a growing need to evaluate their safety. From a practical engineering point of view the engineer would say, we take care of some engineering precautions. The risk expert, however, would say, nevertheless, it should be necessary to quantify on a broad full scale of quantitative risk assessment. The methodology of probabilistic safety analysis allows its predictive valuation. Nuclear engineering has been in the forefront of the development and application of this method. For example in the Reactor Safety Study on US Nuclear Power Plants published in 1975 the risk of an entire technology was investigated systematically and quantified for the first time.

When the Rasmussen Study was published there was an intensive and to some extent also a controversial discussion on the use of probabilistic methods for quantifying safety aspects or respectively quantifying contributions to risk resulting from various technologies.

How to quantify risk, may be an open question. Nevertheless the Rasmussen Study was a milestone introducing PSA methods on a full scale for quantifying safety levels for nuclear power plants.

Meanwhile the methods have continuously been improved and applied to nuclear power stations.

Risk assessment has also been performed in other sectors of industry; for example, for process plants. It can be expected that risk studies will be applied more and more to support decisions on the use and further development of technologies with large hazard potentials.

The main objective of the earlier risk investigations like WASH 1400 or Phase A of the German Risk Study was to assess the risk which is associated with accidents in nuclear power plants.

However, the practical experience gained with plant engineering analyses, mainly in the last decade has shown the great benefits of PSA for technical safety assessment. The practical experience gained from the application of PSA methods to plant systems engineering analyses, and the confirmation of PSA results on the basis of operating experience, have shown that today PSA is an efficient tool for technical safety assessment.

Therefore, today PSA - complementing the deterministic approach - primarily is used to review the safety design of a plant and more generally to further develop the overall safety concept of nuclear power plants.

At present, about one hundred probabilistic studies - mostly of level 1 - for plants in 23 countries have either been completed or are under way. There is a noticeable tendency towards unifying the boundary conditions and scope of the analyses as reflected for example by the corresponding guidelines in several countries. These guidelines are substantial parts in programmes of periodic safety reviews which in some cases have already led to the so-called living PSAs.

A wider use of probabilistic analyses for decisions on proposed accident-management measures for the prevention of severe accidents or the mitigation of their consequences is foreseeable in the near future.

However, there still remain a number of topics which require closer attention, because the state of the art is not yet fully satisfactory. Among them, especially to be noted, are

- common cause failure analysis
- human error
- time dependence
- treatment of uncertainties.

This workshop is devoted to these issues and we feel that progress may best be achieved if there is an international approach.

We very much appreciate that the OECD and our ministry have asked GRS to organize this meeting. We wish all of you a vivid exchange of opinions and hope that you will have benefits from this meeting. You may get an overview of the activities in PSA in different countries and useful suggestions for your own work.

We are grateful to both speakers and participants for making this event possible and hope you'll find the effort of this workshop worthwhile.

OECD / BMU WORKSHOP
Special Issues of Level 1 PSA
Cologne, May 27. - 29. 1991

The Activities of the OECD / NEA
in Risk Assessment
- An Overview -

P.M.Herttrich
Chairman of OECD-NEA Principal
Working Group 5: Risk Assessment

OECD Nuclear Energy Agency
Committee of the Safety of Nuclear Installations
Five Principle Working Groups (PWG's)

PWG 1: Operational Experience and Human Factors

**PWG 2: Transients and Breaks
(Prevention and Control of In-Vessel Accidents)**

PWG 3: Primary Circuit Integrity

PWG 4: Source Term and Environmental Consequences (Confinement of Accidental Radioactive Releases)

- all established in 1981

PWG 5: Risk Assessment

- established in 1983

- 9 meetings (annual budget 2 - 4 days)

**- some nationally sponsored workshops:
Brighton: PSA for Safety management
Hamburg: Living PSA**

**Principal Working Group 5
Risk Assessment
Terms of Reference**

- **Technology and methods of identifying factors contributing to risk and assessing their importance**
- **Input from the other PWG's to develop common understanding of different current PRA-approaches**

Particular worthy of pursuing:

- **dominant contributors to risk (operator, experience)**
- **calculational methods (initiating events, failure prob.)**
- **particular PRA aspects, e.g. external events**
- **sensitivity to uncertainties**
- **PRA in decision making (research priorities, safety improvements)**
- **national efforts to develop quantitative safety goals**

List of PWG 5 Tasks

Tasks Already Finished before 1988

Task 1: Critical Review of Level-1 PRA

Task 2: Survey of PSA Applications

**Task 3: Role of Human Intervention in
the Prevention and Mitigation
of Severe Accidents**

Tasks finished in 1989

**Task 5: Human Reliability in Probabilistic
Safety Assessments, Use of
Operating Experience**

**Task 7: PSA as an Aid to NPP Safety
Management**

List of PWG 5 Tasks (cont'd)

Current Tasks

Regular Task:

**Current Status of PSA
Programmes in Member Countries**

**Task 4: Consideration of Quantitative
Safety Guidelines in Member
Countries**

**Task 8: PSA of LWR-Containment
Systems Performance**

**Task 9: State-of-the-Art of Level-1
PSA Methodology**

**Task 10: Fundamental Principles of
Living PSA for NPP Management**

List of additional PWG 5 Tasks

Task 11: Technical Specifications

- approach under development
- related to CNRA-activities

Task 12: Data Collection and Analysis to Support Living PSA

- detailed task plan, working group

WORKSHOP ON LIVING PSA APPLICATION HAMBURG, 7th - 8th MAY 1990

Living PSA Applications

- Reasons for performing PSA
 - * Regulatory requirement, targets
 - * Corporate requirement, targets
 - * Safety related activity prioritisation
 - * Other
- Logistic of Living PSA management
 - * Corporate management involvement
 - * Decision making levels and guidance
 - * Plant level involvement
 - * Required personnel commitment
 - * Frequency and extent of requantification of PSA
 - * Types of safety/risk parameters to be monitored
 - * Quality assurance on maintaining Living PSA
- Examples of application
 - * Experiences of application
 - * State of Living PSA/e.g. all accident involved
 - * Details of component level involvement

WORKSHOP ON LIVING PSA APPLICATION HAMBURG, 7th - 8th MAY 1990 (cont'd)

Tools for Living PSA

- Data collection systems and codes
 - * Source and type of data collected
 - * Probabilistic parameter quantification
 - * Interface to basic event data
 - * Data code systems

- Living PSA codes
 - * Event and fault tree data base management
 - * Data storage and retrieval
 - * Graphical presentations of ET/FT

- Special support codes
 - * Automated fault tree construction
 - * Human reliability quantification
 - * Uncertainty analysis

PROCEEDINGS:
CSNI-REPORT

CSNI Workshop on PSA Applications and Limitations - Santa Fe

Conclusions and Recommendations covered by PWG 5 tasks

- **Living PSA** task 10
 Definition - Uses - Approaches
- **Limitations / Special topics**
 - Human factors
 - Uncertainties
 - Non full power operationtask 9
- Data task 12
- **Uses / Special topics**
 - CET-Potential Uses for
 different approaches task 8
 - Technical Specifications task 11

STATUS OF PSA-PROGRAMMES IN MEMBER COUNTRIES

Status of PSA-Programmes in Member Countries

- CSNI-Report 172

Country by country

- programme development**
 - status and outlook**
 - tables of studies performed**
 - plant**
 - analysing team, dates**
 - methods used/procedure guide**
 - goal/insights and results/application**
-

Continuously Updated as Required:

Current Extensions:

- formal requirements or commitments
as the basis of PSA programmes in
Member Countries**
- references how to perform and
review PSA's**

TASK 4: CONSIDERATION OF QUANTITATIVE SAFETY GUIDELINES (QSG's) IN MEMBER COUNTRIES

CONTENT OF PROPOSED CSNI-REPORT-177

Definitions and Categorization of QSG's

- Legal/formal status, i.e. acceptance criteria or targets to strive for
- Level of consequence addressed (according to PSA-levels)
- Comprehensiveness (different degrees of completeness)
- Types of QSG's

Quantitative Safety Guidelines in OECD-Countries

TASK 4: CONSIDERATION OF QUANTITATIVE SAFETY GUIDELINES (QSG's) IN MEMBER COUNTRIES

(contd.)

**References to QSG's currently used
in (deterministic) regulations**

Demonstrating Compliance with QSG

- Problem Area: Definition of terms
(f.e. core melt/degradation), boundary
conditions e.g. human interventions;
state of PSA-methodology, use of
expert opinion, cut-off-techniques,
uncertainties, level of detail**

Observations

New Item:

**Discussion of the role of quantitative
PSA-Results in NPP Safety decision making**

TASK 8

PSA of the Containment System Performance

Purpose

**Discussion and comparison of methods:
containment**

- sufficient complexity to make adequate use of available information on severe accident phenomena**
- how to factor this information into a PSA**

Product

**Interim Report available
Draft Report 1991**

TASK 8 (cont'd)

PSA of the Containment System Performance

Scope

Specification of typical event sequences representative for challenges or failures of the containment system

Examination of recent PSA's, guides, handbooks and review guides

Common technical understanding of approaches that can be used for

- plant specific containment systems analysis**
- factoring in phenomenological and source term knowledge**

Level of Detail vs Objective

Approach

	Simple CETs	Inter. CETs	Detailed CETs	Check- list	Extra- polation	Issue Res'n.
1. Containment Surveillance and Inspection	X	X	X	X	*	
2. Identify Design Weaknesses	*	*	X	*	*	**
3. Accident Management			*		*	**
4. Issue Resolution			*			X
5. Safety Goal Comparison	X	X	X	*	X	
6. Research Prioritization	*	*	X	*	*	
7. Model Physical Reality	*	*	*		*	*

X - Successful at accomplishing objective

* - Partially successful

** - Only applicable for specific issue

SANTA FE, HARDER, MOD. By PWG5

PWG5_11

TASK 9: STATE-OF-THE-ART OF LEVEL 1 PSA-METHODOLOGY

- 1. Analysis of Dependencies**
 - first draft
- 2. Human Errors**
 - first draft
- 3. Time-Dependent Phenomena**
 - first status report
- 4. External Events**
 - general approach
 - seismic analysis
 - fire analysis

**5. Uncertainties
- first draft**

**6. Non full power NPP-operation,
shut down conditions**

**THIS WORKSHOP CONTRIBUTES TO
THESE TASKS**

Draft Report 1991

Task 10: DRAFT REPORT ON LIVING PSA FOR SAFETY MANAGEMENT

- 1. INTRODUCTION**
- 2. ELEMENTS OF A LIVING PSA PROGRAMM**
- 3. REVIEW OF EXAMPLES IN MEMBER COUNTRIES**
- 4. MOTIVATIONAL FACTORS BEHIND A LIVING PSA PROGRAM**
- 5. PROGRAM CHARACTERISTICS IMPORTANT TO SUCCESS**
- 6. PROGRAM STRUCTURES AND REQUIREMENTS**
- 7. TOOLS FOR LIVING PSA**
- 8. DATA ACQUISITION AND EVALUATION**
- 9. PSA DOCUMENTATION AND QUALITY ASSURANCE**
- 10. CONCLUSIONS AND RECOMMENDATIONS**
- 11. SUMMARY OF RESPONSES TO LIVING PSA QUESTIONNAIRE**

Observed Applications of living PSA-Programs

- **Monitoring safety systems performance against set reliability targets**
- **Optimization of Technical Specifications, maintenance, and testing of equipment**
- **Identification and optimization of critical operating procedures ("human factors" management)**
- **Identification of design weaknesses**
- **Design optimization during construction**
- **Screening of proposed design changes**
- **"Systems engineering" applications**
- **"Issue-balancing" integration of plant or modifications**
- **Prioritization of critical activities**
- **Modifications to allowable outage times to support continued operation**
- **Justifications for continued operation**
- **Sensibilizing management to risk dominant plant issues**
- **Prioritizing resources for a given plant and among plants within a Utility**
- **Training Optimization**
- **Support of Accident Management**

Benefits Recognized by Users

- **Plant Design and Design Process**
 - identification and resolution of plan vulnerabilities
 - integration capability (multiple safety concerns, design alternatives)
 - safety evaluation
- **Plant Operations**
 - improvements of procedures and technical specifications
 - improved equipment availability
 - improvements in operator performance
- **Internal Decision Process**
 - prioritization of plant modifications
 - elimination of ineffective changes
 - operational strategies
- **Communications with Regulators**
 - Support of regulatory interaction
 - modification of ineffective requirements
 - enhanced credibility

<p>Support to the resolution of the continuous tension between objectives of economic power production and safety</p>
--

Program Structure and Requirements

PSA-model requirements

PSA to model:

- plant configuration
- plant response under different conditions

Level 1, perhaps abbreviated Level 2:

- plant specific
- plant specific data

Program Structure and Requirements (contd.)

PSA model maintenance and update program

- Significant plant design impacting event- and fault tree models
- modifications of operating procedures, incorporation in event/fault-trees
- surveillance procedures:
modifications of test intervals and test result
- Bayesian update of initiating event statistic
- Bayesian update of component reliability data
- Modification of emergency operating procedures with impacts on operator action models
- PSA-model improvements by more refined models or additional sequences
- PSA model requantification
- PSA summary document update

Follow up activities

**Task group reviews comments,
proposals, progress**

- applications
- tools
- documentation
- quality assurance

Task 11:

Technical Specifications
- Working plan in 1991

Task 12:

**Data Acquisition and
Evaluation**

Task 12: Data Collection and Analysis to Support Living PSA

Objectives: Assistance in

- Establishment of
plant specific failure
data collection systems
- Sharing of failure data
- Analysis and application
of such data

Task Force

Schedule Report until Oct. 91

Task 12: Data Collection and Analysis to Support Living PSA

Activities

- **Collect information on existing plant specific data collection systems to support PSA**
- **Data collected: component failure events, maintenance events, test related outages, durations, human error events, initiating events, common cause events**
- **Process of collection**
- **Organizational units and extent of efforts involved**
- **Structure of data base, computer hardware and software used**
- **Component grouping used**
- **PSA input parameters calculated**
- **Methods for updates and quality assurance**

Summary and Conclusion

PSA powerful and useful investigative tool

Plant specific PSA-application necessary for adequate understanding and management of NPP safety and risk

Uncertainties and specific methodological issues need further development

Necessary

**Pragmatic, practicable PSA applications
Logic and engineering first, numbers later !**

SÄTEILYTURVAKESKUS
(STUK) - Säteilyturvallisuuskeskus
Finnish Centre for Radiation and
Nuclear Safety - Helsinki, Finland
Reino Virolainen

**OECD/CSNI Workshop
on Special Issues
of Level 1 PSA
Cologne, May 1991**

OBJECTIVES AND STATUS OF WORK OF PWG 5/TASK 9, "STATE OF THE ART OF LEVEL 1 PSA METHODOLOGY"

1 Introduction

During the annual meeting 1989, PWG 5 discussed the most problematic areas of Level-1 PSA and outlined the contents of possible new Task. Several PSA methods were still regarded to be at issue such as analysis of dependencies, human errors, time-dependent phenomena, external events and analysis of uncertainties. Based on this discussion PWG 5 decided set up Task 9, "State of the-Art of Level 1 PSA methodology". Because of the broad expertise needed, the task was divided in five subgroups according to the aforementioned topics.

As a general objective each subgroup was expected to make a review of the use and maturity of the present methods and to take a glance into the foreseeable future on the subject making remarks on challenges of the expected evolution and on the direction to go. Most of the topics in Task 9 are already "old friends". The analysis of dependent phenomena, however, is a topic which is not generally applied in present PSA studies. Therefore this subject is more into future looking task giving more flexibility to the group and possibilities to pilot work.

2 Subtask 1: Analysis of dependencies

This Task is to review the present CCF methods used in PSAs and evaluate their maturity and needs for developments.

Present status of dependent failure analysis is ambiguous. Functional and causal dependencies can be analyzed by mature qualitative and quantitative methods such as walk- and think-through analysis, fault trees and computer programs where attributes can be set for dependency factors e.g. common support systems, common rooms, common maintenance, same types of components, similar environmental circumstances and so forth whichever can be recognized causing dependencies between components.

Instead, the analysis of subtle statistical and probabilistic correlations is still in dispute. Statistical and probabilistic correlations are e.g. hidden shortages in components inherited often from past actions affecting the components such as design, manufacture, installation, leading e.g. wrong tolerances, wrong materials, flaws in materials, different environmental sensitivities and several others unforeseeable failure causes which need usually harsh circumstances to be realized as failure. Hidden shortages (often called trigger event) may expose the components to failures and if correlation is strong (coupling mechanism exist), it can increase the failure rate of components simultaneously.

This is a mental picture of the evolution of CCFs. To realize this picture, several parametric and few non-parametric CCF methods have been developed.

A common difficulty in parametric CCF methods is that the data is to be interpreted in a semi-deterministic way such that correlation between failures is zero or unity. This leads e.g. to an inevitable conclusion that only tiny credit can be given for additional redundancies of safety systems.

Parametric CCF methods raise also other questions such as how to assign correlation between CCF parameters in uncertainty analysis, how to analyse high redundancy structures (e.g. safety relief systems in BWRs) and how to credit

physical separation of trains. Last but not least problem is the interpretation of sparse data in distinguishing between potential and real CCFs.

Non-parametric methods are an option to the parametric models but a few existing methods are so far in minor use. Interesting non-parametric methods have developed Hartung (1981) and Dörre (1989).

An inevitable problem in context of CCFs is that those are highly plant specific and adequate analysis would require the use of plant specific parameters which is difficult due to sparse data base.

Two major schools of thought on how to deal with dependent and CCFs exist such as

- dependent failures are explicitly treated in fault trees without applying special CCF methods other than qualitative screening of CCFs (IREP and NREP PSA procedures Guides and IPE)
- dependent failures should be dealt with using combination of explicit and parametric methods (IEEE/ANS PRA Procedures Guide NUREG/CR-2300, IAEA Guidelines for PSA, NUREG-1150).

A simple solution would be to use explicit fault tree analysis of dependent failures supported by worldwide direct CCF estimates for systems as given in report EPRI-NP 3967. Such kind of procedure is used e.g. in Loviisa PSA.

The major objective of Task 2 is to assess the maturity of methods frequently used in PSAs for dependent and common cause failure analyses as well as to give recommendations for most urgent development needs.

3 Task 2, Human errors

Analysis of human errors is still an unresolved issue in PSA. This is due to sparse data available for Human Reliability Analysis as well as due to difficulty to cover all kind human errors by existing methods.

According to consensus definition the human errors can be divided in three categories such as

- errors prior to an accident e.g. in maintenance, calibration, testing
- errors causing an accident initiator e.g. human error results in transient
- errors in response to an accident initiator e.g. misdiagnosis of accident initiator or response needed, error in response action.

Two first steps can fairly well be analyzed from plant specific data but human actions during accidents still provide difficulties.

An inherent issue in human performance is its ambiguity. Human interactions provide both beneficial and detrimental contributions to safety. Detrimental actions typically increase the unavailability of plant systems or result in an initiating event. The beneficial actions such as correct diagnosis of initiating event and implementation of recovery of systems decrease the potential to accidents.

A methodological difficulty of human error analysis is inherited from the special nature of human mind. As far as assumption can be made that human errors are only slips or errors in following correct procedures, the present methods cover the possible errors made. If other types of errors (errors of commission) are included, less acceptable methods are available.

The available PRA Procedures guides recommend the use of methods as follows

- THERP method is recommended by IEEE/ANS Guide, IREP Guide
- SHARP procedure with various HRA methods is recommended by NREP Guide
- ASEP HRA method is recommended by NUREG-1150
- SHARP procedure is presented in IAEA guidelines
- use of simulator based TRCs for diagnosis and recovery actions are suggested by IPE Guidelines.

An interesting approach amongst the HRA methods are those based on expert judgement. SLIM-MAUD is an example of these methods. It makes use of both expert judgement and simulator based time reliability curves (TRC). Expert judgement is mentioned in brief in context of HRA in NREP, EWAT, IAEA PRA guidelines and IPE. Expert judgement is mentioned in SHARP Procedure as well.

The contemporary human error analysis suffers from two main unresolved issues such as sparse data base on all human activities and shortage of methods for dealing with errors of unplanned tasks. The sparse data on human activities such as diagnosis errors and other human actions during accident sequence can to the proper extent be replaced by using full-scale plant specific simulator. Instead the treatment of unplanned operator measures is still at early development phase.

Task Force 2 has prepared a detailed content of the report but not yet completed the first draft report.

4 Task 3, Time-dependent phenomena

Time dependent phenomena are an evolutionary topic in PSA. Only a few time dependent phenomena are modeled in PSA studies e.g. time dependent success criteria in long term

accident sequences (French PSAs). Several time dependent phenomena such as aging of component, time dependent unavailabilities (test intervals, latent failures, repair), time dependencies of accident sequences (time dependent success criteria, time dependent operator actions, time dependent physical phenomena) are usually treated in averaged way in PSAs.

In some US PSA studies time dependency of emergency diesel generator mission unavailability from the recovery of offsite power is considered. In Loviisa PSA study trend analysis (aging, learning) of failure rates has been made. Without saying that the examples given above be unique, it is evident that the contemporary PSA procedures tend rather to reject time dependent models than to adopt them. This is evident due to the model complexity and time consuming calculation routines which make the time dependent models rather less attractive.

A major incentive to introduce time dependent models in PSA studies is the extension of PSA towards Living PSA use and short term decision making. In order to deal with increasing or decreasing trends of phenomena e.g. time delays existing for recoveries and competition between degrading system function and decreasing residual heat production, more subtle models are needed.

The time dependency issue is, however, not the most burning problem in PSA but it can be regarded more as a matter of mid-term development and is expected to be introduced in due course with enhanced use of Living PSA.

5 Task 4, External Events

Subgroup, external events, of accident initiators has frequently given a significant contribution to NPP risk. Typical external events such as seismic events, fires and flooding (external, internal) are vital parts of recent PSA

studies. All these accident initiators are of clearly distinct nature as compared with internal initiators. External events are rather predecessor of accident initiators than initiators themselves. This makes the analysis of external hazards different from that of internal events.

The contribution of external events to risk is separately site and plant specific. Quite large contributions of external risks to older plants are plausible and closely argued because of the vulnerable or non-existing physical protection and separation in older designs. In new designs, however, components qualification to stand for harsh environments, adequate physical separation and risk averse lay-out are expected to diminish the risk significance of external events significantly.

An inherent methodological feature of contemporary methods is large uncertainty. Statistical uncertainties engaged in the results are in range 100 to 1000, expressed in terms of error factor. Large uncertainties involved in external risks make it difficult if not impossible to combine these results with those of internal events.

The methodological maturity of external event analysis is still partly poor. Especially the fragility analysis of components in seismic analysis need still development as well as the fire development analysis, too. Especially concerning the last mentioned methods a vital development trend is underway.

A number of fire development analysis models are available and development of several new models is underway. Multicompartment calculation codes are not yet well validated. Therefore, great care should be taken to understand the underlying fire phenomena when using these models for systems composing of complicated or big compartments. When properly used these programs offer even now an invaluable tool for fire development assessment.

The intensive model development associated, e.g. with recent HDR fire experiment program in Germany, give quite promising possibilities for future fire simulation of reactor containment buildings containing real fire loads found in nuclear reactors, such as pump oils and electrical cables. Although much development work is still needed, it is clear that already in the near future there are available validated fire simulation models running on personal computers or workstations, which can be used for quantitative fire risk estimation and mitigation of critical points of nuclear installations.

Task Force 4 has submitted the third draft report for review and only some minor efforts are needed to complete the final draft.

6 Task 5, Uncertainty analysis

Uncertainty analysis in PSA is to give a realistic picture of credibility of analysis containing usually number of uncertain features such as reliability data, modelling assumptions e.g. success criteria, systems interactions, dependent failures and CCFs and expert judgment. The uncertainty in reliability data reflects on one hand the stochastic variability and on the other hand the lack of knowledge. The modelling uncertainty is usually called incompleteness, reflecting the inability to deal with all phenomena or accident possibilities in the model.

It is often said that technical complexity is the decisive point for incompleteness issue. To certain extent this is true. In practice, however, the crucial issue seems to be not the complexity but the lack of design based and physical protection and isolation between vital safety systems, support systems and redundancies and lack of diversity. If the design based physical protection of components and separation between systems and trains are adequately

provided, it implies that reasons for dependencies, interactions and CCFs are cut down and to large extent systems and trains are independent of each other. This facilitates the modelling and lessens the exposure of the plant, systems and component to several external and internal initiators and complex dependent failures.

Even though statistical uncertainty analysis is well-known and mature part of PSA, it still contains some less discussed issues. Problems arise as dependencies are concerned. Dependencies between minimal cut sets are a problem for analytical methods (e.g. moment propagation and DPD). Dependencies between components (dependent and CCFs) raise a question of correlation between parameters of CCF methods. The reliability data itself creates dependencies between otherwise independent components. Pooling of plant specific data makes underlying correlation between parallel identical components and extends the uncertainty of systems significantly.

Uncertainty analysis is a vital part of PSA and it is used to ease decision making whether design of new plant, backfitting of operating plant, operating strategies or other Living PSA uses and compliance of PSA results with safety criteria etc. are concerned.

Task Force 5 has already completed the first draft version for review.

State-of-the-Art of Level 1 PSA.

W. F. Werner

Gesellschaft für Reaktorsicherheit (GRS) mbH

Forschungsgelände

D-8046 Garching

**OECD/BMU Workshop von
Special Issues of Level 1 PSA,
Cologne, FRG
May 28-30, 1991**

1. Introduction

A Level 1 Probabilistic Safety Assessment (PSA) for Nuclear power plants (NPP) determines frequencies and modes of severe damage to the reactor core. Such results cannot be derived directly from statistical observations. Therefore, the analyses are based on the identification of representative sets of conceivable accident sequences in the reactor system. For this purpose models of the technical systems and their components are developed and analysed. Accident sequences in plant systems are represented by event trees, which in a simplified way describe the potential effects of accident initiating events depending on the functioning or failure of the safety systems required for their control. The probabilities of failure of the systems are estimated by fault tree analyses. The use of these probabilities in the event trees then permits the estimation of the expected frequencies of occurrence of core damage. Further investigations are made to determine the mode of core damage. The analyses provide

- the topology of accident sequences;
- quantitative descriptions of the event sequences and estimates of their expected frequencies of occurrence;
- the event sequences which contribute significantly to the risks;
- insights into the adequacy of plant design and operational modes by determining those plant components and modes of operation which contribute most to the expected frequencies of the dominating core damage event sequences.

This forms the basis for judging

- the level of safety of a plant;
- the safety relevance of new scientific and technological results or of specific incidents during plant operation;
- promising approaches for the improvement of safety.

The insights gained from level 1 PSA can be used for

- eliminating vulnerabilities;
- identifying additional possibilities for improving plant safety;
- improving operational procedures;
- improving the training of operators.

In recent years numerous PSAs were completed and their results published. All were successful in at least one of the above listed aspects. The discussions in this paper are mainly based on the methodology used and the results obtained in the following studies

- Phase B of the German Risk Study on Nuclear Power Plants (DRS-B) /1/. The analysed plant is Biblis B, a 1300 MWe pressurized water reactor (PWR) with 4 main coolant loops in a large dry containment, built by Siemens-KWU.
- NUREG-1150 "Severe Accident Risks, an assessment for five US Nuclear Power Plants" /2-16/. In this study nuclear power plants of different designs are analysed:
 - Surry Power Station Block 1, a 788 MWe 3-loop pressurized water reactor of Westinghouse design, in a subatmospheric containment.
 - Zion Nuclear Plant, Block 1, a 1100 MWe 4-loop pressurized water reactor of Westinghouse design, in a large dry containment.
 - Sequoyah Nuclear Power Plant, Block 1, a 1148 MWe 4-loop pressurized water reactor of Westinghouse design, in an ice-condenser containment.
 - Peach Bottom Atomic Power Station, Block 2, a 1150 MWe boiling water reactor (BWR-4) of General Electric design, in a Mark I containment.
 - Grand Gulf Nuclear Station, Block 1, a 1250 MWe boiling water reactor (BWR-6) of General Electric design, in a Mark III containment.
- "Etude Probabiliste de Sûreté des Réacteurs a Eau sans Pression du Palier 900 MWe" (EPS 900) /17/. The analysed plant is a standardized 900 MWe 3-loop pressurized water reactor of Framatome design, in a large dry containment.
- Etude Probabiliste de Sûreté d'une tranche du Centre de Production Nucléaire de PALUEL (EPS 1300) /18/. The analysed plant is a standardized 1300 MWe 4-loop pressurized water reactor of Framatome design, in a large dry containment.
- "Probabilistic Safety Assesment for Typical Japanese BWR Plant". The analysed plant is a 1100 MWe boiling water reactor (BWR-5), in a Mark II containment /19/.
- "Probabilistic Safety Assesment for Typical Japanese PWR Plants." The analysed plant is a 1100 MWe 4-loop pressurized water reactor in a large dry containment /20/.

2. Steps of Level 1 - Probabilistic Safety Assessments

2.1. Generalities

A complete level 1 PSA comprises three tasks:

1. Collection of basic plant data
2. Identification of initiating events
3. Event sequences and reliability analyses

In the first step basic information on the plant and on the operational procedures is collected. The following two steps are concerned with potentially dangerous event sequences inside the plant, including the estimation of expected frequencies of occurrence of such event sequences. The nature of the information and data required in steps 2 and 3 depends on the scope of the analysis.

2.2 Selection of Accident Initiating Events

The selection of accident initiating events depends on the scope of the study. The most important distinction to be made is between plant internal and plant external events. Examples of plant internal events are mechanical failures of active components, malfunctions or failures of measuring or control devices, loss of energy and media supply, and human error. A further important distinction within the category of internal events has to be made with regard to different states of the investigated plant, for example:

- state of power generation, which is investigated in all level 1 PSAs
- low power and shutdown states, which are investigated only in the French studies EPS 900 and EPS 1300
- common cause initiating events which may simultaneously compromise a number of safety systems, for example:
 - internal flooding, which is considered in DRS-B,
 - fire, which is considered in DRS-B and in NUREG-1150 for the plants Surry and Peach Bottom

Among plant external accident initiating events the following are investigated:

- earthquake, which is considered in DRS-B, in NUREG-1150 for the plants Surry and Peach Bottom, and for the Japanese 1100 MWe BWRs and PWRs of latest design.

- Aircraft impact, which is considered in DRS-B
- High wind, which is considered for the Indian Point plant in the United States.

The frequencies of accident initiating transients were determined by plant specific operating data in all studies discussed in this paper.

For the accident initiator frequencies of the various categories of loss of coolant accidents and for accidents caused by steam generator tube rupture the analyses for all the above mentioned plants rely on generic data. In DRS-B the initiator frequencies for large and medium breaks in the main coolant pipes were obtained from a combination of zero events statistics and findings of probabilistic fracture mechanics analyses.

The spectrum of initiating events considered in recent Level 1 PSAs and their frequencies of occurrence can be taken from Table 1.

2.3 Event Sequence Analysis

An initiating event can be coped with by various combinations of functions of operating and safety systems. The relevant combinations of operating systems and safety systems are determined by the simulation of the plant response to the accident initiator. This includes the determination of the required number of redundant system trains of the individual safety systems (minimum success criteria). If the minimum success criteria are violated the initiating event may lead to core damage.

In an event sequence diagram (event tree) /21/ every possibility is considered which may lead to core damage. Event paths are constructed by tracing the sequences from the initiating events to specified end states. Event trees contain branch points for every required system function. At each branch point a path splits into two paths, one of which corresponds to success, the other to failure of the respective system function. Thus, a large number of paths are obtained which either lead to a safe state or to specified states posing a hazard to the reactor core (hazard states). With the exception of DRS-B, hazard states are identical with core damage states.

In order to quantify the availability respectively unavailability of the corresponding system function branching probabilities are being associated with each branch point in the event sequence diagram. The availabilities are conditional probabilities (under the condition caused by the initiating event and the event sequence). In the development of the event sequence diagram mutual dependencies of system functions as well as secondary failures are considered.

2.4 Reliability Analysis

In order to quantify the probabilities at the branch points in the event sequence diagram the failure behaviour of the respective system function has to be estimated. Observations which permit to determine the failure behaviour of the system function directly from operating experience are often not available due to the high reliability of operating and safety systems in nuclear power plants. However, the failure behaviour of components used in large numbers in the systems can be obtained from the operating experience. Therefore, the failure behaviour of system functions is reduced to the failure behaviour of its components.

In safety analyses for nuclear power plants the customary approach for this reduction is fault tree analysis /21/. Given an undesired event (for example loss of cooling) a systematic search is performed for all possible causes leading to this event. In general, this results in a large number of failure combinations of various components or subsystems. The analysis permits a clear representation even of very large technical systems. Independent failures, dependent failures, and human errors are to be included.

Practically, the analysis is performed by means of computer programs. Basically, simulation methods and analytical methods are to be distinguished. Simulation methods can be used for direct simulation of system reliability parameters or for the identification of the minimal cut sets of the fault tree. Analytical methods are also used for the determination of the minimal cut sets.

Simulation methods directly determine the reliability parameters by Monte Carlo simulation of the system behaviour. For large systems it may be extremely costly to obtain sufficiently accurate results.

Simulation methods are also used to determine the minimal cut sets of a system. In this way only the system structure is obtained which avoids the high computing time requirements of direct calculation of reliability parameters. With a practical number of trials Monte Carlo simulations do not find all minimal cut sets of a system, but only those which significantly contribute to system unavailability. This may be desirable if a system has a large number of numerically significant cut sets.

Analytical methods find all minimal cut sets of a system. In contrast to simulation methods, they do not require information on component failure behaviour in order to obtain the minimal cut sets. Component failure data are only needed for the calculation of the failure probability of the system, once the minimal cut sets are determined. For fault trees with a large number of minimal cut sets it may be necessary to apply cut-off criteria.

Direct simulation is a flexible method for the analysis of complex systems. Different maintenance and repair strategies, or the activation of standby systems can be easily accounted for. They are easy to use, but may impose a high demand on computing capacity for analysing highly reliable systems.

Methods based on cut sets provide deeper insights into the structure of the system. However, they are less flexible than direct simulation. For systems with a large number of cut sets, they may also pose computing time problems.

Experience suggests that both methods should be available: simulation methods for large, strongly intermeshed fault trees with not to "small" values of the reliability parameters, and analytical methods for all fault trees with "small" values of the reliability parameters, where the borderline to "small" depends on computing capacity. Presently it is at about 10^{-5} .

2.5 Data Base

In all state-of-the-art studies the data for the frequencies of initiating events, for independent as well as for common cause component failures, and for human failures are described in terms of probability distributions. The uncertainty ranges characterized by the distributions vary in origin. If an estimate is based on plant-specific data, the range should be characteristic of the statistical uncertainty of the data. If an estimate is generic (or non-plant specific) the range should be characteristic of those factors which may affect the failure properties of the component in uses and environments different from which the data for the estimate have been gathered.

The following probability distribution functions are found in level 1 PSAs:

- lognormal distribution, which is used in all recent studies,
- Gamma and Weibull distributions which are used in DRS-B,
- maximum entropy distribution which is used, for example, in NUREG-1150.

If in a plant specific analysis plant specific data are of insufficient quality they are sometimes combined with available generic data by means of Bayes' Theorem. In this case a prior distribution is determined by generic data, which is combined with the available plant specific data in order to obtain an a posteriori distribution to be used for the plant specific analysis. This process is used for example in DRS-B, in NUREG-1150 for the analysis of the Zion plant, and in EPS 900 and EPS 1300.

The sources for data for independent failures of components used in recent studies are compiled in Table 2

- Table 2. Sources of Component Failures Data for Independent Failures

	Plant specific data	Generic data
DRS-B	/31/	/32 - 34/
NUREG-1150	LER, OLB*	/3/
EPS 900, EPS 1300	/30/	
Japan	Japanese operating experience	/3/, Japanese operating experience

*) LER: Licensee Event Reports for US Commercial NPPs.
OLB: Operator log books

Uncertainties of failures data:

The error factors (95% quantile: 50% quantile of the lognormal distribution) vary between 1.03 and 11. The error factors for plant specific data usually do not exceed 5.

In NUREG-1150, the Japanese studies, and in DRS-B the differentiation with regard to location and operating conditions of components is more detailed than in EPS 900 and EPS 1300. On the other hand, the data base in EPS 900 and EPS 1300 is much larger (200 reactor years for the standardized 900 MWe plants and 10 reactor years for the standardized 1300 MWe plants, which all have identical components) than in any other study. Accordingly, the error factors are considerably smaller for many components in EPS 900 and EPS 1300.

2.6 Dependent failures

Besides independent failures of system functions, so called dependent failures may occur. Their consequences may be severe if they simultaneously compromise the function of redundant components or subsystems. Distinction is made between

- failures of two or more redundant components or subsystems caused by functional dependencies.
- Failures of two or more redundant components or subsystems as a result of a single previous failure; such failures are called secondary failures.
- Failures of two or more redundant components or subsystems due to an unspecified single shared cause; they are called common cause failures (CCF).

Usually dependent failures and secondary failures are explicitly treated in the fault trees. Then there remain the common cause failures which, for example, may be due to a common construction or maintenance error.

In the highly reliable systems of nuclear power plants common cause failures are extremely rare. Therefore they can normally not be quantified on the basis of operating experience. Instead, recourse must be taken to models which have evolved from insights of past PSA studies and from the evaluation of operating experience.

Most of the common cause failure models used like the Beta Factor Model (BFM) and the Multiple Greek Letter Model (MGL) have no causal structure.

The parameters of these models are free parameters to be fitted to the available data on observed single (potentially common cause), double, triple, etc. failure events. The Binomial Failure Rate Model (BFR) has an underlying causal structure. Mechanisms, called shocks, are considered, which affect all components in a redundancy. The probabilities of multiple failures are described on the basis of the frequencies of the shocks and according to the assumption that the numbers of failed components are binomially distributed.

The success of quantitative common cause failure analysis depends primarily on the quality and quantity, as well as on the interpretation of reliability data. Since data on multiple failures are extremely scarce, significant improvement in the quantification is not to be expected soon. With presently available common cause failure probabilities some PSAs show very large contributions to the core damage frequency from common cause events.

In recent PSAs the following common cause failures models are used:

The BFM-model with modifications accounting for failures of triple or higher redundancies /22/ is used in NUREG-1150, in EPS 900 and EPS 1300, and in the Japanese studies of 1100 MW BWRs and PWRs.

An error factor of three is used to describe the uncertainty about the common cause failures for all degrees of redundancies.

The BFR-model /22/ is used in the Biblis B analysis. Error factors of five, seven, respectively twelve, based on engineering judgement, are used to express uncertainties for common cause failures of two, three, respectively four

redundancies. For the analysis of common cause failures in the scram system of the Biblis B reactor the uncertainty distributions are consistently obtained from uncertainties for single failure, shock rate, and binomial parameter.

The resulting error factor for the mean unavailability of the rods required according to the minimum success criterion (failure of > 7 rods out of 61 rods) is about 500.

To reduce the large influence of common cause failure rates on the analysis result, it is desirable to

- systematically inspect observed single failures for potential common cause mechanisms in order to enlarge the common cause failure data base.
- to introduce more diversity in the systems design as a defence against the influence of common cause failures on highly redundant components or systems.

2.7 Human Factor

Two kinds of human errors are to be considered in PSAs.

- Error of omission (an operator does not fulfill a required task) which is treated in all recent PSAs. The standard method used for its quantification is the THERP method /23/, and in some cases SLIM /24/.
- Error of commission (acts by operators outside of procedures, caused by vague procedures, misleading instrumentation, simply errors on the side of the operator).

Errors of commission are not comprehensively treated in PSAs for nuclear power plants. However, recent evaluations of operating experience and theoretical analyses indicate that the influence of errors of commission may be significant, in particular in low power and in shutdown states.

In all PSA's the influence of the human error on the analysis results is significant, see tables 4,6

3. Uncertainties and Limitations

Uncertainties and limitations are inherent to all PSAs.

- Quantifiable Uncertainties

Quantifiable uncertainties are an integral part of every PSA. They result from the uncertainties about initiating event frequencies, reliability parameters, the actions of the operating team (parameter uncertainties) and from uncertainties related to the physics of the evolution of the accident (modelling uncertainties). The latter are sometimes formally expressed as parameter uncertainties by introducing weighted sums of model alternatives.

The standard technique to quantify parameter uncertainties is to perform Monte Carlo sampling from the probability distributions describing the various uncertainties and propagating the samples through the steps of the analysis, thus generating a mapping from the parameter uncertainties to the uncertainties of the results of the analysis.

Monte Carlo sampling is either done directly, which permits to quantify the sampling error by tolerance limits, or it is done by Latin Hypercube sampling which is sometimes numerically more efficient than direct Monte Carlo sampling, however, at the disadvantage of not providing a mechanism for quantifying the sampling error.

The influence of the parameter uncertainties on the analysis results is shown in all studies but EPS 900.

No published Level-1 PSA contains a comprehensive treatment of modelling uncertainties

- Limitations of scope

PSA results are limited to certain classes of issues that can be readily included in the structure of PSA models. The scope of accident sequences analysis is generally limited to component failures of specific types and operator errors to correctly perform prescribed actions. The consideration of initiating events is also limited in scope. It is important to be aware of the potential implications of such limitations.

Today, PSAs exclude a large number of very low probability events, because of their anticipated unimportance, or the difficulty of modelling them. For example, errors of commission are often excluded simply because there is no generally accepted modelling approach.

Many PSAs produce core damage frequencies between 10^{-6} and 10^{-4} per reactor year. In that situation it is reasonable to neglect accidents that

occur with frequencies two or three orders of magnitude below the core melt frequency.

However, the insights from PSAs have served to drastically reduce the contribution to the core damage frequency from those failures and events that are generally modelled.

In some recent PSAs core damage frequencies lower than 10^{-6} per year result. With the core damage frequency being so low the quantitative results may be questioned, as there is no technical basis for concluding that events outside the scope of the PSA would not contribute at least at that level.

Uncertainty analyses conducted for recent PSAs provide realistic characterisations of the quantifiable uncertainties. However, issues whose uncertainties are not quantified, because they are outside the scope of a PSA may become significant. Some of these are discussed below:

- Accidents occurring at low power and shutdown conditions

Until recently, virtually all PSAs for nuclear power plants were performed for full power conditions. This was considered to be a conservative approach, based on having the maximum amount of energy available in the core, which maximizes the system response requirements and minimizes the time available to prevent core damage. However recent PSAs and precursor events indicate that accidents occurring at conditions other than full power may be significant contributors to the core damage frequency.

Some of the reasons for these findings are:

- Major maintenance activities related to safety are often carried out during shutdown. Depending on the particular shutdown mode technical requirements for safety systems may be minimal. Thus the redundancy usually required at full power may not exist.
- Sufficient decay heat is still present to lead to core damage.
- The operators' response can be expected to be less proficient in shutdown conditions. Emergency operating procedures are limited for shutdown conditions; the plant's state is often not clear due to the large number of maintenance activities under way, and the control room staff may be less attentive.
- The integrity of the primary cooling system may be compromised as a result of ongoing operations. With the primary system depressurized and partially drained down in some cases, the boil-off time is reduced and the effectiveness of retention of radionuclides in the primary system may be degraded.

- Containment integrity may be compromised during shutdown. Thus, the likelihood of radionuclides being held in the containment is reduced and offsite releases may be expected to occur within minutes after the onset of core damage.

The analysis of low power and shutdown accidents is difficult. Within different plant operating modes, different technical requirements apply and therefore different plant configurations are possible, requiring separate analysis. A larger number of usually more complex human interventions may be required. This poses problems of quantification.

- Design and construction errors

In a PSA it is generally assumed that all components in the plant are properly constructed and designed. These assumptions are only confirmed in cases where components are correctly tested under the same conditions that will be present during an accident. Unfortunately, many safety systems do not fall in this category along with non-safety systems that could be used as alternative coolant injection sources such as firewater systems.

Currently, the technical basis for comprehensively estimating the importance of design and construction errors is weak. However, such errors could dominate results of PSAs which exhibit low core damage frequencies.

- Operator errors of commission

Operator errors of commission are acts by operators outside specified procedures. They can occur as a result of vague procedures, misleading instrumentation, or simply errors of the operators. Including such errors in PSAs is extremely difficult, because the number of possible actions to be considered is almost unlimited. Even if such actions can be identified, quantification remains difficult.

However, with a few exceptions, such errors are not considered for the postaccident phase. Yet, analyses of events observed during recent years indicate that serious errors of commission in the control room which could bring a plant into a deteriorated state with regard to safety systems could have frequencies of occurrence comparable to the frequency of occurrence of technically initiated incidents [25-29]. Therefore, the investigations in the studies may not be balanced between the analysis of accident sequences caused by technical failures and the analysis of sequences caused by errors of commission.

- Common cause failures affecting multiple systems

All recent PSAs consider common cause failures of identical components within a system. The effect of some common cause failures, such as faulty maintenance is not limited to components within a particular

system. However, such failures between systems are not generally included in PSAs.

- Sabotage

Sabotage differs from an operator error of commission in that it implies willful damage to the facility. Sabotage frequencies are generally not quantified in PSAs for several reasons

- Sabotage is not an accident and is usually considered to be inherently different from the events normally included in PSAs.
- The frequency and character of the sabotage events are very difficult to determine.

4. Numerical Results of Level 1 PSAs

The numerical results of level 1 PSA are obtained in terms of probability distributions, (cf. Fig. 1). In tables exhibiting PSA results, point values characterizing the distribution function are usually shown, e.g. the median or the mean. Frequently, the lower 5% and upper 95% quantile are also shown.

The results of accident sequence analyses explicitly refer to

- core damage and additionally to
- intermediate states reached prior to core damage.

Intermediate states prior to core damage are introduced in NUREG-1150 and in DRS-B. Their definition, however, is different in the two studies.

In DRS-B the intermediate states are defined by the failure of those functions of the engineered safety systems and actions of the personnel according to the operating manual which are needed to cope with the initiating event. Such failures lead to insufficient decay heat removal from the core. The conditions are called "hazard states" in DRS-B. Without appropriate measures to restore heat removal capabilities, hazard states will finally lead to core damage. (These measures are called "anlageninterne Notfallmaßnahmen" which translates as "plant internal accident management measures" in the DRS-B study). All modifications to hardware and procedures found appropriate during the analysis, also future ones if already decided upon, are accounted for in the estimation of frequencies of the hazard states.

The hazard states are further differentiated with regard to characteristics like pressure in the reactor coolant loop, failures on primary side and/or secondary side systems, and the time intervals available to perform accident management measures. End points of the systems analysis event trees, respectively, top events for the associated fault trees are the hazard states (not core damage).

By plant internal accident management measures the plant can be returned from a hazard state to a safe state. If all plant internal accident management measures applicable to a given hazard state fail, core damage will result.

With regard to hazard states the DRS-B study explicitly presents:

- the expected frequencies of occurrence of the various hazard states
- the contributions of unavailabilities of system functions to the individual hazard states and to the sum of the expected frequencies of all hazard states, (Fig. 2)
- the contributions of groups of initiating events to the sum of the expected frequencies of all hazard states.

In NUREG-1150, EPS 900, EPS 1300 and the Japanese studies, the level 1 results refer to core damage. In NUREG-1150, intermediate states analogous in a way to the hazard states in DRS-B are considered in the analysis. Their frequencies can be obtained from the study.

Accident management measures which, in principle correspond to the plant internal accident management measures considered in DRS-B are incorporated into the event trees and the fault trees in all other recent studies. In NUREG-1150 they are called "recovery actions". They are not always directly comparable to the plant internal accident management measures accounted for in DRS-B. For example, some of the recovery actions considered in NUREG-1150 for the termination of accident sequences caused by steam generator tube ruptures are applied in the area of design basis accidents.

The EPS 900 and EPS 1300 studies consider accident management measures called H- and U-procedures.

The combined numerical effectiveness of accident management measures applicable to event sequence classes is explicitly given for all event sequence groups in DRS-B, and for the majority of event sequence groups in EPS 900 and EPS 1300 in terms of reduction factors between core damage frequencies without and with consideration of accident management measures. In NUREG-1150 such figures are not explicitly shown, but can be derived from the quantified event trees.

All studies discussed in this paper present the sum of the relative frequencies of core damage caused by plant internal initiators, and show how the individual groups of initiating events contribute to this sum (Figs. 3-8).

Fig. 9 compiles the total core damage frequencies obtained in recent studies, and the associated uncertainty ranges (from 5% to 95% quantiles), if available.

Other typical results are the importance, according to one of the commonly used measures, of component failure rates (single or common cause), systems unavailabilities, and of human failure rates (Tables 3-6).

5. Summary

The strengths of the PSA methodology arise from both the integration of different techniques of analysis and from the integration of the various aspects of design and operation of a NPP. Integration of systems analysis, probability models, human reliability modelling and models to describe the physical phenomenology of accident scenarios into one coherent framework enables one to manage a much wider range of accident scenarios in a single analysis than can be handled by alternative approaches. In doing PSA a this give a picture of the safety or risk profile of a nuclear power plant that is more comprehensive and balanced than other approaches to reactor safety assessment.

A PSA is different from a traditional deterministic safety analysis in that it has better chances of being complete in indentifying accident sequences that can occur from a broad range of initiating events, and it involves the systematic determination of accident frequencies and consequences.

However, the accuracy and the robustness of the results of a PSA are limited by our overall state of knowledge. PSA is only a model for collecting and treating the available body of knowledge. This knowledge is expressed in accumulation of data and in models for system behaviour and for physical and chemical processes. Any set of PSA results therefore reflects the limitations in the database as well as the limitations and simplifications of the modelling approach that result from our state of knowledge.

Despite such limitations, the principal benefit in using level 1 PSAs to increase insights and to support decisions concerning reactor safety is to take advantage of the power of PSAs to give a comprehensive, realistic and balanced picture of reactor safety without becoming vulnerable to misconceptions arising from the many substantial uncertainties involved. The fact that PSAs provide a mechanism for displaying the causes and magnitudes of uncertainties (more so than do conventional deterministic analyses) is actually the strength of PSA rather than evidence of a weakness of the PSA methodology, because it can provide additional qualitative and quantitative perspectives on the overall importance of uncertainties.

The most valuable products of PSA are the insights gained and the actions taken to address those insights. Additionally, the results are considered to be of importance in assessing the significance of safety issues, and to support and promote allocation of resources to the resolution of these issues.

This is illustrated by the following list of reported successful uses of level 1 PSAs.

- Uses for Optimisation of Plant Design and Operation
 - conceptual or detailed plant design;
 - supplementary analyses during licensing procedures;

- plant-specific evaluation of operational experience or other new information;
 - evaluation of plant modifications from a safety viewpoint;
 - evaluation and assessment of management and operational policies in shutdown and startup conditions;
 - evaluation of accident management policies;
 - evaluation of maintenance and testing activities;
 - evaluation of precursor events as a measure of performance to desired goals;
 - living PSAs;
 - prioritization of competing research needs
-
- Regulatory Uses
 - guidance to regulatory standards development;
 - specific applications of deterministic principles (classification of design basis events according to their expected frequencies);
 - demand of periodic reassessment of plant safety on a probabilistic basis using plant-specific "as-operated" data;
 - supplementary information for licensing purposes;
 - establishing probabilistic "safety assessment principles" or quantitative design or safety goals;
 - aiding in the determination of whether or not backfits should be required;
 - emergency planning;
 - demonstrating compliance with safety goals.

References

- /1/ Deutsche Risikostudie Kernkraftwerke, Phase B
Verlag TÜV Rheinland, Köln, 1990
- /2/ Severe Accident Risks: An Assessment for Five US Nuclear Power Plants,
Summary Report, 2nd Draft for Peer Review, NUREG-1150, Vol.1 and 2,
June 1989
- /3/ D.M. Ericson, Jr., (Ed.) et al.: Analysis of Core Damage Frequency:
Methodology Guideline
Sandia National Laboratories, NUREG/CR-4550, Vol. 1, Rev. 1,
SAND86-2084, Jan. 1990
- /4/ T.A. Wheeler et al.: Analysis of Core Damage Frequency from Internal
Events: Expert Judgment Elicitation, Sandia National Laboratories,
NUREG/CR-4550, Vol. 2, SAND86-2084, April 1989
- /5/ R.C. Bertuccio and J.A. Julius: Analysis of Core Damage Frequency: Surry
Unit 1, Sandia National Laboratories, NUREG/CR-4550, Vol. 3, Rev. 1,
SAND86-2084, April 1990
- /6/ A.M. Kolaczowski et al.: Analysis of Core Damage Frequency: Peach Bott
Unit 2, Sandia National Laboratories, NUREG/CR-4550, Vol. 4, Rev. 1,
SAND86-2084, Aug. 1989
- /7/ R.C. Bertuccio and S.R. Brown: Analysis of Core Damage Frequency:
Sequoyah Unit 1, Sandia National Laboratories, NUREG/CR-4550, Vol. 5,
Rev. 1, SAND86-2084, Jan. 1990
- /8/ M.T. Drouin et al.: Analysis of Core Damage Frequency: Grand Gulf Unit 1,
Sandia National Laboratories, NUREG/CR-4550, Vol. 6, Rev. 1,
SAND86-2084, Sept. 1989
- /9/ M.B. Sattison and K.W. Hall: Analysis of Core Damage Frequency: Zion
Unit 1, Idaho National Engineering Laboratory, NUREG/CR-4550, Vol. 7,
Rev. 1, EGG-2554, May 1990
- /10/ E.D. Gorham-Bergeron et al.: Evaluation of Severe Accident Risks:
Methodology for the Accident Progression, Source Term, Consequence, Risk
Integration, and Uncertainty Analyses, Sandia National Laboratories,
NUREG/CR-4550, Vol. 1, Draft Revision 1, SAND86-1309, to be
published.
- /11/ F.T. Harper et al.: Evaluation of Severe Accident Risks: Quantification of
Major Input Parameters, Sandia National Laboratories, NUREG/CR-4551,
Vol. 2, Draft Revision 1, SAND86-1309, to be published.
- /12/ R.J. Breeding et al.: Evaluation of Severe Accident Risks: Surry Unit 1,
Sandia National Laboratories, NUREG/CR-4551, Vol. 3, Draft Revision 1,
SAND86-1309, to be published.

- /13/ A.C. Payne, Jr., et al.: Evaluation of Severe Accident Risks: Peach Bottom Unit 2, Sandia National Laboratories, NUREG/CR-4551, Vol. 4, Draft Revision 1, SAND86-1309, to be published
- /14/ J.J. Gregory et al.: Evaluation of Severe Accident Risks: Sequoyah Unit 1, Sandia National Laboratories, NUREG/CR-4551, Vol. 5, Draft Revision 1, SAND86-1309, to be published
- /15/ T.D. Brown et al.: Evaluation of Severe Accident Risks: Grand Gulf Unit 1, Sandia National Laboratories, NUREG/CR-4551, Vol. 6, Draft Revision 1, SAND86-1309, to be published
- /16/ C.K. Park et al.: Evaluation of Severe Accident Risks: Zion Unit 1, Brookhaven National Laboratories, NUREG/CR-4551, Vol. 7, Draft Revision 1, BNL-NUREG-52029, to be published
- /17/ Etude Probabiliste de Surete' des Reacteurs a` Eau sous Pression du Palier 900 MWe, Rapport de Synthese, IPSN, April 1990
- /18/ Etude Probabiliste de Surete' d'une tranche du Centre de Production Nucleaire de Paluel (1300 MWe), Rapport de Synthese, ESP 1300, Mai 1990
- /19/ H. Murakami: Probabilistic Safety Assessment for Typical Japanese BWR Plants, IAE-R8903, Proceeding of 4th National Symposium on Probabilistic Safety Assessment, 1989
- /20/ Y. Tsujikura: Probabilistic Safety Assessment for Typical Japanese PWR Plants, IAE-R8903, Proceeding of 4th National Symposium on Probabilistic Safety Assessment, 1989
- /21/ U. Hauptmanns, W. Werner: Engineering Risks, Evaluation and Valuation, Springer Verlag, 1991
- /22/ Mosleh, Flemming, Parry, Paula, Worledge, Rassmuson: Procedures for Treating Common Cause Failures in Safety and Reliability Studies NUREG/CR-4780, Vol. 1, Jan. 1988
- /23/ A.D. Swain and H.E. Guttman: Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications, NUREG/CR-1278, SAND80-0200, Sandia National Laboratories, Albuquerque, NM, August 1983
- /24/ E.E. Embrey, et al.: Success likelihood Index Methodology (SLIM-MAUD), An Approach to Assessing Human Emer Probabilities Using Structured Expert Judgement, NUREG/CR-3510, Vol 1,2, 1984
- /25/ J.M. Gandit: Enseignement et actions correctives de'cide'es apre`s l'incident survenu a` Bugey 5, le 14 avril 1984: -International Conference on the Performance and Safety of Nuclear Power Plants, Vienna, Austria, 28 September-2 October, 1987, IAEA-CN-48/122

- /26/ Blayais 3, indisponibilité de l'injection de sécurité lors du redémarrage: Rapport d'activité 1986, Service Central de Sécurité des Installations Nucléaires, p 94, Ministère de l'Industrie des PTT et du Tourisme
- /27/ Violation of Technical Specifications for Operation of the Oskarshamn 3 NPP on July 24, 1987, Swedish Nuclear Power Inspectorate Technical Report 87/5 (In Swedish, with English summary)
- /28/ Hörtnér, H.: Zum Nichtschliessen der Erstabsperrarmatur im Not- und Nachkühlssystem im Kernkraftwerk Biblis, Block A am 17.12.87, Atomwirtschaft, Dezember 1989, pp 580-82
- /29/ AEOD Concerns Regarding the Power Oscillation Event at LaSalle 2 (BWR), NRC AEOD Report AEOD/S803
- /30/ J. Dorey, P. Bergeron (EdF): SRDF - Le système de recueil de données de fiabilité d'Electricité de France, Second colloque international sur la fiabilité et la maintenabilité, Perros-Guirec, Septembre 1980
- /31/ P. Hömke, H.W. Krause, W. Ropers, C. Verstegen, H. Hüren, H.V. Schlenker, P. Dörre, A. Tsekouras: Zuverlässigkeitskenngrößenermittlung im Kernkraftwerk Biblis B, Abschlußbericht, GRS-A-1030/Band I bis VI, Dezember 1984
- /32/ RWTÜV, GRS, TÜV-Rheinland: Untersuchung der Zuverlässigkeit von Druckabsicherungen in Kernkraftwerken, Ergebnisse des vom Bundesminister des Inneren geförderten Forschungsvorhabens SR 214, Berichts-Nr.: 911-258/81, TÜV Rheinland, Köln, September 1981
- /33/ TÜV-Leitstelle Kerntechnik bei der VdTÜV: Statistische Untersuchung der Zuverlässigkeit von Notstromdieselanlagen in deutschen Kernkraftwerken, Verlag TÜV Rheinland, Köln, 1983
- /34/ GRS, TÜV Rheinland, RWTÜV: Auswertung der Betriebserfahrungen mit Sicherheitsarmaturen, Ergebnisse des vom Bundesminister des Inneren geförderten Vorhabens SR 297, RWTÜV, Essen, Januar 1985

Table 1.1

Initiating Events and Frequencies Used in the Surry PSA

Description	Mean Frequency (per year)
Loss of Offsite Power	7.7 E-2
Transients with Loss of Main Feed Water (MFW)	9.4 E-1
Transients with MFW Initially Available	7.3
Non-Recoverable Loss of DC Bus A	5.0 E-3
Non-Recoverable Loss of DC Bus B	5.0 E-3
Steam Generator Tube Rupture	1.0 E-2
Large LOCA, 6" - 9"	5.0 E-4
Medium LOCA, 2" - 6"	1.0 E-3
Small LOCA, 1/2" - 2"	1.0 E-3
Very Small LOCA, less than 1/2"	1.3 E-2
Interfacing LOCA	1.6 E-6

Table 1.2

Initiating Events and Frequencies Used in the Grand Gulf PSA

Desription	Mean Frequency (per year)
Loss of Offsite Power (LOSP) transient	0.11
Transients with Loss of Power Conversion System (PCS)	1.62
Transients with PCS initially available	4.51
Transients involving Loss of Feedwater (LOFW) but with the steam side of the PCS initially available	0.76
Transient caused by an Inadvertent Open Relief Valve (IORV) on the reactor vessel	0.14
Transient caused by Loss of Instrument Air	8.1 E-4
Large Loss of Coolant Accident (LOCA)	1.0 E-4
Intermediate LOCA	3.0 E-4
Small LOCA	3.0 E-3
Small - small LOCA (recirculation pump seal LOCA)	3.0 E-2

Table 1.3

Initiating Events and Frequencies used in the EPS 900

Family	Main sub-Initiating events	Frequency per reactor year
LOCA	<div> <div> Large breaks Intermediate breaks Small breaks Breaks with RHRS connected </div> <div> } RHRS disconnected } </div> </div>	1×10^{-4} 3×10^{-4} 2×10^{-3} 5×10^{-4}
SSLB	<div> Large SLB inside containment Small SLB in any location Small FWLB </div>	1×10^{-4} 7×10^{-3} 1×10^{-3}
SGTR and SSLB + SGTR	<div> Rupture of one steam generator tube Rupture of two steam generator tubes </div>	6×10^{-3} 5×10^{-4}
Loss of Systems RRI/SEC (H1)	<div> Loss of water intake Loss of CCW/SEC in two engineered safety feature trains Large leak in one CCW train </div>	7.5×10^{-5} 1.5×10^{-5} 1.3×10^{-2}
Loss of steam generator feedwater supply (H2)	<div> Loss of the MFW Loss of the AFW in shutdown on the AFW </div>	1.92 6.9×10^{-4}
Power blackout (H3)	<div> RHRS disconnected RHRS connected </div>	4.1×10^{-4} 5.3×10^{-5}
ATWS	<div> Total loss of the MFW (power > 30% nominal) without scram Partial loss of the MFW (power > 30% nominal) without scram Total or partial loss of the MFW (power < 30% nominal) without scram </div>	1.8×10^{-5} 3.8×10^{-6} 6.5×10^{-6}
Primary system transients	<div> Spurious safety injection Spurious heater demand Progressive spurious dilution (all states) Dilution by water front (hot shutdown) </div>	0.32 4.1×10^{-2} 3.5×10^{-2} 1.1×10^{-6}
Secondary transients	<div> Total loss of secondary load Closure of one main steam valve </div>	8.7×10^{-2} 0.1
Loss of electrical power supplies	<div> Main off-site supply Off-site supplies Bus LH (6.6 kV) LC (48 V) LDA (30 V) </div>	0.3 2.9×10^{-2} 1.9×10^{-3} 2.3×10^{-3} 1.1×10^{-2}
Loss of compressed air	<div> Loss of System SAP (compressed air production) Loss of System SAR reactor building emergency supplied section </div>	2.8×10^{-3} 6.1×10^{-4}

Table 1.4

Initiating Events and Frequencies used in DRS-B

Initiating Event	Leak Cross Selection (cm ²)	Frequency (1/a)	
		Initiating Event	Triggering Event
<u>leaks in reactor coolant piping</u> large and medium leak	< 200	< 10 ⁻⁷	
small leak 1	80 - 200	9,0x10 ⁻⁵	
small leak 2	50 - 80	7,5x10 ⁻⁵	
small leak 3	25 - 50	7,5x10 ⁻⁵	
small leak 4	12 - 25	1,4x10 ⁻⁴	
small leak 5	2 - 12	2,8x10 ⁻³	
<u>leaks at pressurizer</u> small leaks at pressurizer caused by transients			
loss of main feedwater	20	1,4x10 ⁻¹	3,2x10 ⁻⁵
loss of main heat sink	20	1,4x10 ⁻¹	3,3x10 ⁻⁵
other transients	20	5,3x10 ⁻¹	1,2x10 ⁻⁴
small leaks at pressurizer due to inadvertent opening of safety valve	40	2,0x10 ⁻²	8,5x10 ⁻⁴
leak in connecting line to annulus	2 - 500	10 ⁻² to 10 ⁻⁵	< 10 ⁻⁷
<u>steam generator tube rupture</u>			
small leak 1	6 - 12	1,0x10 ⁻³	
small leak 2	1 - 6	6,5x10 ⁻³	

Table 1.4 Continued

Initiating Event	Frequency (1/a)
<u>operating transients</u>	
loss of preferred power	0,13
loss of main feedwater with power conversion system available (long-term)	0,15
loss of main feedwater and power conversion system	0,29
loss of power conversion system without loss of main feedwater	0,36
<u>transients caused by leaks in main steam line</u>	
large leak	
- inside containment	$1,6 \times 10^{-4}$
- outside containment	$4,8 \times 10^{-4}$
medium leak	
- inside containment	$2,7 \times 10^{-5}$
- outside containment	$1,1 \times 10^{-4}$
<u>operating transients with failure of reactor scram (ATWS)</u>	
ATWS during loss of main feedwater	$4,7 \times 10^{-6}$
ATWS during loss of power conversion system	$3,4 \times 10^{-6}$
ATWS during loss of main heat sink and main feedwater	$7,5 \times 10^{-6}$
ATWS during other transients	$2,3 \times 10^{-5}$

Table 1.5

Initiating Events and Frequencies used in the PSA for Japanese 1100 MWe PWR

Initiating Events	Occurrence Frequency (Mean, 1/RY)	Comment
Large LOCA	4.8×10^{-5}	- upper bound of small LOCA is obtained assuming occurrence of one time - 554 RY is used, which is operating years of Japanese and US PWRs - ratio among large, medium and small LOCA from WASH- 1400
Medium LOCA	1.5×10^{-4}	
Small LOCA	4.8×10^{-4}	
SGTR	2.5×10^{-3}	- lower bound from US PWR experience
Secondary side break	2.4×10^{-3}	- mean value from US PWR experience
Loss of offsite power	1.0×10^{-2}	- occurred three times (experience of Japanese PWRs and BWRs) - operating years of Japanese plants PWR: 136 RY, BWR: 154 RY (till March 1988)
Loss of PCS	3.7×10^{-2}	- operating experience of Japanese PWRs
Other Transient	2.1×10^{-1}	

Table 1.6.

Initiating Events and Frequencies used in the PSA for Japanese 1, 100 MWe-class BWR

Initiating Event	Occurrence Frequency (Mean value) (RY)	Remarks
Large LOCA (A)	8.0×10^{-5}	<ul style="list-style-type: none"> - The small LOCA is assumed to have occurred once and taken as the upper bound. - The 508 reactor years of Japan and U.S.BWR operation experiences is used. 148RY (Japan) + 360RY (the U.S.A.): (up to December, 1978) - The proportions of large, intermediate and small LOCAs are determined according to WASH-1400 evaluation method.
Intermediate LOCA (S_1)	2.7×10^{-4}	
Small LOCA (S_2)	8.0×10^{-4}	
Transient with the PCS initially available (T_A)	0.47	<ul style="list-style-type: none"> - The domestic BWR experiences are used. 154 reactor years (up to March, 1988).
Transient with the PCS initially unavailable (T_U)	0.078	
Loss of Offsite Power (T_E)	1.0×10^{-2}	<ul style="list-style-type: none"> - Occurred three times. - The domestic plant experiences are used. 154RY (BWR) + 136RY (PWR): (up to March, 1988)

Table 3

Results of Sensitivity Study in which Common Cause Failures were eliminated from Fault Trees, (NUREG-1150).

Plant	Base Case Analysis	Sensitivity Study No Common Cause Failures	Percent Reduction
Surry	4.01 E-5	3.08 E-5	23
Sequoyah	5.72 E-5	4.57 E-5	20
Peach Bottom	4.50 E-6	4.07 E-6	10
Grand Gulf	4.05 E-6	3.10 E-6	26

Table 4

Core Damage Frequencies with and without human Errors of Ommission, (NUREG-1150)

Plant	Core Damage Frequency		
	Base Case	No Errors	Factor of Reduction
Grand Gulf	4.1 E-6	6.2 E-7	6.6
Peach Bottom	4.5 E-6	9.5 E-7	4.8
Sequoyah	5.7 E-5	2.5 E-5	3.5
Surry	4.0 E-5	1.1 E-5	3.8

Table 5

Contributions of Common Cause Failures to Hazard States at Biblis-B

Event Sequence	Common Cause Contribution in %
Loss of Offsite Power	80
Loss of Power Conversion System	80
Loss of Main Feedwater	65
Main Steam Line Break	50

Table 6

Contributions of Human Errors of Omission to Hazard States at Biblis-B

Event Sequence	Human Error Contribution in %
Loss of Offsite Power	15
Loss of Power Conversion System	50
Loss of Main Feedwater	50
Main Steam Line Break	5

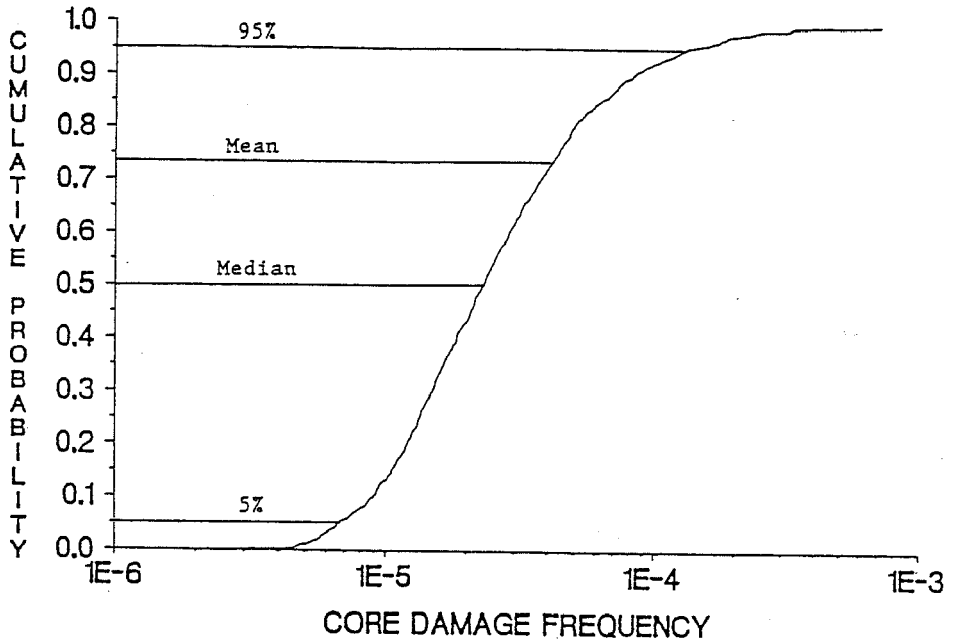


Fig. 1

Probability distribution of the expected frequency of core damage at the plant Surry (from/5/)

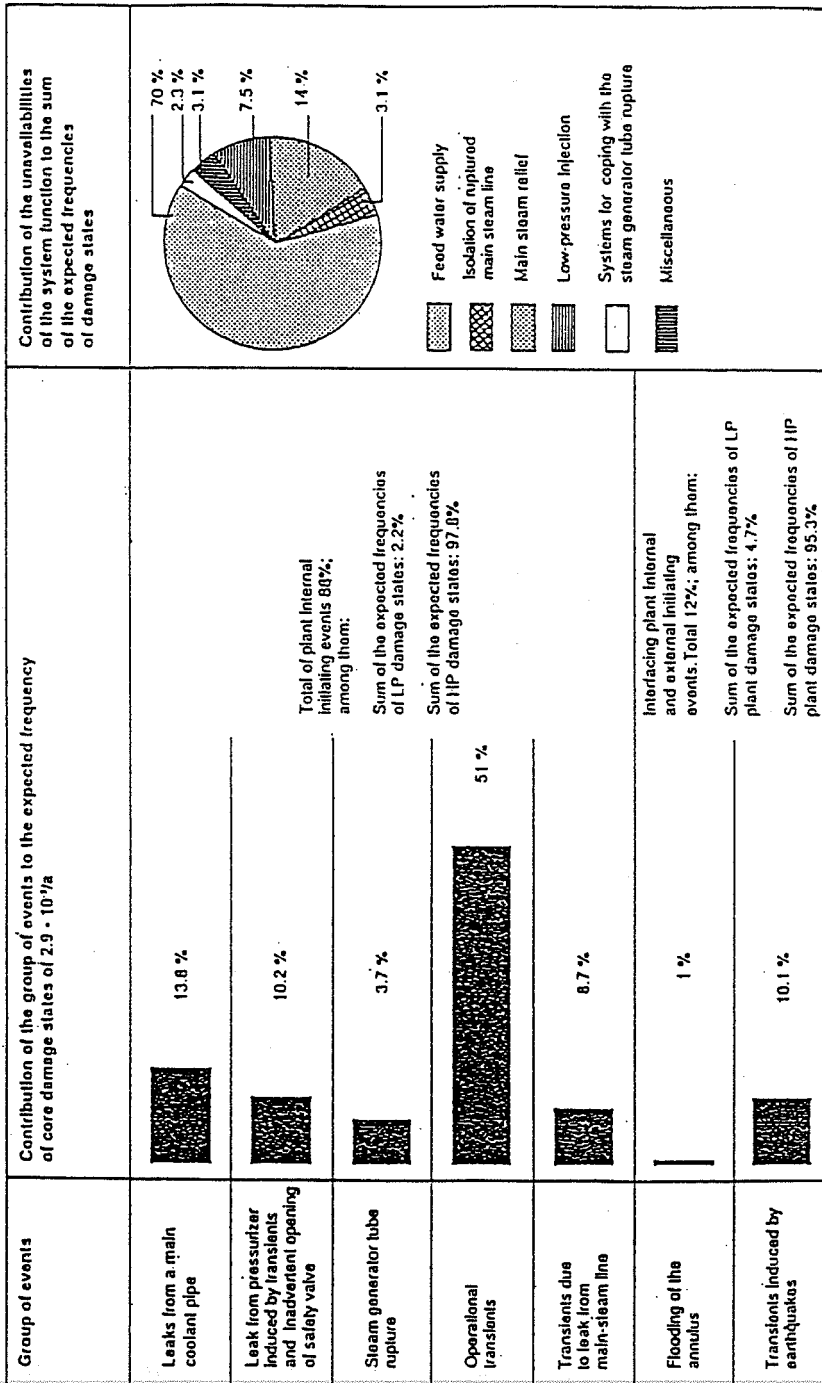


Fig.2

Contributions of the principal accident sequences to the frequency of hazard states (DRS-B)

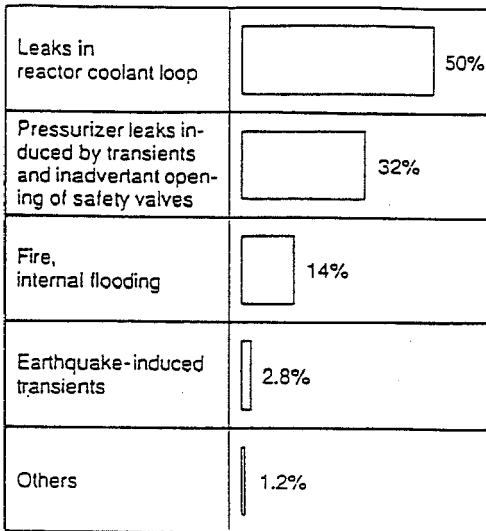


Fig. 3.1

Contributions of the principal accident sequences to the frequency of core damage at low pressure (DRS-B)

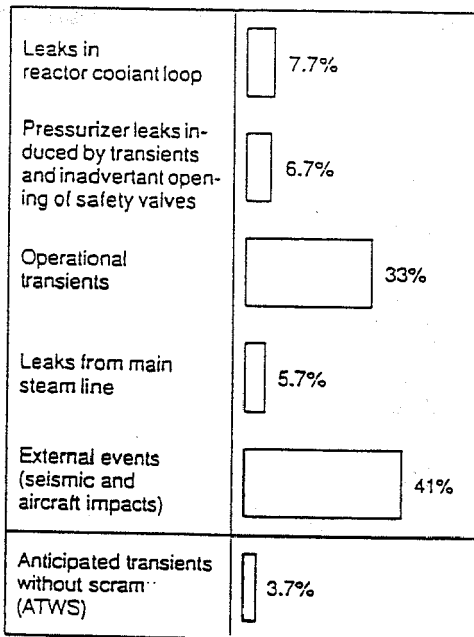


Fig. 3.2

Contributions of the principal accident sequences to the frequency of core damage at high pressure (DRS-B)

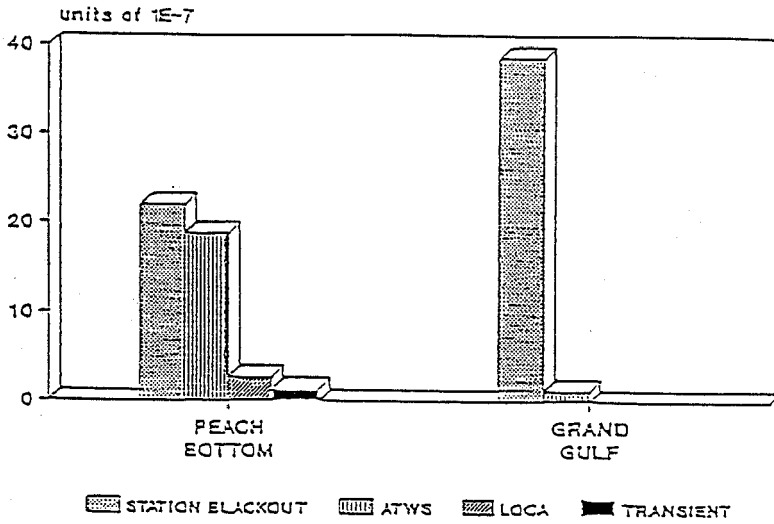


Fig. 4.1

BWR principal contributors to core damage frequency (NUREG-1150)

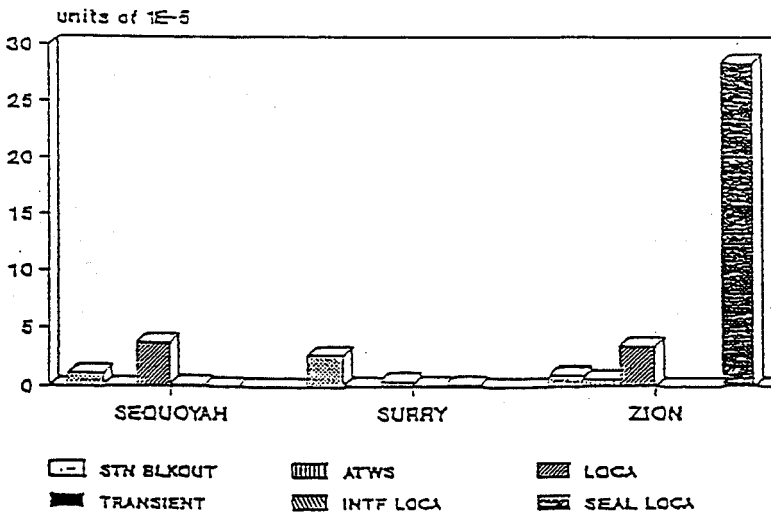
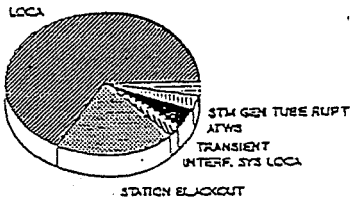


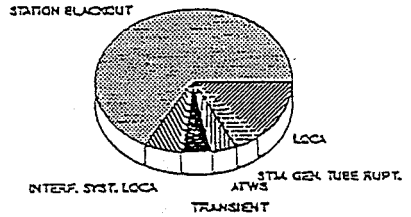
Fig. 4.2

PWR principal contributors to core damage frequency (NUREG-1150)

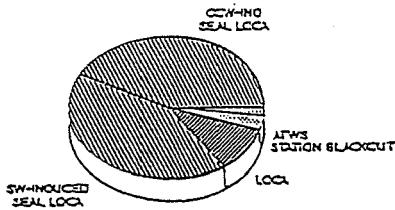
SEQUOYAH



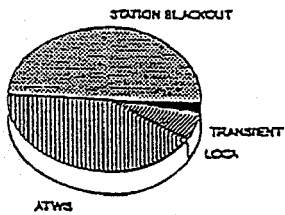
SURRY



ZION



PEACH BOTTOM



GRAND GULF

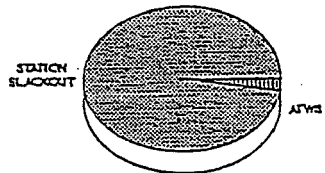


Fig. 4.3

Principal contributors to core damage frequency (NUREG-1150)

PROBABILITY OF CORE MELTDOWN

Contribution of families

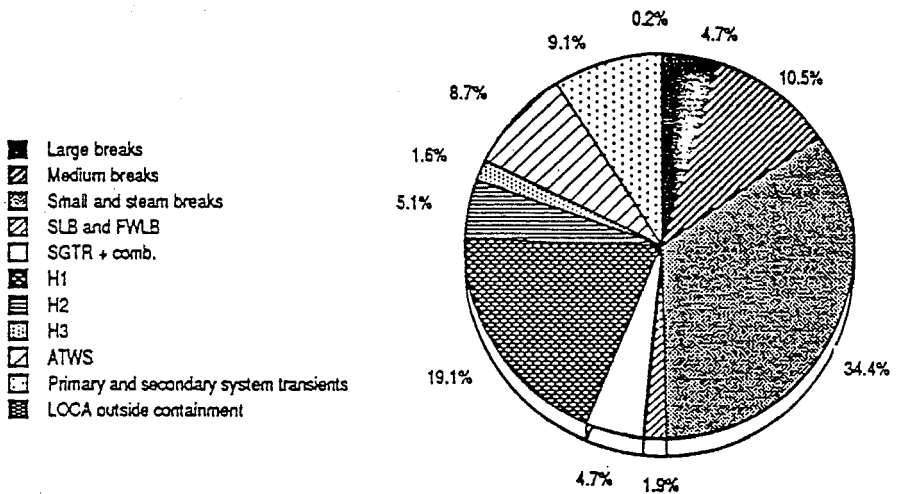
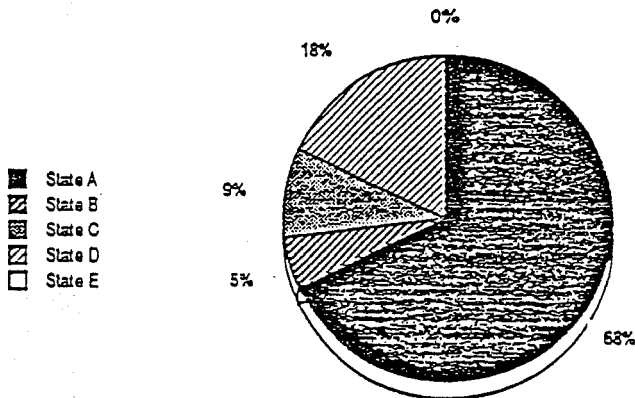


Fig. 5.1

Contributions of the principal accident sequences to the frequency of core damage (EPS 900)

PROBABILITY OF CORE MELTDOWN

Contribution of States



STATE	DESCRIPTION
A	Operating point (pressure and temperature) above (P11/P12) (139 bar, 284°C), corresponding to standard reactor states: <ul style="list-style-type: none"> • reactor under power with generator on-line or not, • reactor in hot shutdown, • upper part of intermediate shutdown range.
B	Operating point (temperature and pressure) between (P11/P12) and RHRS conditions (30 bar, 177°C)
C	Shutdown on RHRS, primary system full; closed and vented.
D	Primary system partially drained or open. To ensure conservativeness; all state D conditions are equated with the half-full condition for which the primary coolant mass is minimal.
E	Reactor cavity full with at least one fuel element in the reactor vessel.
F	Any primary system state in which the fuel is completely unloaded. This state only relates to the probabilistic safety assessment due to the fact it is not taken into consideration; it corresponds to hydraulic tests and containment tests, operations with loops empty and all other work necessitating complete defuelling (reactor vessel inspection, work on lower internals etc.)

Fig. 5.2

Definition of plant states and their contributions to the frequency of core damage (EPS 900)

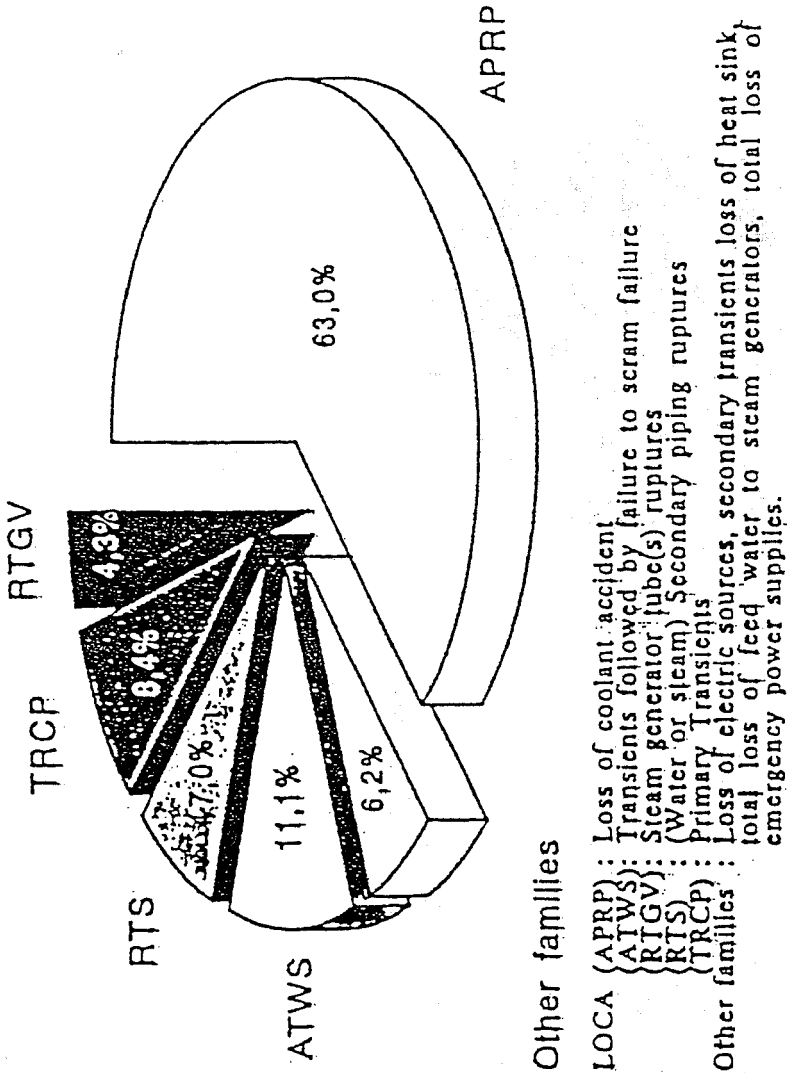
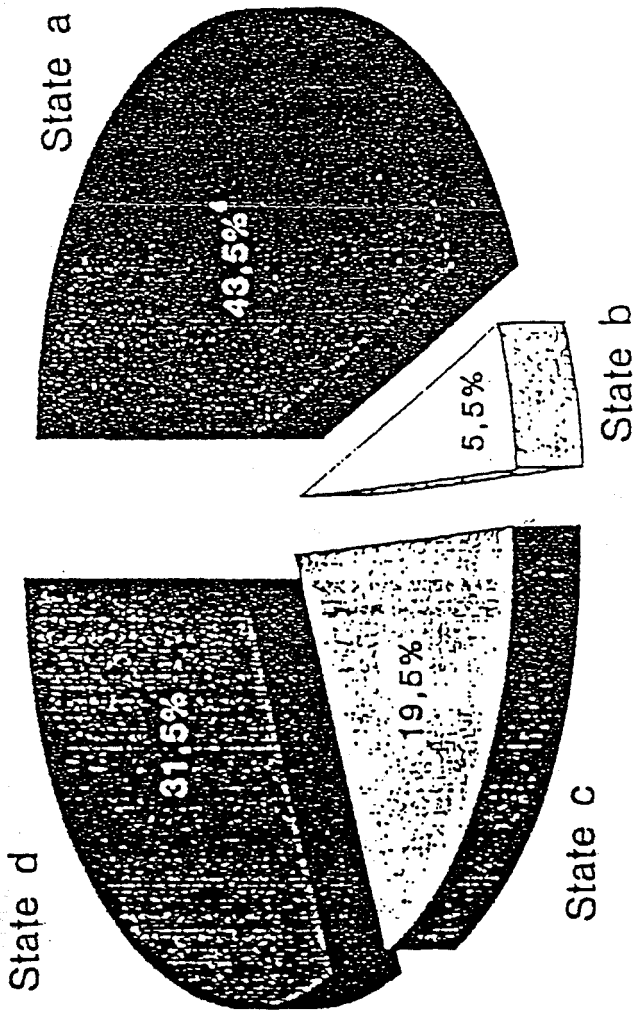


Fig. 6.1

Contributions of the principal accident sequences to the frequencies of core damage (EPS 1300)



States

- State a: Power operation, hot standby, hot shutdown,
- State b: Between state a and state where RHRS is valved in,
- State c: RHRS valved in, primary system full and vented,
- State d: RHRS valved in, primary system open.

Fig. 6.2

Definitions of plant states and their contributions to the frequency of core damage (EPS 1300)

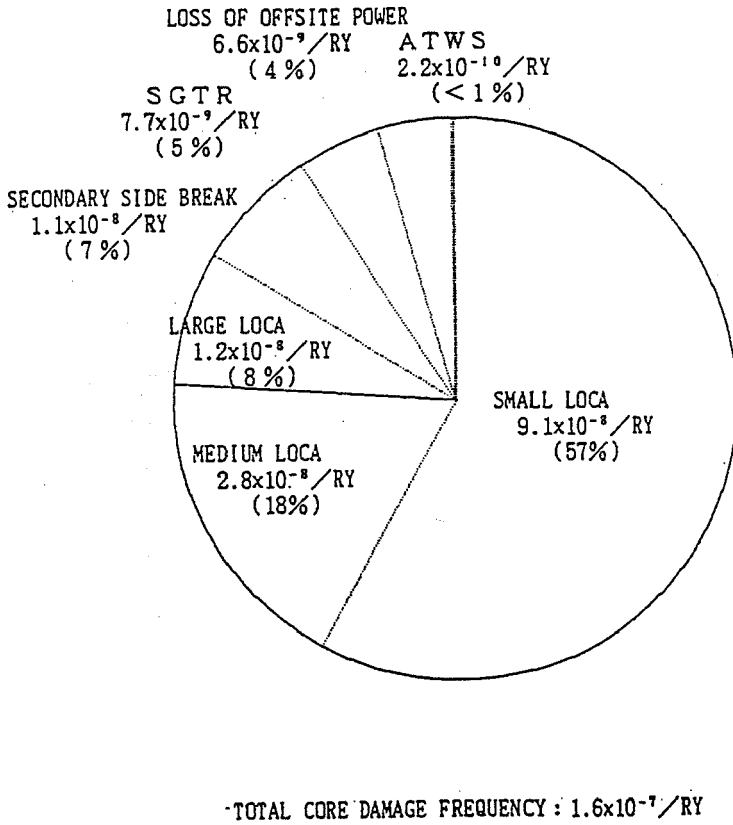


Fig. 7

Contributions of the principal accident sequences to the frequency of core damage for Japanese 1100 MWe PWR

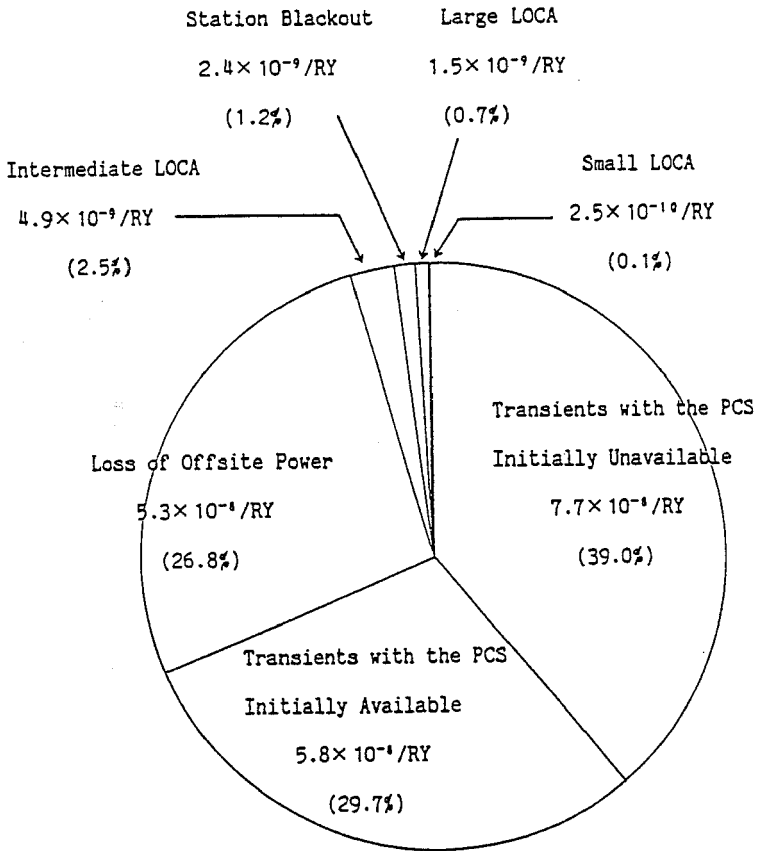


Fig. 8

Contributions of the principal accident sequences to the frequency of core damage for Japanese 1100 BWR

● mean value

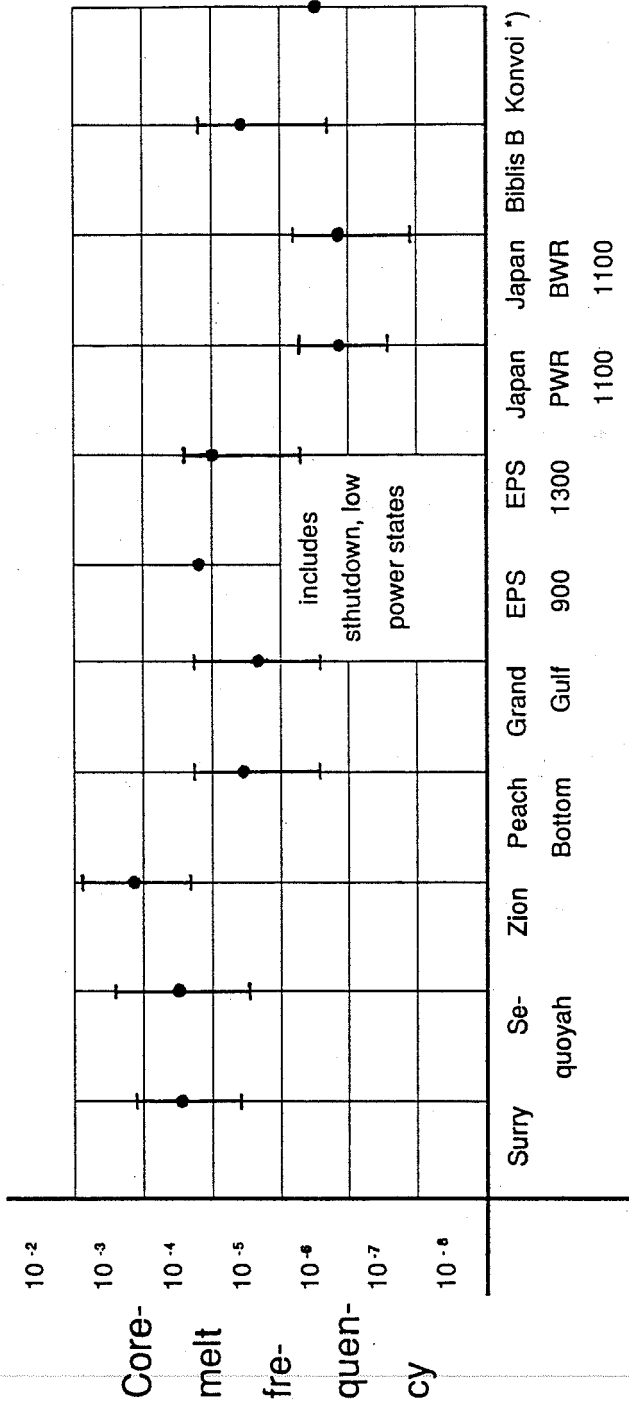


Fig. 9

Core damage frequencies with the lower 5 % and upper 95 % quantiles for 11 recent studies

Analysis of Dependencies

Chairman: U. Hauptmanns

U. Hauptmanns

Gesellschaft für Reaktorsicherheit (GRS) mbH

Cologne, FRG

ISSUE PAPER on Dependent Failure

Dependent failures are a major concern in the safety analysis of nuclear power stations because they thwart the benefits accruing from redundant design by leading to the simultaneous unavailability of more than one of the redundant trains of a system.

Three classes of dependent failures are generally distinguished: functional dependencies, secondary or consequential failures, and common cause failures. The first two classes are modelled directly in the fault trees. Their probabilities of occurrence are obtained as follows:

- functional dependencies (e.g. dependency on a common electricity or instrument air supply): from the usual reliability data for independent failures
- consequential failures (e.g. rupture of a steam line due to impact from an adjacent steam line): corresponding physical or chemical models constitute the bases of the probability estimation

Both types of dependent failures can be treated satisfactorily.

This is, however, not the case for common cause failures, as explained below.

Common Cause failures are due to shared causes such as design, construction or maintenance errors (e.g. unsuitable lubricants in pump bearings). They generally make a major contribution to the unavailability of the systems destined to cope with an initiating event, for example, the German Risk Study Phase B /1/ indicates con-

tributions of up to 85 %. For the important sequence triggered by the initiating event "Failure of the main coolant pumps and failure of the main heat sink" it amounts to 76 %. In NUREG-1150 /2/ contributions between 15 % and 25 % have been found.

Before common cause failures can be introduced into a fault tree their probabilities of occurrence have to be estimated. This is usually done using parametric models to evaluate the data base on multiple failures in nuclear reactor systems.

The models generally in use are:

- Beta-factor model
- Alpha-factor model
- Multiple-Greek-Letter (MGL) model
- Binomial failure rate (BFR) model

These are discussed in detail in reference /3/.

The Beta-factor model was originally developed for systems with two redundancies; in the MGL model it is extended to systems with more redundancies. The Alpha-factor model is similar to the Beta-factor model.

All three models require that simultaneous failures of a number of up to the redundancies to be treated have been observed unless parameter estimation on the basis of a zero failure statistics is accepted (e.g. upper 95 % centiles).

Unfortunately the number of multiple failures observed is very small so that plant-specific evaluations of common cause failures must be regarded as impossible. At most, they may make a small contribution to a data base, which is otherwise drawn from general experience with nuclear power systems. This dearth of data and the resultant uncertainty of failure rates is in marked contrast with the aforementioned importance of common cause failures for many reactor systems. In addition, in general the number of observation of simultaneous failures is smaller the higher the number of redundancies affected. It is for this reason that the BFR model is usually preferred when highly redundant systems are to be treated. It allows one to consi-

stently extrapolate from the observed failures of fewer redundancies for calculating the failure rate of a greater number of redundancies, if the assumption of an underlying binomial distribution is accepted. However, it is claimed that the pooling of several observed common cause failures to calculate the failure probability parameter, p , may lead to over or underestimation of the failure rates of higher redundancies.

No matter which model is used for data interpretation, the essential task in common cause analysis is the acquisition of the required failure data. These must be retrieved from records on abnormal occurrences and collections of reliability data.

In this process a considerable amount of engineering judgement has to be exercised. In order to progress in the field, international co-operation is an imperative because data from all nuclear power stations should be available for review when common cause failure rates are prepared for a PSA study.

In view of the foregoing exposition the following issues are considered worthy of discussion:

- which data bases on abnormal occurrences and reliability data are available in the different countries and do they satisfy the common cause information requirements (cf. /4/)?
- what aspects should be taken into account in judging occurrences of observed failures as common cause?
- should single failures be included in common cause analysis?
(this would increase the number of occurrences available for parameter estimation, but require more engineering judgement as an input)
- what are the criteria to be used for considering NPP systems as comparable for the purposes of common cause analysis?
- what direction should further model development take?

REFERENCES

- /1/ Deutsche Risikostudie Kernkraftwerke, Phase B
Köln 1990 (English Summary: German risk study nuclear power plants,
phase B.
GRS-74, Köln 1990)**

- /2/ Severe accident risks: An assessment for five US nuclear power plants.
Summary report-second draft for peer review.
Vols. 1 and 2.
NUREG-1150, June 1989**

- /3/ Mosleh, A. et al.:
Procedure for Treating Common Cause Failures in Safety and Reliability
Studies.
Final Report NUREG/CR - 4870, Vol. 1 (February 1988), Vol. 2 (Decem-
ber 1988),**

- /4/ Parry, G.W. et al.:
Data Needs for Common Cause Failure Analysis in:
G. Apostolakis (Ed.):
Probabilistic Safety Assessment and Management, Vol. 2.
New York, Amsterdam, London 1991**

This paper has been prepared for the
CSNI Workshop on Special Issues of Level-1 PSA
(Cologne, 27-29 May, 1991)

WHY IS THE MARKOV METHOD NOT USED AS A STANDARD TECHNIQUE IN PSA?

Enrico Silvestri
Ansaldo SpA, Nuclear Division, Genoa (Italy)

ABSTRACT

The Markov method is one of the most well-known and most widely applied techniques for modelling and quantifying a variety of problems of stochastic nature. This method, owing to its great flexibility and versatility, performs successfully in the diverse domains of system modelling and reliability/availability quantification, easily including common cause failure aspects, of test/maintenance optimization studies, of stochastic modelling of many physical processes, also including operator actions. Contrasting with this versatility is the relatively limited favour that the method finds in PSA applications.

This paper aims at identifying the uses, the perspective applications, the limitations of the method in the context of PSA. In particular, it reviews its current applications in PSA, and discusses its perspectives in the various subdomains of PSA, like Markov vs. fault trees in system analysis and Markov vs. event trees in event sequence quantification, in both of which it is deemed that combined use of Markov and fault trees or event trees, respectively, would produce more effective (and also more efficient) modelling; or the capability of the method to deal with special topics, f.i., human reliability analysis and modelling of certain time-dependent phenomena. Finally, the paper attempts at defining under what specifications can the Markov method be made a standard guideline in PSA.

INTRODUCTION

In the course of some years of practice in probabilistic analysis the specialist has the opportunity to appreciate the versatility and flexibility of the Markov method to model and solve the most diverse stochastic problems. The method itself is normally the next step in reliability engineering apprenticeship after the most elementary models that produce the standard text probability distributions. This contrasts with the observation that only rarely does one come across

examples of the application of the method in PSA, as results from consulting also recent literature on the subject. This brief note is intended only as a digression to raise some questions related to the relatively scarce use that is made of the Markov model.

The event tree/ fault tree approach has become the established framework within which PSA is structured, owing to its numerous advantages, among which:

- logical simplicity; ease of applications by non-experts with limited training;
- ability to model systems of high complexity in a manageable way;
- good degree of standardization, traceability and verifiability.

This approach, however, has two basic limitations that are relevant to PSA, namely:

- the basic events must be essentially independent;
- time factors cannot be explicitly modelled or parametrized.

It is precisely when dependences or stochastic dynamics are important in the analysis that the Markov method may represent a valid alternative to more conventional methods.

One briefly recalls the assumptions on which the method is based.

1) The system to be modelled can be decomposed into elements ("components"), each one being characterized by a finite number of discrete "states" the element can experience by undergoing "state transitions".

2) The combinations of all possible states of all system elements determine the ensemble of system states in an unambiguous way; the possible element state transitions define as many system state transitions. The collection of all system states and the transitions the system can experience are a "stochastic process", which is Markovian by virtue of items 4) and 5) below.

3) the "transition rates" are the conditional probabilities of transition per unit time, given that the system has reached the state from which the transition depends, at a given time.

4) the "transition rates" between any two connected states depend only on the two states themselves and on time computed from the beginning of the process. It is not a requirement for a system to be Markovian that the transition rates between its states be constants, as is often held. If they do not depend on time, then the process that the system undergoes is termed time-homogeneous.

5) The probabilities of multiple transitions in a time increment tend to zero as the time increment is made to tend to zero.

Mathematically, the stochastic evolution of the system in time is described by a set of linear differential equations whose solution is the vector of state probabilities.

The applicability of the model, given its characteristics, must be carefully checked against the real situation to which it is adapted. Typically, a process for which the transition rates do depend in any way on the previously visited states is not Markovian. As an example, consider a system made up of components whose rates of existence in the "up"- and "down"-state are constants. This is a typical Markovian system. The implication of the model is that each time a failed component is restored to the nonfailed condition, its failure characteristics are returned to the initial condition. If this was not the case for certain components, then the failure rates for these would depend on the number of failure/repair cycles, and consequently, the transition from the states describing the failure of these particular components would depend on which and how many other states have been visited before the state for which the transition is considered. Another example is given by the same system as above when the component restoration times are not exponentially distributed. In this case, the Markov approximation may be kept for system unavailability quantification, because the fraction of time each component spends being repaired is small with respect to its "up" state. In any case, an adequate state space representation can in principle provide as good an approximation through a Markov model as is required (see, f. i., refs. 1 and 2).

WHICH TYPES OF PROBLEMS CAN BE MANAGED BY MEANS OF MARKOV MODELLING AND HOW THEY STAND WITH RESPECT TO PSA

Basically, the versatility of the Markov method is related to the fact that the representation is indifferent to the presence of dependent events. All

forms of dependences can be accounted for by defining the appropriate state space and transitions.

Typical dependence problems that appear in system analysis are:

- standby components in redundant systems;
- maintenance/repair dependences caused by personnel unavailability for multiple parallel repairs;
- test interval/maintenance strategy/ repair procedures interactions to determine system unavailability;
- common cause failures.

By definition, only the last type of dependence can be treated adequately in the fault tree framework. Even in this case, certain situations where common cause failures do not manifest themselves in coincidence of time, this conservative assumption must be made.

As to maintenance crew type of dependence, it can be verified that if the repair rate is at least one order of magnitude greater than the failure rate of the components in a cutset, then the error in the unavailability is also small. For example, in the case of two redundant parallel components with $\mu > 30\lambda$, the error made in the assumption of independent repair is only -3.2% (in the nonconservative sense). The error increases dramatically, however, if the cutset order increases. This means that significant errors may be made in the unavailability evaluation of highly redundant systems (this is also the typical problem with common cause failures in the same type of systems).

Test/maintenance schemes cannot at all be quantified correctly with fault trees, as any event in the process is conditioned to the outcome of another. The Markov method can accommodate this case also.

Another case when a different approach from fault tree is necessary in system unavailability/unreliability evaluation is when operating (process) systems with standby redundancies and recovery/repair are possible with the system in operation. In such case, dependences exist through the standby/operate interaction and through the recovery processes. Again, as already said, this is a case where the Markov approach is required. In PSA this situation is found basically in two cases:

- unavailability of (continuously operated) support systems;

- frequency of failure of continuously operated systems that determine certain initiating events.

The first case is of particular relevance to PSA, as is pointed out in ref. 3.

The Markov method can model the stochastic behaviour of other systems than than engineered systems made of physical equipment; it serves to model also certain physical processes. Of particular interest are the applications to operator/system interactions modelling. An interesting application can be found as an extension of the Human Cognitive Reliability (HCR) model in ref. 4. In this application, very much in the spirit of ref. 2, where the method is applied in an entirely different context, the distribution of operator time to act is modelled as a discrete-state transition model, where each state represents an elementary step in the process of human action. The idea is that such steps are defined in a way that allows to obtain reliability data from relatively simple experiments. A complete system analysis including human errors is developed with the Markov method in ref. 5.

Of particular relevance to PSA is the problem of quantifying time-dependent accident sequences. The event tree methodology has remained essentially unchanged from its initial applications (e. g., WASH-1400); for each initiating event the safety systems that need be operated to perform the appropriate functions to mitigate the consequences of the events are identified and used as headings in the event tree. The various combinations of the states of the systems define the event sequences generated by the initiating event. The sequence frequency quantification process is done by multiplying the frequency of the initiating event by system unavailabilities, usually calculated using fault tree methodology. In this way, system failure and recovery, or operator actions changing the course of the events cannot be readily factored in; but it must be recognized that in major incidents like TMI or Chernobyl this is exactly what happened, so it cannot be concluded that these contributing factors are of minor importance in determining core damage frequency. Several authors have pointed out this fact, all basically arriving at the conclusion that a state space approach with, in general, nonlinear transitions best represents the accident sequence stochastic timing. At the same time, semi-markovian or Markovian approximations can represent acceptable solutions to take account of dynamic factors in event sequences. One wants to mention ref. 6 for an application to accident sequences with human

intervention, ref. 7 for an application to the quantification of the accident sequence of core uncover caused by the protracted loss of Offsite and Onsite Power event, and refs. 8, 9 and 10 for more general considerations and methodological approaches.

In a similar way, although in a different application, the Markov approach is being referred to for fire growth/ fire suppression process modelling in the fire risk analysis context (e. g., ref 11).

DISCUSSION AND FINAL REMARKS

The Markov modelling technique applied to reliability analysis is an effective tool, whenever the stochastic behaviour of a system is affected by dependent behaviour in its constituting elements.

What in effect represents an obstacle in its generalized use in PSA is then to be found in the algorithmic difficulties it presents.

Needless to say, a detailed decomposition of a system in its components causes an exponential growth in the number of system states, with the associated computing difficulties in solving the stochastic equations. The normal strategy is then to reduce the system to a limited number of aggregate parts, or "supercomponents", characterized by failure and restoration rates. This can be accomplished by a more detailed analysis of the aggregate parts. Several systematic reduction techniques allow to deal with relatively large Markov systems (see, f. i., ref. 12).

It must be conceded that application of such reduction strategies requires a very thorough understanding of system behaviour and deep knowledge and experience in the technique of Markov method. Thus it is not an easy task for system analysts, also considering that usually they are introduced to fault tree analysis without much basis or experience in formulating and in modelling problems of a stochastic nature.

As a starting point, referring to the fault tree/ event tree matrix structure of today PSA, one suggestion is to introduce the use of Markov methodology at the "bottom level" and at the "top level" of the conceptual fault tree that describes an event sequence. This means that The method could be used in an integrated structure with fault tree, both to deal with subsystems or component aggregates at the detail level where certain types of dependences exist like those described in the previous section, and at the system top event level in the event

sequence quantification, where the physically possible combinations of system top level states represent plant states in a (semi)Markov formulation.

The first step, in particular, should not present unsurmountable obstacles, to integrate Markov modules along with elementary event descriptions in a fault tree structure. This step would allow more precise modelling and quantification of support system unavailabilities and failure rates.

The fault tree/ event tree framework represents a very powerful reference in PSA, and presents undoubtable advantages in its simplicity, which is an asset when considering the complex reality of a nuclear power plant that must be modelled in PSA. It is also true that certain "grey areas" exist in PSA, because of the inability of this framework to deal with certain specific problems. But it is argued that these problem areas are of no minor importance in today and future PSA.

Thus it is argued that the limited, non-standard use of the Markov method does not represent its inability to treat adequately certain specific problems. Rather, it represents the inability to move from procedures that have become tradition by now.

It is not claimed that the use of Markov methods may represent the panacea to all headaches in PSA, however it is held that thinking in terms of this approach in PSA would produce new ideas beneficial to the effect of finding acceptable solutions in areas as those described above, even if the algorithm-generating ability of the method is still really to be tested for PSA.

REFERENCES

1. D. R. Cox, "The Analysis of Non-Markovian Stochastic Processes by the Inclusion of Supplementary Variables", Camb. Philos. 51,3 (1955), p. 433.
2. C. Singh, R. Billinton, "Reliability Modelling with Non-exponential Downtime Distributions", IEEE PES Summer Meeting, San Francisco, Ca., July 1972.
3. J. H. Bickel, "Impact of Support System Failure Limitations on PSA and Regulatory Decision Making", CNSI Workshop at Santa Fe (New Mexico), 1990.

4. Y. D. Lukic, D. H. Worledge, G. W. Hannamah, A. J. Spurgin, "Modeling Framework for Crew Decisions During Accident Sequences", Advances in Human Factors in Nuclear Power Systems, Knoxville, Tennessee, April 1986.
5. B. S. Dhillon, S. N. Rayapati, "Modeling of Redundant Systems with Human Errors", *ibid.* .
6. G. Apostolakis, T. L. Chu, "Time-dependent Accident sequences Including Human Actions", Nucl. Tech. (64), Feb. 1984, p. 115.
7. E. Silvestri, S. Serra, D. F. Paddleford, "A Model for the Probability of Core Uncovery in LOOSP Induced Accidents, As Applied in the PSS for ENEL PWR Standard Power Plant", ANS/ ENS Int. Topical Meeting on Probabilistic Safety Methods and Applications, San Francisco, Calif., Feb. 1985.
8. A. Villemeur, M. Bouissou, A. Dubreuil-chambardel, "Accident Sequences: Methods to Compute Probabilities", ENS/ ANS/ SNS Int. Topical Meeting on PSA and Risk Management, Zurich, Aug.-Sept. 1987.
9. A. Amendola, "Accident Sequence Dynamic Simulation Versus Event Trees", Reliability Engineering and System Safety 22 (1988), p. 3.
10. D. C. Bley, D. R. Buttmer, J. W. Stetkar, "Light Water Reactor Sequence Timing: Its Significance to PSA Modeling", *ibid.*, p. 27.
11. N. Siu, G. Apostolakis, "Modeling the Detection and Suppression of Fires in Nuclear Power Plants", ANS/ ENS Int. Topical Meeting on Probabilistic Safety Methods and Applications, San Francisco, Calif., Feb. 1985.
12. J. Cantarella, J. Devooght, C. Smidts, "Methodological Progress in Markovian Availability Analysis and Applications", ENS/ ANS/ SNS Int. Topical Meeting on Probabilistic Safety Assessment and Risk Management, Zurich, Aug.-Sept. 1987.

**OECD/CSNI WORKSHOP ON SPEZIAL
ISSUES OF LEVEL-1 PSA**

Cologne, Germany
27th-29th May 1991

K. Lützow, C. Fuhrmann

The conditional applicability of the β -Factor-Method for structural redundancies

Abstract

The β -Factor-Method allows to model Common Causes Failures in fault trees in a relatively simple way.

The β -Factor-Method is based on the simplified assumption that the occurrence of an CCF-Event leads directly to the failure of all components of the system.

In general they think to be in the "sure region" with this assumption.

But that's not true in each case.

The following Benchmark-Exercise shall verify the statement that the application of the β -Factor-Method for structural redundancies may lead to an undervaluation of the failure probability.

Above all this concerns systems in which the failure of two components already leads to the system failure or a hazardous situation.

The structural importance of the Double-Failure as a minimal cut of first order is very high because of its high number.

And so it delivers a great contribution to the failure probability of the system notwithstanding its small frequency of occurrence.

If such systems are treated with the β -Factor-Method now the frequency of the Double-Failure will be added to the frequency of the complete failure of the system (lethal shock) the structural importance of which is not so high because it only occurs solely.

This case leads to an undervaluation of the failure probability of the system.

1.Introduction

Common causes failures require special treatment within reliability analysis /1/, /2/.

Therefore the simplest procedure is the β -Factor-Method. The basic assumption of the β -Factor-Method is that a fixed percentage of all failures occurring are dependent failures.

This percentage (in general about 10 %) is represented by the β -Factor. Furthermore it is assumed that the occurrence of one CCF-Event leads directly to the failure of all components of the system.

Moreover this simplification should make the procedure especially safe, i.e. it should avoid an undervaluation of the failure probability of the system in each case.

The aim of this script is to demonstrate, that the application of the β -Factor-Method, however, may lead to an undervaluation of the failure probability of the system /4/.

In the following chapters the reliability of a fictive sample system of four identical components will be evaluated for all possible redundancy structures /3/ (1,2,3,4 of 4-systems).

By means of a definition of exact "system specific data" it is possible to estimate directly the primary data of the fault tree of the system (Basic-Parameter-Model).

This failure probability of the system determined in such a way will be postulated as the so called "true value". Then the failure probability of the system will be estimated by means of the simplifications necessary for the β -Factor-Method.

The absolute and relative deviations from the "true value" of the results are shown in chapter 4.1..

By means of the minimal cut sets the structures of the single systems are broken down and the deviations are motivated.

In chapter 5.0. the influence of data on the results is shown.

Finally it's possible to derive common conclusions for the modelling of CCF's.

2.Sample fault trees

The sample system consists of four components, in the following called A, B, C and D for convenience. (fig.1)

For example the components may be pumps and

at the 1 of 4-system each pump should have 25% of power

"	2 of 4-system	"-"	33%	"
---	---------------	-----	-----	---

"	3 of 4-system	"-"	50%	"
---	---------------	-----	-----	---

"	4 of 4-system	"-"	100%	"
---	---------------	-----	------	---

Here the k of n-systems refers to the failure of the system.

The Boolean Variables corresponding to the components are named:

X_A , X_B , X_C and X_D .

Eleven further Boolean variables representing the possibilities of the corresponding failures due to common causes are necessary for the complete modelling of CCF /1/.(fig.2)

With the β -Factor-Method only the complete failure of all components (X_{ABCD}) will be modelled.

The fault tree reduces itself as follows.(fig.3)

3. Used data

The fictive circumstances are: exactly 500 failures (N_a) occurred at one component at 100,000 demands (N).

50 (10%) of these 500 failures were dependent failures (N_c). These dependent failures are divided into 15 Double-Failures (N_{c2}), 5 Triple-Failures (N_{c3}) and 30 Quadruple-Failures (N_{c4}). Thus it is possible to determine the following characteristics:

Q_t - total failure probability of the component

$$Q_t = N_a/N = 5.0 \cdot 10^{-3}$$

Q_u - independent failure probability of the component

$$Q_u = (N_a - N_c)/N = 4.5 \cdot 10^{-3}$$

Q_c - probability of the occurrence of a CCF

$$Q_c = N_c/N = 5.0 \cdot 10^{-4}$$

β - portion of the dependent failures (β -Factor)

$$\beta = N_c/N_a = Q_c/Q_t = 10\%$$

Q_{1g} - probability of the occurrence of a Single-Failure

$$Q_{1g} = Q_u = 4.5 \cdot 10^{-3}$$

Q_{2g} - probability of the occurrence of a Double-Failure

$$Q_{2g} = N_{c2}/N = 1.5 \cdot 10^{-4}$$

Q_{3g} - probability of the occurrence of a Triple-Failure

$$Q_{3g} = N_{c3}/N = 5.0 \cdot 10^{-5}$$

Q_{4g} - probability of the occurrence of a Quadruple-Failure

$$Q_{4g} = N_{c4}/N = 3.0 \cdot 10^{-4}$$

It is necessary to investigate the following probabilities (P) for the complete modelling of all components in the fault tree (fig.2).

Therefore all components are assumed to have the same failure mode.

$$Q_1 = P(X_A) = P(X_B) = P(X_C) = P(X_D)$$

$$Q_1 = Q_{1g} = Q_u = 4.5 \cdot 10^{-3}$$

$$Q_2 = P(X_{AB}) = P(X_{AC}) = P(X_{AD}) = P(X_{BC}) = P(X_{BD}) = P(X_{CD})$$

$$Q_2 = 1/3 \cdot Q_{2g} = 5.0 \cdot 10^{-5}$$

$$Q_3 = P(X_{ABD}) = P(X_{ACD}) = P(X_{BCD})$$

$$Q_3 = 1/3 \cdot Q_{3g} = 1.67 \cdot 10^{-5}$$

$$Q_4 = Q_{4g} = 3.0 \cdot 10^{-4}$$

The following simplification will be used for the modelling by means of β -Factor-Method (fig.3):

All occurring CCF's lead directly to the failure of all four components in each case:

$$\text{Therefore: } N_{c2} + N_{c3} + N_{c4} = N_c$$

or

$$Q_c = N_c/N = \beta \cdot Q_t = 5.0 \cdot 10^{-4}$$

$$P(X_{ABCD}) = Q_c$$

4. Results

4.1. Interpretation of the calculation results.

The following table 1 shows the results of the calculations carried out.

Column 1:	System structure
Column 2:	Q_s - Failure probability of the system without inclusion of CCF's
Column 3:	Q_{sc} - Failure probability of the system with inclusion of CCF's (true value)
Column 4:	$Q_{s\beta}$ - Failure probability of the system by means of the β -Factor-Method
Column 5:	A_a - absolute deviation from the "true value" $A_a = Q_{s\beta} - Q_{sc}$
Column 6:	A_r - relative deviation $A_r = (Q_{s\beta} - Q_{sc}) / Q_{sc}$

To the 1 of 4-system:

It is not usual to include series systems into CCF considerations. It was done here only for completeness.

It becomes apparent, that the results of both methods don't differ very much from each other. That, among other things, is connected with the high failure probability of the series system itself.

A comparison with the failure probability of the system without inclusion of CCF's shows, that they are even in the "sure region" if CCF events are not modelled at series systems at all.

To the 2 of 4-system:

At this system the application of the β -Factor-Method unambiguously leads to an undervaluation of the failure probability of the system.

The relative deviation from >20% into the negative region is very important.

It will be demonstrated in the following chapter what this deviation is due to.

But at present it can simply be stated as wrong to apply the β -Factor-Method to such systems.

To the 3 of 4-system and 4 of 4-system:

At this system structures the β -Factor-Method involves an overvaluation of the failure probability of the system.

Indeed the deviations from the "true value" are considerable.

At a deviation of about 70% (4 of 4-system) one has to consider how "safe this region should be" to be regarded as useful. Finally it is possible to say, that the simple application of the

β -Factor-Method is unsuitable (for this system of four components) resp. it even leads to the "forbidden" region (fig.4) at a 2 of 4-structure.

The reason for that and possibilities to carry out simplifications which guarantee sufficiently exact results will be demonstrated in the following chapter.

4.2. Structural analysis

Now the minimal cut sets of the single redundancy structures will be broken down with respect to kind, order and probability of occurrence and this will be compared with the minimal cut sets estimated under the conditions of the application of the β -Factor-Method.

That makes it possible to find out the causes of the deviations from the true value with regard to the results of the β -Factor-Method.

The following abbreviations will be used:

n - number of the minimal cuts of the group

O - order of the minimal cuts of the group

W - occurrence probability of the minimal cuts of the group

W% - percentage of the minimal cut sets of the group within the complete failure probability of the system

A - kind of the CCF, i.e. Double (Z)-, Triple (D)- or Quadruple (V)-CCF

E - single failure

To the 1 of 4-system:

The tables 2 and 3 show, that the difference of the results of these two methods is small because almost nothing but the independent failures affect the failure probability of the system.

To the 2 of 4-system:

This system structure (tables 4 and 5) shows an enormous importance (about 40%) of the double failures which make them equivalent to the Quadruple-Failures.

The Triple-Failures make a considerable contribution (with nearly 10%) to the complete failure probability of the system too.

The Quadruple-Failure with its probability of occurrence of 3.0×10^{-4} (about 40%) is not so important as at the β -Factor-Method (5.0×10^{-4} resp. 80%).

However the accumulated number of the probabilities of all CCF's is much higher and this makes clear, that the simplifications of the β -Factor-Method are unpermissible here.

To the 3 of 4-system:

Here the Triple- and the Quadruple-Failures (tables 6 and 7) have the main share of the failure probability of the system.

All other combinations can be neglected.

However, the importance of the combination Double-Failure/Independent-Failure (Z/E) may increase if the primary data are different.

rent. The accumulated number of the CCF-Minimal-Cuts doesn't reach the value of the complete failure if the β -Factor-Method is used.

The permissibility of the overvaluation of the failure probability with regard to the β -Factor-Method can be discussed.

To the 4 of 4-system:

Regarding this "clear redundancy" (tables 8 and 9) only the complete failure is important of course.

The combination Triple-Failure/Independent-Failure (D/E) may make a very small contribution if the primary data are different.

The β -Factor-Method leads to an enormous overvaluation of the failure probability of the system because it assumes the probability of occurrence of the complete failure with a much too high value.

The most important information of the tables 4-9 are shown graphically in figure 5 again.

5. Further regards

5.1. The variation of the total failure probability

The former calculations were carried on only for certain system structures and certain data.

Now it is important to recognize whether the given statements refer only to the calculated results or are matters of principle. To appraise the influence of the data the primary data were varied.

Picture 6 shows the results if the total failure probability of the components (Q_t) increases to the tenfold ($Q_t = 5 \cdot 10^{-2}$) resp. decreases to one tenth ($Q_t = 5 \cdot 10^{-4}$) of the former value.

The percentage of the dependent failures remains constant in each case.

At the relatively high failure probability of the components ($Q_t = 5 \cdot 10^{-2}$) the deviations A_r from the "true value" of the results of the β -Factor-Method decrease since the independent failures or failure combinations increase in importance.

Strictly speaking, only the calculated importance of the independent failures increases, whereas the structural importance remains constant.

The decrease of Q_t has opposite consequences of course.

Here the difference between the results of the β -Factor-Method and the "true value" increases since the importance of the independent failures goes down.

5.2. The variation of the share of the Common-Causes-Failures in the total failure probability

Here the probabilities of occurrence of the CCF's remain constant.

At first the value of the independent failure probabilities was increased to the fivefold. Thus the value of the total failure

probability of the components also increases to $Q_t = 2.3 \cdot 10^{-2}$. The percentage of the CCF's decreases to $\beta = 2.2\%$. After that, the independent failure probability was reduced to one fifth and this corresponds to $\beta = 35.7\%$ and $Q_t = 1.4 \cdot 10^{-3}$. (fig. 7) It could be expected that the increase of the CCF share of the failure probability of the component (decrease of the independent part) also causes the increase of the deviations of the results of the two methods from each other, whereas the decrease of the CCF-percentage also decreases the deviations. But on principle the formerly given statements do not vary.

Another possibility to vary the data is to vary the relations between the single kinds of CCF's (Q_2, Q_3, Q_4). The result is foreseeable.

The more the probabilities of occurrence of the Double- and Triple-Failures increase in relation to the Quadruple (complete)-Failure the more the β -Factor-Method will deviate from reality.

Vice versa the applicability of the β -Factor-Method increases if the probability of occurrence of the Double- and Triple-Failures is low in relation to the complete failure.

6. Proposal for a simplification concerning the CCF modelling

The realizations of chapter 4 and 5 offer possible simplifications of the CCF-Modelling of k of n-systems.

Thus only those kinds of CCF which are important for the complete failure of the system have to be modelled.

That means that only the CCF kinds from k to n occur as basic events in the fault tree.

This essential simplification of the fault tree is obviously (fig. 8 and 9).

If the (k-1)-Failure has an unexpectedly high probability of occurrence it will also have to be modelled.

It forms minimal cuts of second order with the independent failures.

By multiplication of the occurrence probabilities of the (k-1)-Failure and the independent failure it is possible to appraise the influence of this minimal cuts.

7. Conclusions

The results of the calculations carried on have shown, that the β -Factor-Method is unsuitable for the modelling of CCF's at higher redundancies.

At redundancy structures in which small CCF-Combinations occur as minimal cuts of first order, the β -Factor-Method leads to an undervaluation of the failure probability of the system.

Redundancy structures of this kind resp. structures which due to system meshings and subsequent failure connections cannot be directly recognized, should be treated with multiple parameter models on principle.

At the CCF-Modelling of k of n-systems it is possible to make simplifications.

Only those CCF kinds which are important for the complete failure of the system have to be modelled.

That means, that only the kinds of CCF reaching from k to n occur as basic events in the fault tree which leads to an essential simplification of the fault tree.

REFERENCES

1. A. MOSLEH, K.M. FLEMING, G.W. PARRY, H.M. PAULA, D.M. WORLEDGE, D.M. RASMUSON, "Procedures for Treating Common Cause Failures in Safety and Reliability Studies", EPRI NP-5613, NUREG/CR-4780, Vol. 1, Electric Power Research Institute (1988).
2. N. McCORMICK, "Reliability and Risk Analysis", ACADEMIC PRESS (1981).
3. K. REINSCHKE, I.A. USAKOV, "Zuverlässigkeitsstrukturen", Verlag der Technik, Berlin (1987).
4. C. FUHRMANN, "Untersuchungen zum Einfluß von Common Cause Fehlern in PSA für WWER-440, Typ-213", Technische Hochschule Zittau (1990).

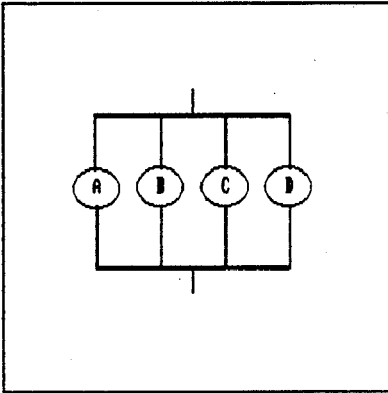


Figure 1
Sample system

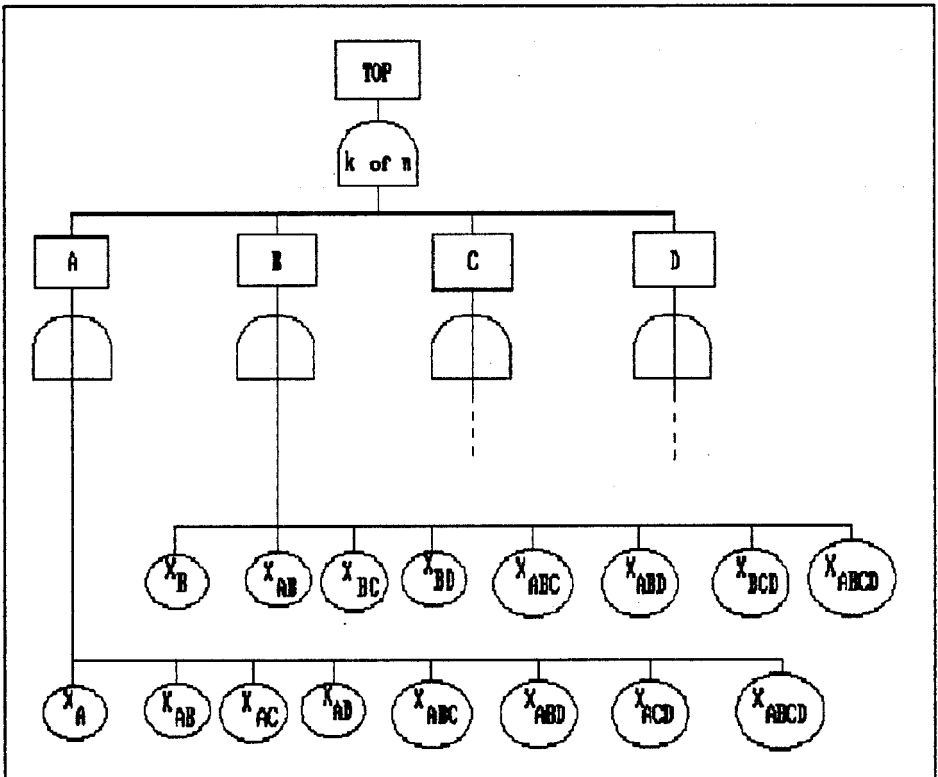


Figure 2.
Fault tree, complete modelling of CCF

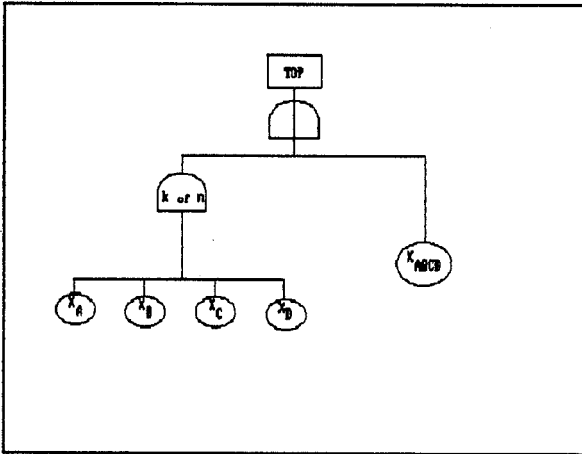


Figure 3.
Fault tree, modelling by means
of the β -Factor - Method

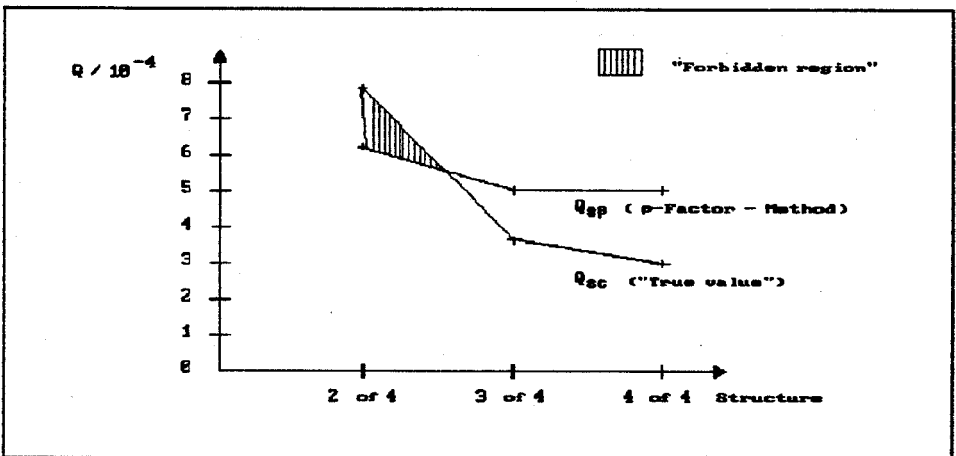


Figure 4.
"Forbidden" region

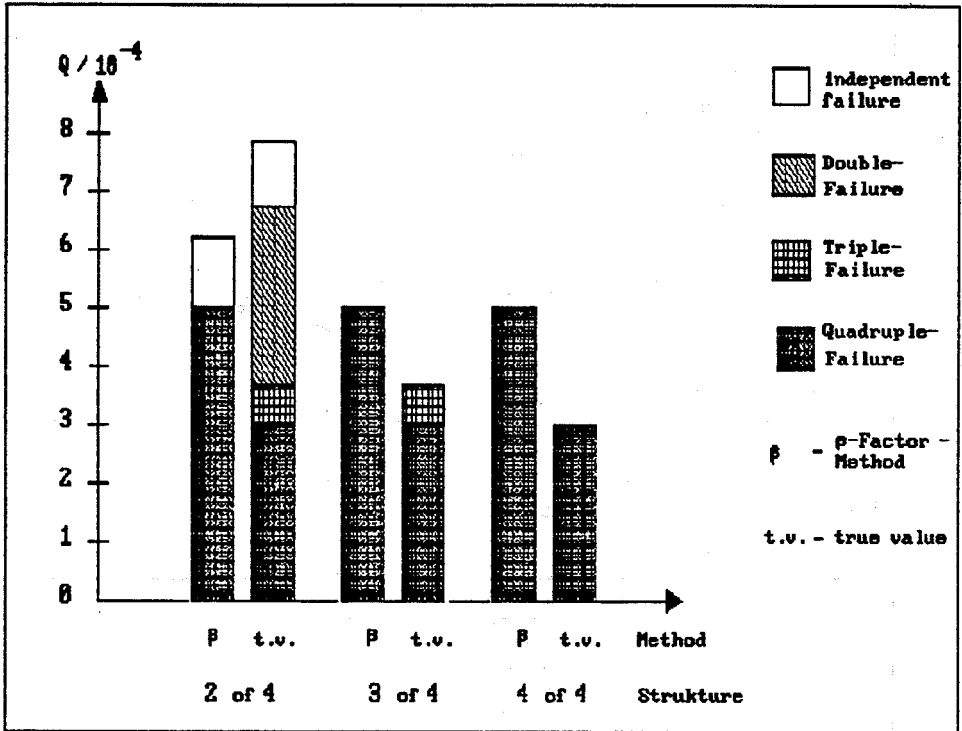


Figure 5.
Contribution of the single CCF kinds to
the failure probability of the system

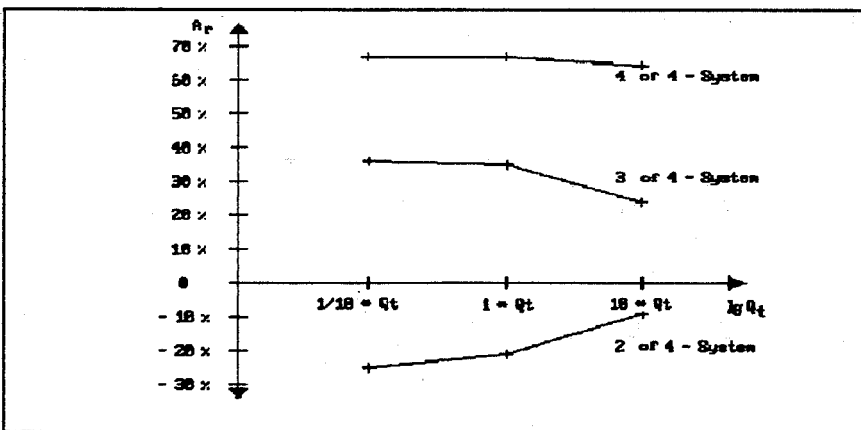


Figure 6.
Relative deviation A_r if the total failure
probability (Q_t) of the components vary

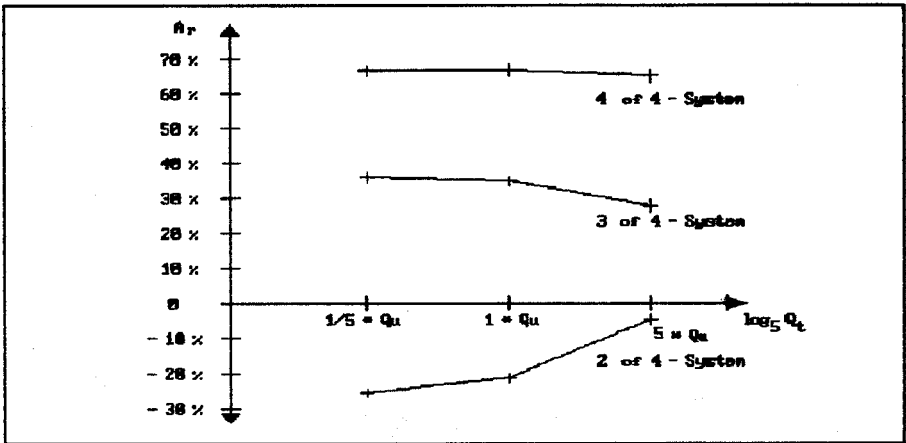


Figure 7.
Relative deviation A_r if the share of the independent failures (Q_u) vary

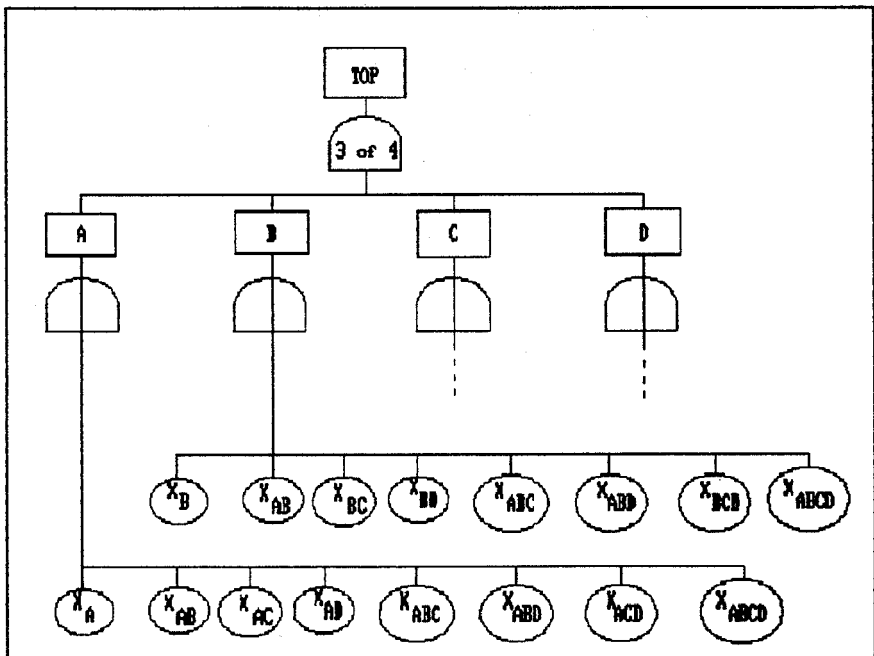


Figure 8.
Complete fault tree of a 3 of 4 - system

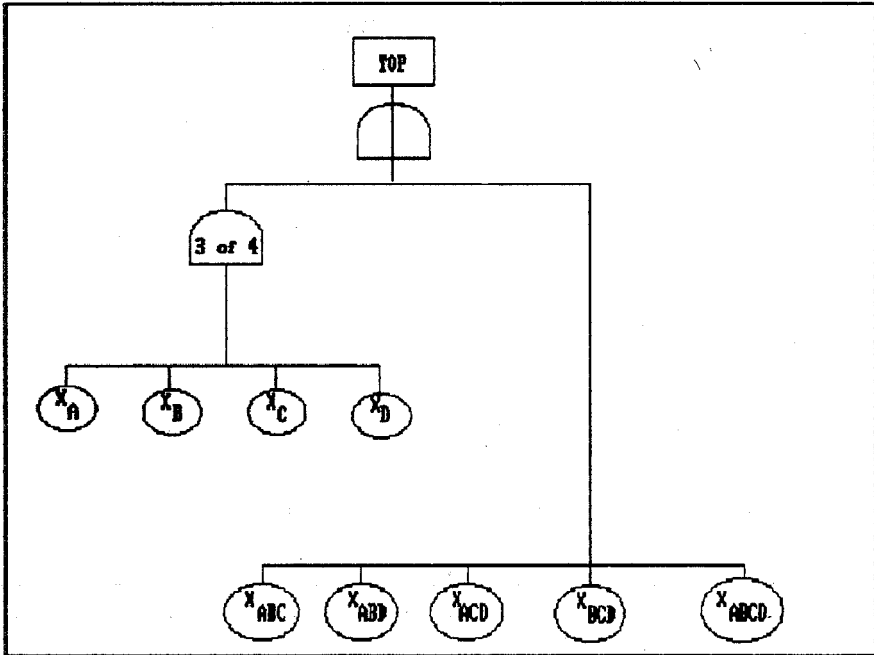


Figure 9.
Simplified fault tree of a 3 of 4 - system

Table 1.
Results of the calculations

	Q_s	Q_{sc}	Q_{sp}	A_a	A_r
1/4	2,0 E-2	1,87 E-2	1,85 E-2	-2,0 E-4	-1,1%
2/4	1,5 E-4	7,88 E-4	6,21 E-4	-1,67E-4	-21,8%
3/4	5,0 E-7	3,7 E-4	5,0 E-4	1,3 E-4	35,8%
4/4	6,25 E-10	3,0 E-4	5,0 E-4	2,0 E-4	66,7%

Table 2.
"True value" (1 of 4-System)

$Q_{sc} = 1,87 \cdot 10^{-2}$							
independent share			CCF share				
n	0	$U / U\%$	n	0	A	$U / U\%$	
4	1	1,8 E-2 96,42%	6	1	Z	3,0 E-4 1,61%	
			4	1	D	6,67 E-5 0,36%	
			1	1	V	3,0 E-4 1,61%	
							$\Sigma = 6,67 E-4$ 3,57%

Table 3.
 β -Factor - Method (1 of 4-System)

$Q_{sp} = 1,85 \cdot 10^{-2}$							
independent share			CCF share				
n	0	$U / U\%$	n	0	A	$U / U\%$	
4	1	1,85 E-2 97,30%	1	1	V	5,0 E-4 2,78%	

Table 4.
"True value" (2 of 4-System)

$Q_{SC} = 7,88 \cdot 10^{-4}$							
independent share			CCF share				
n	0	U / W%	n	0	A	U / W%	
6	2	1,22 E-4 15,48%	6	1	Z	3,0 E-4 38,87%	
			4	1	D	6,67 E-5 8,64%	
			1	1	V	3,0 E-4 38,87%	
							$\Sigma = 6,67 E-4$ 84,5%

Table 5.
 β -Factor - Method (2 of 4-System)

$Q_{SP} = 6,22 \cdot 10^{-4}$							
independent share			CCF share				
n	0	U / W%	n	0	A	U / W%	
6	2	1,22 E-4 19,61%	1	1	V	5,0 E-4 80,38%	

Table 6.
"True value" (3 of 4-System)

$Q_{SC} = 3,7 \cdot 10^{-4}$							
independent share			CCF share				
n	0	U / W%	n	0	A	U / W%	
4	3	3,6 E-7 0,09%	4	1	D	6,67 E-4 18,02%	
			1	1	V	3,0 E-4 81,88%	
			15	2	Z/Z	3,75 E-8 0,01%	
			12	2	E/Z	2,7 E-6 0,72%	
							$\Sigma = 3,69 E-4$ 99,9%

Table 7.
β-Factor - Method (3 of 4-System)

$Q_{sp} = 5,8 \cdot 10^{-4}$							
independent share				CCF share			
n	0	W / W%		n	0	A	W / W%
4	3	3,6 E-7 0,87%		1	1	V	5,8 E-4 99,92%

Table 8.
"True value" (4 of 4-System)

$Q_{sc} = 3,083 \cdot 10^{-4}$							
independent share				CCF share			
n	0	W / W%		n	0	A	W / W%
1	4	4,1 E-10 0,00%		1	1	V	3,0 E-4 99,99%
				6	2	D/D	1,67 E-9 0,00%
				3	2	Z/Z	7,5 E-9 0,002%
				12	2	Z/D	1,0 E-8 0,003%
				4	3	Z/Z/Z	5,0 E-13 0,00%
				4	2	E/D	3,0 E-7 0,10%
				12	3	E/Z/Z	1,35 E-10 0,00%
				6	3	E/E/Z	6,1 E-9 0,002%
							$Z = 3,083 E-4$ 99,99%

Table 9.
β-Factor - Method (4 of 4-System)

$Q_{sp} = 5,8 \cdot 10^{-4}$							
independent share				CCF share			
n	0	W / W%		n	0	A	W / W%
		4,1 E-10 0,00%		1	1	V	5,8 E-4 99,99%

Table 10.

Increase of Q_t to the tenfold :

	Q_s	Q_{sc}	Q_{sp}	A_a	A_r
1/4	2,0 E-1	1,87 E-1	1,85 E-1	-2,0 E-3	-1,1%
2/4	1,5 E-2	1,88 E-2	1,71 E-2	-1,7 E-3	-9,8%
3/4	5,8 E-4	4,31 E-3	5,36 E-3	1,85E-3	24,4%
4/4	6,25 E-6	3,84 E-3	5,0 E-3	1,96E-3	64,5%

Table 11.

Decrease of Q_t to one tenth of the former value :

	Q_s	Q_{sc}	Q_{sp}	A_a	A_r
1/4	2,0 E-3	1,87 E-3	1,85 E-3	-2,0 E-5	-1,1%
2/4	1,5 E-6	6,79 E-5	5,12 E-5	-1,67E-5	-25,8%
3/4	5,8 E-10	3,67 E-5	5,0 E-5	1,33E-5	36,8%
4/4	6,25 E-14	3,8 E-5	5,0 E-5	2,0 E-5	66,7%

Table 12.

Increase of the independent share (Q_u) to the fivefold:

($\beta = 2,2\%$)

	Q_s	Q_{sc}	Q_{sp}	A_a	A_r
1/4	9,2 E-2	9,87 E-2	9,85 E-2	-2,8 E-4	8,2%
2/4	3,17 E-3	3,7 E-3	3,54 E-3	-1,6 E-4	-4,3%
3/4	4,87 E-5	4,26 E-4	5,46 E-4	1,2 E-4	28,8%
4/4	2,8 E-7	3,82 E-4	5,0 E-4	1,98E-4	65,5%

Table 13.

Decrease of the independent share (Q_u) to one fifth of the former value :

($\beta = 35,7\%$)

	Q_s	Q_{sc}	Q_{sp}	A_a	A_r
1/4	5,6 E-3	4,27 E-3	4,1 E-2	-1,7 E-4	-3.98%
2/4	1,18 E-5	6,72 E-4	5,05 E-4	-1,67E-4	-24.8%
3/4	1,1 E-8	3,67 E-4	5,0 E-4	1,33E-4	36.2%
4/4	3,84 E-12	3,0 E-4	5,0 E-4	2,0 E-4	66,7%

Session II-A :Analysis of Dependencies

CSNI WORKSHOP ON SPECIAL ISSUES OF LEVEL-1 PSA

Cologne, Germany 27th-29th May 1991

**Evaluation Criteria of Safety
System Unavailabilities for
Nuclear Power Plants**

Hideaki MURAKAMI	(Tokyo Electric Power Company)
Singo ODA	(Hitachi Engineering Co.Ltd.)
Takashi SATO	(Toshiba Corporation)
Masaki MATSUMOTO	(Hitachi, Ltd.)
Satoshi MIURA	(Hitachi Engineering Co.Ltd.)

Abstract

Nuclear power plants have been installed a number of safety systems to make a safely shutdown under the postulated designing basis accidents. Such a kind of safety system has been designed to achieve a highly reliability and to get a large redundancy. Even if a multiple failure of safety systems takes place in same time, the safety systems have a possibility to avoid a large core damage accident.

Probabilistic safety assessments(PSAs) have been developed as an analytical method to evaluate the safety ability of nuclear power plants, quantitatively. Also, the improvement items for plant safety would be presented during the evaluation process.

From the level 1 PSA, in which core damage frequencies were evaluated, the improvements based on prevention approach were assessed. But, the conclusions were highly depended on the hypotheses on unavailability evaluation of safety systems or on the reliability of base data.

In this paper, the results of level 1 PSA performed in Japanese boiling water reactor (BWR) industry group were presented. And, the evaluation criteria and experience data of safety system unavailabilities were assessed. Especially, TB sequence, which was caused by the loss of all AC power, was analyzed, because the TB sequence was highly depended on the Japanese data.

1.Results of BWR level 1 PSA in Japan

1.1 Outline of typical BWR plants

Figure-1 shows the comparison of safety system configurations of BWR-3, - 4 and - 5.

In Japan, four types of BWR(BWR-2, -3, -4 and -5) are operating. And, two types of primary containment vessel(Mark-I and -II) were presented. In the level 1 PSA, BWR-3 with Mark-I, BWR-4 with Mark-I and BWR-5 with Mark-II were selected as typical BWR plants. Because, the type of primary containment vessel(PCV) is less effect for the results of level 1 PSA, and the designing of BWR-2 is almost same as that of BWR-3.

Feature of typical BWR plants are described as follows.

(1) BWR-3 plant

Safety systems of BWR-3 are constructed with two diesel generators(D/Gs) for emergency power supply, a turbine driven high pressure core injection system(HPCI),

two motor driven core spray systems(CSs) and two isolation condensers(ICs) for core cooling. Also, two shutdown heat cooling systems(SHCs) and two containment cooling systems(CCSs) are installed for decay heat removal.

(2) BWR-4 plant

Safety systems of BWR-4 are constructed with two D/Gs, an HPCI, two CSs, two motor driven low pressure core injection systems(LPCIs, two pumps per each system) and a turbine driven reactor core isolation cooling system(RCIC). Also, two residual heat removal systems(RHRs) are installed. The pumps of RHR and LPCI are held in common.

(3) BWR-5 plant

Safety systems of BWR-5 are constructed with three D/G, a motor driven high pressure core spray system(HPCS), a motor driven low pressure core spray system(LPCS), three LPCI(one pump per each system) and a RCIC. Also, two RHRs are installed. The pump of RHR and LPCI are held in common.

1.2 Categorizing of accident sequences

A large number of accident sequences are described as a combination of initiating events and failures of safety systems. But, these accident sequences are categorized into some typical accident sequences with same thermal-hydraulic transient. Typical accident sequences are defined as follows.

- (1) TC sequence: Transients or LOCA with failure of reactivity control
- (2) TB sequence: Transients with loss of AC power supply
(Station blackout)
- (3) AE,S1E,S2E: LOCAs without make-up water
sequences (A:Large LOCA, S1:Intermediate LOCA,
S2:Small LOCA)
- (4) TQUV sequence: Transients with failure of high and low
pressure core cooling systems
- (5) TQUX sequence: Transients with failures of high pressure
core cooling systems and depressurization
systems
- (6) TW sequence: Transients or LOCAs with failure of decay heat
removal

1.3 Comparison between BWR-3, -4 and -5

Figure-2 shows the comparison of core damage frequencies of BWR-3, -4 and -5. Core damage was defined over 1200 °C, due to the multifailures of safety systems.

Core damage frequencies of BWR-3, -4 and -5 were below 1.0×10^{-6} /r.y. (r.y.:reactor year). From the comparison of frequencies among each accident sequences, the accident sequences caused by LOCAs were dominant for BWR-3 plant. Because a number of core cooling system in BWR-3 was less than that in BWR-5. While, the accident sequences caused by transients were dominant for BWR-4 and -5. Because BWR-4 and 5 had only two high pressure core cooling systems, but BWR-3 had three(an HPCI and two ICs).

The core damage frequencies by TC, AE, S1E, S2E and TQUV sequences were mainly depended on the safety system unavailabilities calculated with fault tree analysis.

So, the result of above sequences should have some conservatism, because component failure rates applied for fault tree analysis were based on the data from general industry. The core damage frequencies from TW and TQUX sequences were mainly depended on the human errors or human credits. So, the result of TW and TQUX sequences should have some uncertainty. Finally, the core damage frequencies from TB sequences was mainly depended on the data from Japanese operating experience. The annual frequency of offsite power loss, and failure rates of D/G and offsite power recovery were determined by the Japanese data. In following section, the reliability of offsite power based on Japanese operating experience would be discussed.

2. Reliability of offsite power in Japan

2.1 Feature of two physically separated transmission line trip

Operating experiences of two physically separated transmission line (over 187 kV nominal voltage) trip were analyzed with the data from start of operate to 1987, due to define the reliability of offsite power in Japan. 163 of two physically separated transmission line trip had occurred until 1987. From this data, the frequency of two physically separated transmission line trip was obtained to about $7.3 \times 10^{-2}/100\text{km/year}$.

(1) Causes of transmission line trip

Figure-3 shows the accident causes of offsite power loss.

Dominant cause was thunderbolt (82% of all). Almost of them was recovered within 5 minutes. Because, the transmission line trip caused by thunderbolt was temporarily event, and was recovered in a short time. On the other hand, the two physically separated transmission line trip caused by snowfall or typhoon was in low frequency, but continued in a long time.

(2) Topography of transmission line trip occurs.

Figure-4 shows the topographies occurred offsite power loss.

Dominant topography was mountains (77% of all). Almost of them was recovered within 10 minutes. In mountains, the transmission line trip caused by snowfall or typhoon was in low frequency, but was required long time to recover.

(3) Time dependency

Figure-5 shows the frequencies of two physically separated transmission line trip.

In the early time of operation, about $1.0/100\text{ km/year}$ of transmission line trip was occurred. But, decreased after 1962. Recently, the transmission line trip has been decreased to about $5 \times 10^{-2}/100\text{ km/year}$, because of the improvement to thunderbolt or the application of rapid reclosing system.

2.2 Reliability and recovery profile of offsite power in Japan

(1) Definition of offsite power loss

Figure-6 shows the power supplying system of nuclear power plants.

A loss of offsite power is defined as the event in which there is no way to supply the power to safety system, except diesel generator. This is the event with the losses of offsite power and of preferred power.

The offsite power was lost by the failure of external or internal equipment, and the preferred power was avoided with the failure of switchover to start-up or auxiliary transformer.

The frequency of offsite power loss defined above was $1.4 \times 10^{-2}/\text{r.y.}$ for BWR. There were 2 experiences of offsite power loss within 153.8 reactor years for BWR. In these cases, D/G supplied power to emergency buses, and the offsite power was recovered within 30 minutes, actually.

(2) Recovery profile of offsite power

Figure-7 shows the recovery profile of offsite power.

Usually, the loss of offsite power in nuclear power plant was occurred, when the accident of transmission line was caused by external incident or by internal event. So, the recovery profile of offsite power was closely depended on recovery of two physically separated transmission line. But, the failure frequency of two physically separated transmission line have been reduced after 1962.

In the level 1 PSA, the recovery profile of two physically separated transmission line was assessed with the conservative method. At 24 hours after accident, once of transmission line trip was assumed in actual trips. Thus, the recovery curve made some over estimation up to 24 hours (a duration time of safety systems).

3. Summary

Probabilistic safety assessments (PSAs) have been developed not only to evaluate the unavailability of safety systems and the reliability of plants, but also to improve the safety of plants. The level 1 PSA, which assesses the frequency of core damage or core melt, are applicable to improvements based on prevention approach. In this paper, the system unavailabilities used in level 1 PSA for typical Japanese BWR were discussed. And, the reliability of dominant sequences was presented. Finally, the reliability data of offsite power, which are collected in Japan, were assessed. From this assessment, there was a little experiences of offsite power loss in Japan. The large contribution of offsite power losses in Japan was occurred by thunderbolt at mountains. And, such a kind of accident was usually temporary event, and recovered in a short time.

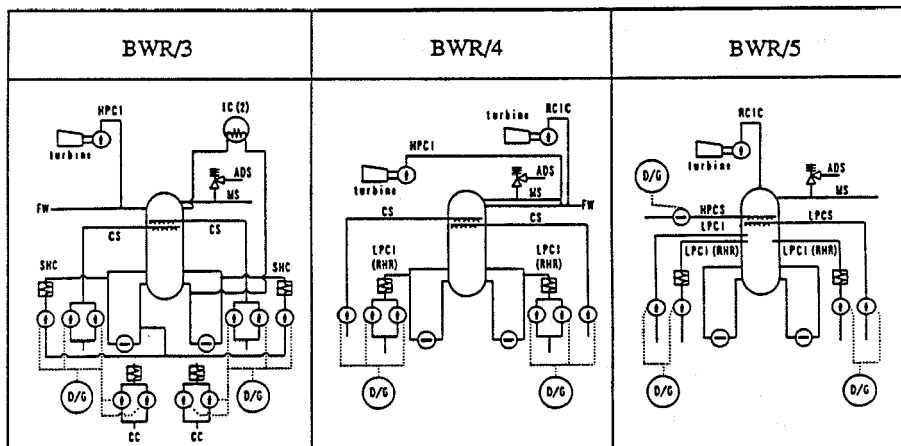


Figure-1 Comparison of System Configuration of ECCS/RHR and D/G

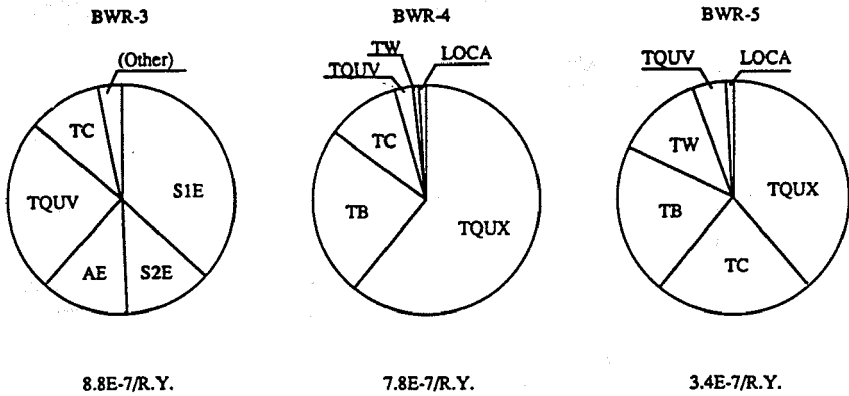


Figure- 2 Comparison of core damage frequencies

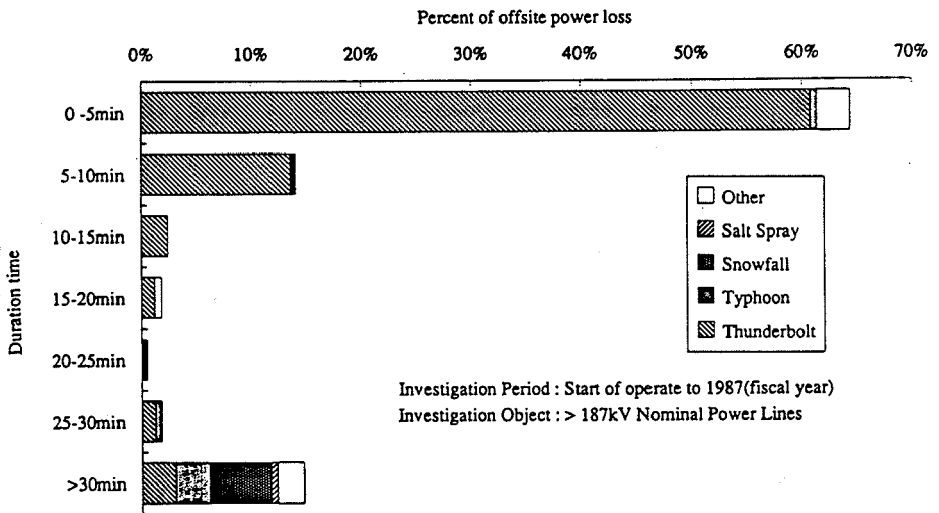


Figure-3 Accident causes offsite power loss.

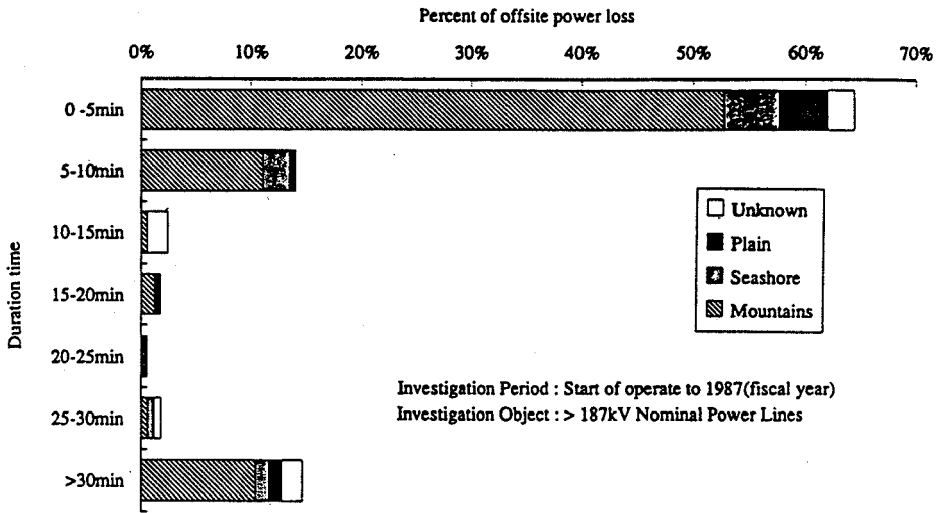


Figure-4 Topographies occurred offsite power loss.

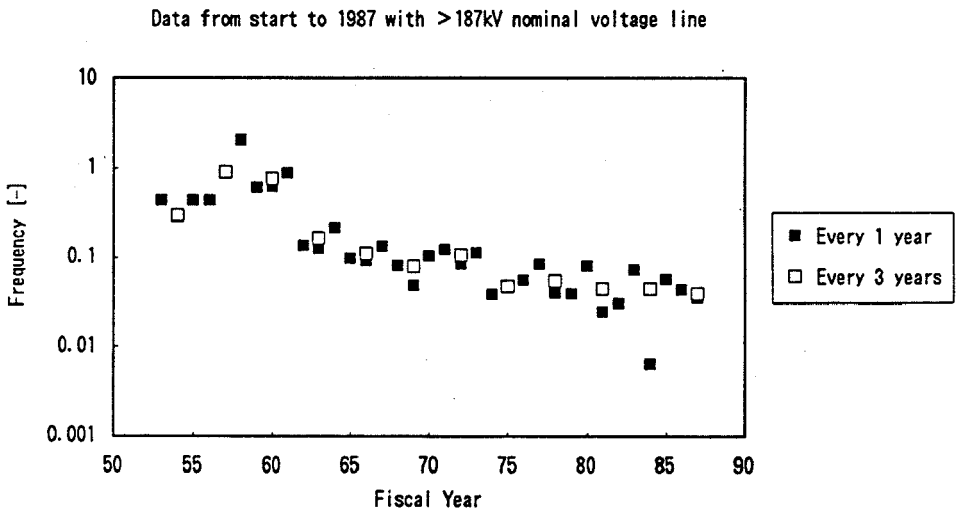


Figure-5 Frequencies of two physically separated transmission line trip

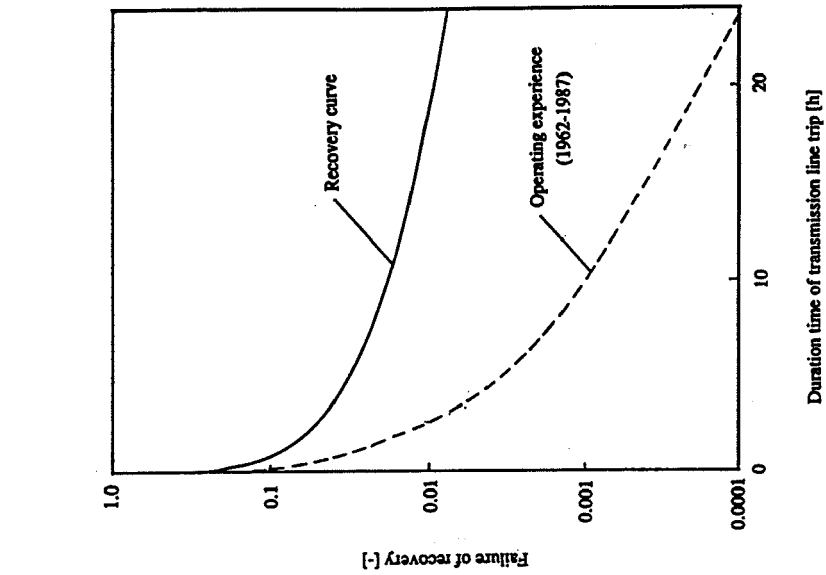


Figure-7 Recovery profile of offsite power

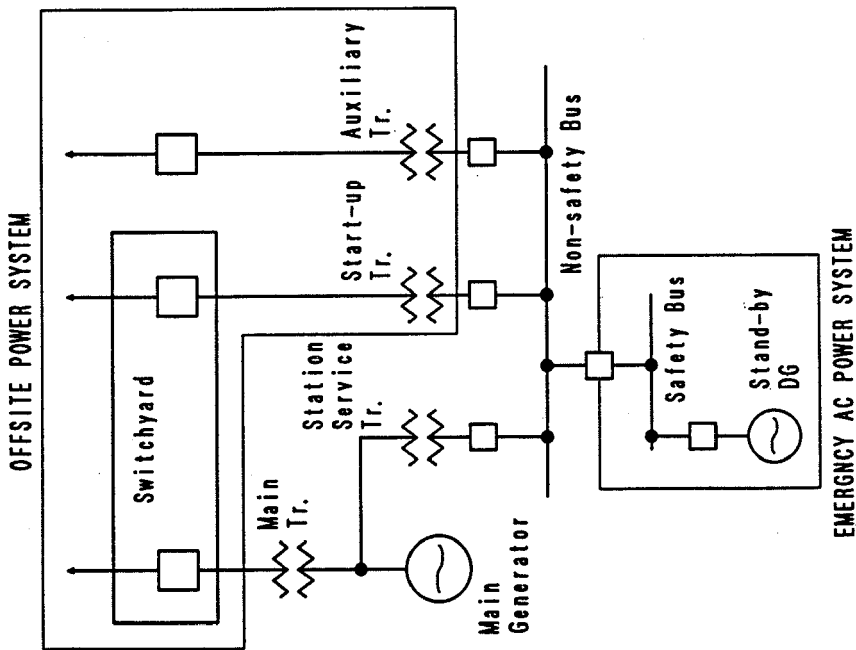


Figure-6 Power Supplying System

SIEMENS

OECD/BMU - Workshop

Special Issues of Level 1 PSA

Cologne, FRG

27th - 29th May 1991

PSA Convoy

Influence and Modelling of Common Cause Failures

A. Feigel, J. Wenzel
Siemens AG, KWU
Erlangen
FRG

PSA Convoy

Influence and Modelling of Common Cause Failures

A. Feigel, J. Wenzel
Siemens AG, KWU
Erlangen, FRG

1. Introduction

For the realized PWR 1300 MW - Convoy plants a PSA on basis of a selected number of initiating plant internal events (reference sequences) has been performed; external and area events are not investigated. Moreover the valuation is accordant to the actual German PSA-guide. The used efficiency conditions for the systems needed to cope with the accidents are of best estimate character. Due to the current engineering with highly redundant safety systems a high safety level is expected. Thus the contribution of common cause failures treatment becomes important.

SIEMENS

PSA Convoy

Influence and Modelling of Common Cause Failures

Objective

- Probabilistic Valuation of Convoy Plants with actual data and methodology
- Application of "Stochastic Reliability Analysis Model (SRA)" for Common Cause Failure valuation

SIEMENS

Background

- Different Common Cause Failure models are worldwide used, e.g.:
 - + simplified β - factor model
 - + Multiple Greec Letter model (MGL)
 - + Binomial Failure Rate model (BFR)
- Actual Trend towards BFR
- Stochastic Reliability Model (SRA) uses BFR - formalism with consequent stochastic interpretation of component behaviour

2. Common Cause Failure Verification

In the frame of Convoy PSA a new common cause failure approach was used. By long during experience and cooperation to several panels the "Binomial Failure Rate Model with Lethal Shock" (BFR) was developed to a "Stochastic Reliability Analysis Model" (SRA). The detailed basis and justification of this approach is described in full detail in various publications /1 - 4/. Therefore in the following only a short description of the background of the SRA model is given mainly with respect to practical application. Before explaining the SRA model the BFR approach is reminded, see fig.3:

SIEMENS

BFR Formalism

- Interpretation within the Basic Parameter model family

$Q_i(k)$ multiple failure event frequency of failure of exactly
i from k identical redundant components
(for $i \geq 2$ dependent)

Examples:

$$Q_1(3) = Q_1$$

$$Q_3(3) = \omega + \mu p^3 + Q_1^3$$

$$Q_2(3) = \mu p^2 (1 - p) + Q_1^2$$

$$P_{3/3} = Q_3(3) + 3 Q_2(3) Q_1(3) + (Q_1(3))^3$$

Disadvantage: difficult fault tree handling for highly
redundant systems

- "Stochastic" Interpretation

$$P_{i/k} = \omega \delta_{ik} + \mu p^i (1 - p)^{k-i} + Q_1^i$$

$\delta_{ik} = 1$ if $(i = k)$ and $= 0$ otherwise (Kronecker delta)

ω : frequency of lethal shocks, fails all components
("coupling parameter" value $p_0 = 1$)

μ : frequency of non-lethal shocks, fails ≥ 1 component

p : non-lethal shock efficiency coefficient (coupling parameter)

Q_1 : "independent" failure rate / probability, fails only 1 component

PSA Convoy

RAU/C-REWE/ES-11

Fig.3: Binomial Failure Rate Model with Lethal Shock (BFR)

(Note: BFR model is created by simply adding another shell (μ, p) to the β -factor model thus now 4 independent parameters have to be determined from data).

This BFR approach means - as the other models too - establishing Common Cause Failure as an extra phenomenon which has to be treated with extra methods in reliability and data analysis. In reality dependencies do not result from Common Cause but from different failure behaviour, that means by inhomogeneous populations. This requires the use of stochastic models - SRA - which consider:

- variability in failure behaviour in an inhomogeneous population where besides of normal failure behaviour outliers (enhanced failure rate without physical coupling) and lethal shocks due to a stochastic process are implemented.
- connection to existing approach for modelling the behaviour of inhomogeneous populations, e.g. thermodynamic populations.

The stochastic process which has to be considered in these models is expressed by a discrete probability density function

$$f(x) = \sum_{i=0}^{n-1} a_i \delta(x - p_i)$$

where the factors a_i of the n discrete shells (n subpopulations with the failure probability p_i) must be determined. The simplest sufficient flexible approximation involves 3 shells; thus yields a model with 4 parameters:

$$f(x) = a_0 \delta(x - 1) + a_1 \delta(x - p_1) + a_2 \delta(x - p_2)$$

$$a_2 = 1 - a_0 - a_1$$

The event "failure of exactly r from k redundant components" is described by

$$P_{r/k} = a_0 \delta_{rk} + a_1 p_1^r (1 - p_1)^{k-r} + a_2 p_2^r (1 - p_2)^{k-r}$$

SRA formalism is shown in fig.4.

SIEMENS

SRA Formalism

- Generalized Binomial Distribution Model

Failure of exactly r from k identical redundancies is described by

$$P_{r/k} = a_0 \delta_{rk} + a_1 p_1^r (1 - p_1)^{k-r} + a_2 p_2^r (1 - p_2)^{k-r}$$

with $\delta_{rk} = 1$ for $r = k$ and $= 0$ otherwise

- Sum rules

$$\sum a_i = 1 \quad \text{Composition completeness}$$

$$\sum P_{r/k} = 1 \quad \text{Event completeness (sum from } r=0 \text{ to } r=k)$$

- Total failure probability

$$Q = \langle p \rangle = P_{1/1} = a_0 + a_1 p_1 + a_2 p_2$$

- Fault tree representation

Failure of at least r from k redundancies (r/k - gate) is quantified by

$$P_{\geq r/k} = \sum P_{l/k} \quad (\text{sum from } l = r \text{ to } k)$$

- SRA directly yields $P_{r/k}$

- BFR yields $P_{r/k}$ only indirectly via Basic Parameters $Q_i(k)$, e.g.:

$$P_{3/3} = Q_3^{(3)} + 3 Q_2^{(3)} Q_1^{(3)} + (Q_1^{(3)})^3$$

PSA Convoy

Fig.4: Stochastic Reliability Analysis Model (SRA) (1)

SIEMENS

Meaning of SRA Model Parameters (version with 3 shells)

- Population composition parameters a_i ("global" parameters)

a_0 occurrence frequency of "lethal" outliers
($p_0 = 1$: "coherent failure", "superfailure")

a_1 occurrence frequency of "non-lethal" outliers

a_2 occurrence frequency of "normal" component failure behaviour

- Subpopulation failure parameters p_i ("local" parameters)

p_1 "non-lethal" outlier failure probability

p_2 "normal" (generic) failure probability

PSA Convoy

Fig.5: Stochastic Reliability Analysis Model (SRA) (2)

The valuation of the parameters is shown in fig.5 to 9.

Fig.5 contains the meaning of SRA parameters.

The 3 shells of the failure behaviour are:

- normal ("generic") failure behaviour with importance a_2 (relative part of the relevant model population). Within this behaviour type independent failures occur with the probability p_2 .
- "outliers", e.g. by design failure or excessive operation conditions (importance a_1 , typical in the range of few percent, independent failures with enhanced probability p_1).
- physical couplings which cause coherent failure of all redundants. The condition for coherent failure is the importance a_0 , the failure probability in this subpopulation is $p_0 = 1$.

Fig.6 shows a relational comparison between SRA and BFR parameters.

Fig.7 contains the valuation of lethal shock frequency a_0 .

The parameter a_0 is valued in a qualitative engineering judgement which identify dependencies and missing barriers in a system. Rare multiple failures from worldwide experience can contribute. This has to be taken into account but in general it can not be transferred to the system to be valued. Furthermore a_0 defines a limit up to that an improvement of reliability by enhancement of redundancy grade is possible.

SIEMENS

Approximate correspondence

- Similarity

$a_0 \sim \omega$ (direct comparable)

$a_1 \sim \mu$ (outliers versus non-lethal shocks)

- Different meanings

p (BFR) \longleftrightarrow p (SRA)

p (BFR) : "coupling parameter"

p (SRA) : probability

PSA Convoy

Fig.6: Relational comparison between SRA and BFR

SIEMENS

Valuation of lethal shock frequency a_0

- Hard Limitations on a_0

- Preliminary tool

Recording of dependency - relevant features like

- spatial separation,
 - absence of common hardware,
 - absence of common personnel activities,
- by check list (non - numerical information)

- Preliminary quantification

Typical range for good designs

$$10^{-6} < a_0 < 10^{-4}$$

- Linear dependence on test interval, as test is efficient against failure accumulation, minimum value ("experience horizon"):

$$4 \text{ weeks: } a_0 = 1 \cdot 10^{-6}$$

$$1 \text{ year: } a_0 = 1.3 \cdot 10^{-5}$$

- Every single dependency feature alone can make things bad (additive model for compound effect of several features is preferred)

Soft limitations on P_{FK}

Rough compliance with multiple failure experience, evaluated with in the vague CCF concept

PSA Convoy

Fig.7: Dependent Failure Modelling - "Data Interface"

The valuation of lethal shock frequency considers design features recorded in non-numerical information, see fig.8.

The range of SRA parameters is shown in fig.9.

SIEMENS

Influence factor	Independence	Dependence	Explanation
Component type (construction)	different	0 : same	0 :
Manufacturer	different	0 : same	0 :
Location	different	0 : same	0 :
Control	separate	0 : common	0 :
Power supply	separate	0 : common	0 :
Auxiliary systems	separate	0 : common	0 :
External impacts	secured	0 : not sec.	0 :
Internal impacts	secured	0 : not sec.	0 :
Test interval	different persons/	same person/	0 :
Mainten. interval	different	0 : same	0 :
Department	Name	Tel.:	Date:

PSA Convooy
Fig.8: Check list for recording dependency - relevant features

SIEMENS

B_0 = Lethal Shock Occurrence Frequency

- Quantification basis is the worldwide experience
- 0 - failure statistics delivers values of 10^{-6} ... 10^{-4} for components with yearly tests
- plant specific test intervals are considered

a_1 = Outliers Frequency, Spectral Density of p_1

- Quantification basis is the plant specific statistic
- General approach: 1 ... 5% of the mean value
- Specific approach:
 - - Spectral analysis of the observed failure samplings, or
 - - Fitting of a distribution function (e.g. log normal) to the observed sampling of failures
- In PSA Convooy: $a_1 = 5\%$ $p_1 = 10 p_2$

a_2 = Normal Component Failure Behaviour

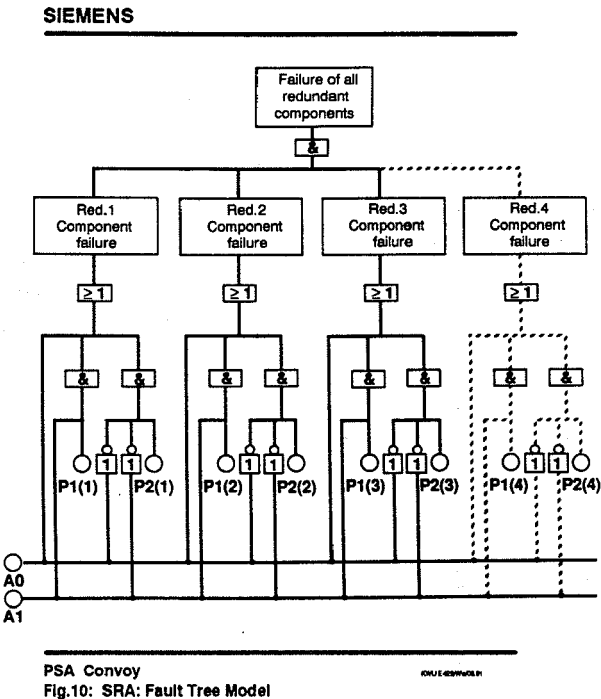
- Quantification: $a_2 = 1 - a_0 - a_1$

PSA Convooy
Fig.9: Determination of Occurrence Frequency

A stochastic evaluation of β - factors in terms of SRA model parameters can be performed:

$$\beta_r^k = \frac{a_0 \delta_{rk} + a_1 p_1^r (1 - p_1)^{k-r} + a_2 p_2^r (1 - p_2)^{k-r}}{a_0 + a_1 p_1 + a_2 p_2}$$

The fault tree structure of SRA model is shown in fig.10.



The advantages of the use of SRA are summarized in fig.11:

SIEMENS

Advantages of SRA - Model:

- Easy handling in fault tree structure
- Transparency of parameters for component failure behaviour
- Criteria for design influence of lethal shock are considered
- Check of parameters in BFR - formalism and β - factor approach with respect to plausibility

PSA Convoy
Fig.11: Advantages of Stochastic Reliability Model (SRA)

SIEMENS

System Efficiency Matrix

Sequence	Scram	RHR (incl. cooling chain)	Steam Release	Feedwater Supply
LOCA (Plant shutdown)				
• Small 1 (D = 2 - 25 cm ²)	X	1/4 LP	Main Steam Bypass or 1/4 Relief Valve	1/3 Main FW or 2/2 Start-up Pp. or 2/4 Emerg. FW
• Small 2 (D = 25 - 80 cm ²)	X	1/4 HP/Recirc. and 1/3 LP/Flooding (h) and 1/3 LP/Recirc. (h)		
• Pressurizer Safety Valve Fail open PORV (D = 40 cm ²)	X	1/4 HP and 1/4 LP/Flooding and 1/4 LP/Recirc.		
Transients (hot, subcritical)				
• Loss of Main Feedwater	"ATWS" 3-4/4 Extrabor. 3/3 Press. Valve 2/6 FW-Supply	J.	Main Steam Bypass or 1/4 Relief Valve or 1/4 Safety Valve	1/2 Start-up Pp. or 1/4 Emerg. FW
• Emergency Power Mode	"ATWS" (s. a.)	J.	1/4 Relief Valve or 1/4 Safety Valve	1/2 Start-up Pp. incl. Aux. DG or 1/4 Emerg. FW incl. Emerg. DG

PSA CONVOY

(1/4 = 1 out of 4 trains)

KWU E42
Dr. Fabian
05.91

Fig. 13: System Efficiency Matrix

4. Results

Taking into account the detailed analysed reference sequences and the estimation of further sequences the total frequency of events not coped with by operating and safety systems results in $F \sim 3 \cdot 10^{-6} / a$.

It should however be pointed out that this frequency is by no means identical with core damage because a consideration and valuation of accident management measures is not taken into account. In any case the core damage frequency will result in a value of less than the above mentioned.

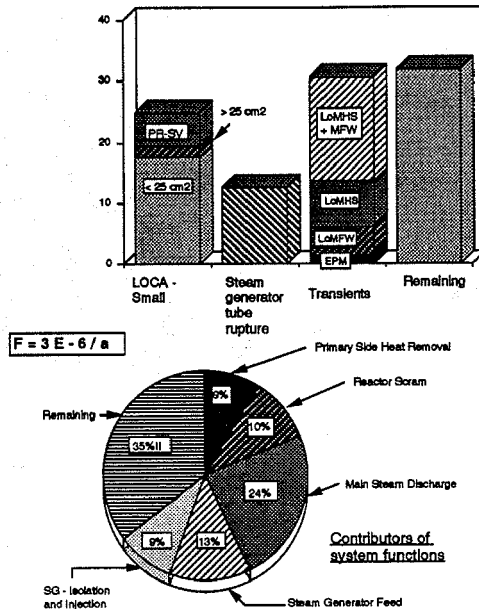
The contributors of sequences and safety functions to the frequency of uncoped events is shown in fig.14. The result indicate the high safety level of the design and the balanced safety concept.

The remaining sequences are e.g.

- Large and Medium Break LOCA,
- Leaks at Pressurizer (due to transients demands),
- Interfacing System LOCA
- Steam and Feedwater Line Breaks,
- ATWS
- Fire, Earthquake

SIEMENS

Contributors of Sequences



PSA Convoy

KWU E422/Wa06.91

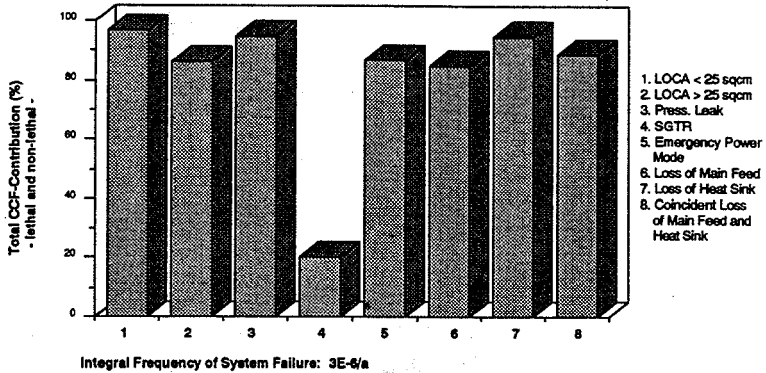
Fig.14: Contributors of Sequences and System Functions

The structure of Common Cause Failures in the results (lethal shock and non-lethal shock contribution) can be shown only with this SRA model.

The result of the analysis is determined essentially by lethal contributors dependent on the high grade of redundancy. The dominance of CCF to integral systems failure is characteristic for "good" designed systems. Independent failures at components will be compensated by redundancy in design and thus they are less relevant. The total Common Cause Failure contribution (lethal and non-lethal) to the min-cuts is shown in fig.15

The CCF-contributors of the sequences are with the exception of "Steam Generator Tube Rupture" (SGTR) in the range of 80 - 95%. For coping with SGTR many functions are necessary, thus failure at single components are still important and the CCF-contributor in this case is only about 20%.

SIEMENS



PSA Convoy

KWU E42/W05.91

Fig.15: Total Contribution of CCF to Frequency of Events uncoped by Operating and Safety Systems

The valuation of the PSA-result for Convoy-design is summarized in fig.16.

SIEMENS

Valuation of PSA result for Convoy design

- + The advanced design of Convoy plants results in a high safety level
 - Integral Frequencies for uncoped sequences: $F \sim 3 \cdot 10^{-6} / a$
 - not considering accident management procedures
- + Contributors from Leaks and Transients are in the same order of magnitude, thus the design is balanced
- + Balance of design also reflects the contribution of system functions
- + The high safety level is extremely shown by high contributors of CCF. The unavailability of high redundant systems is typically dominated by CCF. Independent component failure will be compensated by redundancy

PSA Convoy

KWU E 42/W05.91

Fig.16: Valuation of PSA - Result

The investigation of safety level and balance of systems in a nuclear power plant with advanced engineering like the realized German Convoy - plants can be performed adequate using the SRA model within the PSA. The limit of systems unavailability improvement by enhancement of redundancy can be interpreted using SRA model which is an adequate tool taking into account design features also. The improvement of systems reliability up to 4 redundancies is reasonable also from commercial point of view.

5. Literature

- /1/ Hughes, R.P., A new approach to common cause failure.
Reliab. Engng. 17 (1987) 211 - 236
- /2/ Dörre, P., Basic aspects of stochastic reliability analysis for redundancy systems,
Reliab. Engng. and System Safety 24 (1989) 351 - 376
- /3/ Dörre, P., Stochastic reliability analysis: the interface for component data
evaluation, In Trans. 10th International Conference on Structural Mechanics in
Reactor Technology SMiRT-10 (ed. A. Hadjian), Anaheim, California, USA,
August 17-21, 1989, Vol. P: Probabilistic Safety Assessment, P. 25 - 30
- /4/ Dörre, P., Stochastic reliability analysis - its application to complex redundancy
systems, Reliability Data Collection and Use in Risk and Availability Assessment,
Proceedings of the 6th EuReData Conference (ed. V. Colombari); Siena, Italy,
March 15 - 17, 1989, Springer Verlag, Berlin, Heidelberg, New York, London,
Paris, Tokyo 1989, P. 155 - 166

Time Dependent Phenomena/Uncertainties

Chairman: H. Pulkinnen

UNCERTAINTY ANALYSIS

An issue paper to be presented at
OECD/BMU Workshop on "Special Issues of Level-1 PSA"
May 27th – 20th, Cologne, Germany

Urho Pulkkinen
Technical Research Centre of Finland VTT

1 Problem description

The uncertainties of PSA are inherited from to several sources. A part of the uncertainty originates from the random phenomena and mechanisms of the component failures. The other uncertainties are due to simplifying assumptions and incomplete understanding of the phenomena and the nuclear power plant under analysis.

The basic types of uncertainty are usually divided in to two categories:

- uncertainty due to stochastic variability of the quantity of interest
- uncertainty due to lack of knowledge on phenomena modelled in PSA

The objectives of an uncertainty analysis in PSA are:

- to identify the uncertain assumptions, modelling principles and parameters applied in the PSA model
- to evaluate the significance of the identified uncertainties in the results of PSA

- to provide quantitative and qualitative information and proper interpretation on the impact of uncertainties
- to measure the credibility of the results of PSA
- to provide methods for decreasing the uncertainty and to give basis for decision making.

The problems of uncertainty analyses connected to the above issues are both methodological and philosophical. The latter are closely related to the interpretation of the results of the uncertainty analyses and the concept of probability. The methodological problems are related to the quantification of uncertainty contribution, selection of uncertainty distributions and identification of uncertain issues in the PSA-model.

2. Documents stating the state of the art

In the following some references dealing the uncertainty analyses in PSA are listed. The list is not intended to be complete, and some important references may be missing. The references listed here are selected mainly from the practical point of view. The references are listed in alphabetical order.

LIST OF DOCUMENTS

1. Analysis of Core Damage Frequency: Internal Events Methodology. (1990) NUREG/CR-4550, vol. 1, Rev. 1. U.S. Regulatory Commission, Washington, DC, January 1990.

2. Apostolakis, G.E. (1989) Uncertainty in Probabilistic Safety Assessment. Nuclear Engineering and Design, 115, pp. 173-179, North-Holland, Amsterdam, 1989.
3. Chhibber, S., Apostolakis, G., Okrent, D. (1991) On the Quantification of Model Uncertainty. Proceedings of the International Conference on Probabilistic Safety Assessment and Management (PSAM), Beverly Hills, CA, U.S.A. pp. 1483-1488. February, 1991.
4. Hirshberg, S., Jacobsson, P., Pulkkinen, U., Pörn, K. (1989). Nordic Reference Study on Uncertainty and Sensitivity Analysis. PSA'89 - International Topical Meeting on probability, Reliability and Safety Assessment, Pittsburgh, Pennsylvania, U.S.A., April 2-7, 1989.
5. Iman, R.L., Helton, J.C. (1985) A comparison of Uncertainty and Sensitivity Analysis Techniques for Computer Models. NUREG/CR-3904, SAND84-1461. Sandia National Laboratories, Albuquerque, NM, U.S.A., 1985.
6. Iman, R.L., Hora, S.C. (1990) A Robust Measure of Uncertainty Importance for Use in Fault Tree System Analysis. Risk Analysis, Vol. 10, No. 3, pp. 401-206.
7. Iman, R.L., Shortencarrier, M.J. (1984), Fortran 77 Program and User's Guide for the Generation of the Latin Hypercube and Random Samples for the Use with Computer Models. NUREG/CR-3624, Sand83-2365, Sandia National Laboratories, NM, March 1984.
8. Iman, R.L., Shortencarrier, M.J. (1986) A User's Guide for the Top Event Matrix Analysis Code (TEMAC), NUREG/CR-4598, SAND86-0960, Sandia National Laboratories, Albuquerque, NM, August 1986.

9. Oconee PRA (1984) A Probabilistic Risk Assessment of Oconee Unit 3. NSAC-60. The Nuclear Safety Analysis Centre, Electric Power Research Institute, California and Duke Power Company. 1984.
10. Oyster Creek Probabilistic Safety Analysis (1982). Plant Analysis update. PLG-0253. Pickard, Lowe and Garrick, inc. 1982
11. PRA Procedures Guide. (1983) NUREG-2300, U.S. Regulatory Commission, Washington, DC, January 1983.
12. Reactor Risk Reference Document. (1987) NUREG-1150, U.S. Regulatory Commission, Washington, DC, February 1987.
13. Seabrook Station Probabilistic Safety Assessment (1983) Pickard, Lowe and Garrick, Inc. Rev. 2.

3. Areas with well established and validated methodology

In the following the areas with well established and validated methodology are listed.

the methods for uncertainty propagation and sensitivity analyses, including computer tools

the statistical methods for determining the uncertainty distributions for failure model parameters (failure rates, failure probabilities per demand)

The development of uncertainty analysis methods was started first for the above mentioned issues. The recent methods are rather user friendly and several computer codes exist for these areas.

4. Areas where improvements are necessary

The traditional uncertainty analysis consisted merely on the propagation of uncertainties. However, the uncertainty analysis can be seen from a broader perspective, which reveals some need for further development. In the following the most important areas are listed:

- the methods for identification of uncertain assumptions of PSA

- the evaluation of incompletenesses of PSA

- the analysis of modelling uncertainties

- the determination of uncertainty distributions for dependent basic events (including the most complex knowledge dependencies and the methods for expert judgements (for example in human error analysis))

- the uncertainty analyses in living PSA

- the interpretation and presentation of the uncertainty analysis results

- the use of "uncertain" PSA in safety related decision making

- the uncertainty importance analyses

In the above mentioned areas lot of research has been performed. The results are still in rather impractical and theoretical form. Further work is needed in order to make practical applications possible.

Uncertainty study in probabilistic risk assessment for TVO I/II nuclear power plant

Jan Holmberg
Technical Research Centre of Finland
Laboratory of Electrical Engineering and Automation Technology
Otakaari 7 B, SF-01250 Espoo, Finland

Risto Himanen
Teollisuuden Voima Oy, SF-27160 Olkiluoto, Finland

ABSTRACT

The level 1 probabilistic risk assessment (PRA) for the TVO I/II nuclear power units is a utility driven effort to identify and prioritize accident sequences that can lead to a core damage. The main report of the level 1 PRA consisting of a study of internal initiators was submitted to the Finnish regulatory body for review in the end of 1989. It included a study of uncertainties of risk models and methods. The objective of the uncertainty study was to identify the major uncertainties, to assess their importances, and to demonstrate their impact in results. The methodology of the uncertainty study mainly based on earlier uncertainty studies in PRAs.

Uncertainties were studied both qualitatively and quantitatively. In the qualitative study the uncertainties were identified and classified following the hierarchy of the PRA models. The qualitative mapping out of the uncertainty factors turned out to be a useful way to plan effective quantitative studies. It also served as an internal review of the assumptions made in the PRA.

In the quantitative study the importance of the most significant uncertainties were verified by sensitivity calculations. The impact of statistical uncertainties was demonstrated by performing uncertainty range propagation for core melt frequencies in all initiator classes as well as for the total core melt frequency. The Monte Carlo method was chosen as the propagation method.

The most significant uncertainties were related to the modelling of human interactions, dependencies and common cause failures, loss of coolant accident frequencies and containment response. However, given the boundary conditions and limitations of the PRA, no major issue dominated as an uncertainty source because of the great detailness of the TVO's models.

1 Introduction

The Olkiluoto nuclear power plant, located on the western coast of Finland, is operated by Teollisuuden Voima Oy. The plant consists of two identical ASEA-ATOM (nowadays ABB-ATOM) BWR units, TVO I and TVO II. The net electrical power of a single unit is 710 MW.

TVO I/II PRA was initiated in 1984 by the utility. The main report containing level 1 PRA study for internal initiators was submitted to the Finnish regulatory body (STUK) for review in spring 1989. It was completed with an uncertainty study by the end of 1989. Identification and prioritization of those human interactions and dependences which are most important to the core melt probability were among the main goals of the PRA study. In the uncertainty study these topics were proved to have most significant sources of uncertainty, too.

As a part of the PRA-project uncertainties of risk models and methods were systematically studied in order

- to identify uncertainties in models and parameters,
- to assess their importances, and
- to demonstrate their impact in results.

Uncertainties originate from limitations of methods and models in PRA as well as from the subjectivity in the estimation of basic probabilities and initiating event frequencies. Therefore uncertainties are usually divided in completeness, modelling, and parametric uncertainties. In our uncertainty study we have considered completeness uncertainties to be modelling uncertainties and interpreted them as boundary conditions of the models.

The methodology of the uncertainty study was based on earlier uncertainty studies in PRAs [1-7] and on a retrospective study of the methodology made by U. Pulkkinen, K. Kuhakoski and T. Mankamo [8]. Uncertainties were studied both qualitatively and quantitatively. We put much effort in the qualitative phase since we considered it more instructive and fruitful than mere evaluations of uncertainty measures.

The qualitative study which was the preliminary phase of the uncertainty study contained identification of uncertainties and qualitative assessments of their importance. The PRA was introduced and identified assumptions and uncertainties behind the models were documented. Meanwhile, the most significant uncertainties were selected by importance measures or other calculations based on the PRA's models for further quantitative studies.

The quantitative study contained sensitivity studies and propagation of uncertainty ranges. In the sensitivity studies uncertain assumptions or parameters were varied in order to illustrate the sensitivity of the models. The propagation of uncertainty ranges demonstrated the joint impact of uncertainties and gave uncertainty measures. Also the possible benefits from some plant modifications were assessed using the sensitivity studies.

There is a list of characteristics of both the qualitative and the quantitative study in the table 1.

TABLE 1
Comparison of qualitative and quantitative studies

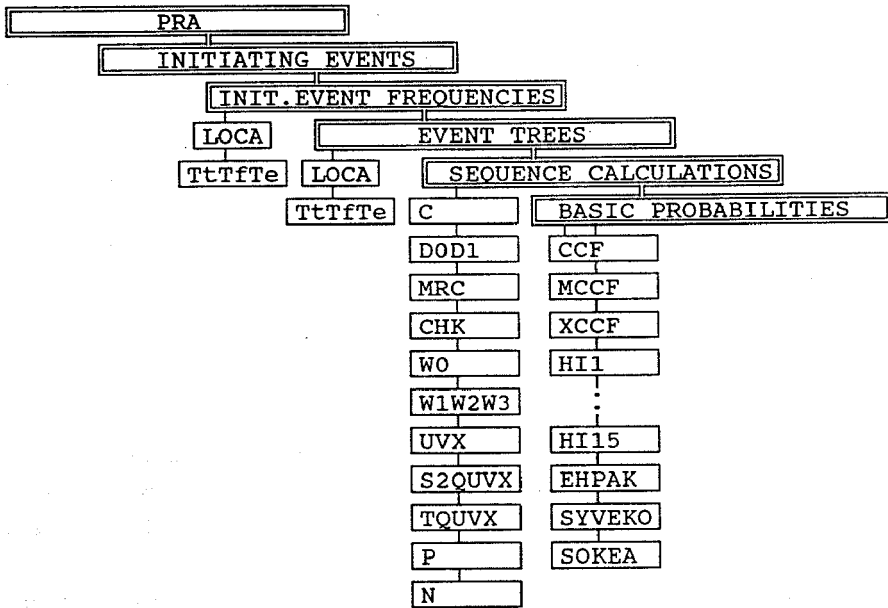
	<i>QUALITATIVE STUDY</i>	<i>QUANTITATIVE STUDY</i>
<i>Goals</i>	<ul style="list-style-type: none"> ● <i>identification</i> ● <i>description</i> 	<ul style="list-style-type: none"> ● <i>assessment of importance</i> ● <i>demonstration of impact</i> ● <i>assessment of importance</i>
<i>Treatments</i>	<ul style="list-style-type: none"> ● <i>check lists</i> ● <i>comparison between different uncertainties</i> 	<ul style="list-style-type: none"> ● <i>sensitivity studies</i> ● <i>uncertainty range propagation</i>
<i>Description of uncertainties</i>	<ul style="list-style-type: none"> ● <i>verbal</i> ● <i>classification (large/small uncertainties, over- or underestimating)</i> 	<ul style="list-style-type: none"> ● <i>numerical</i> ● <i>importance measures</i> ● <i>uncertainty distributions</i>
<i>Benefits (+) and limitations (-)</i>	<ul style="list-style-type: none"> + <i>flexible to cope with all kinds of uncertainties</i> - <i>uncertainties from various sources cannot be combined</i> 	<ul style="list-style-type: none"> + <i>provides comparable measures</i> - <i>difficult to treat modelling uncertainties</i> - <i>interpretation problems</i>

2 The qualitative study

The uncertainties were identified and classified following the hierarchy of the PRA models. The hierarchy consists of several modelling levels being characteristic to the PRA beginning from general assumptions and methodological limitations down to basic failure probabilities. The hierarchy of the modelling levels or the submodels of the PRA described in fig. 1. These submodels can be classified in logical and data models.

Logical models present how single failures or errors together can break down systems. Models mostly rest on functional schemes of the plant. Data models are methods by which probabilities of faults or errors and their combinations are estimated. Probabilities are parameters of logical models. Other quantitative models

(e.g. success criteria) were considered as assumptions behind models. Uncertainties in logical models are modelling uncertainties and in data models parametric ones.



Legend: LOCA, TtTfTe = Initiating event class frequencies and corresponding event trees: loss of coolant accidents and transients
 C, D0D1, ... , N = Categories of event sequences or safety functions, e.g. C = hydraulic scram
 CCF, ... , SOKEA = Categories of basic events, e.g. CCF = Common Cause Failures of 4-redundant components

Fig. 1 The hierarchy of the PRA's models

The identification work began with common assumptions of the PRA and continued towards more specified models and issues. In the various levels the following details were peered:

- 1) PRA
 - definition of the risk and core damage
 - limitations of PRA's methods
 - restrictions of the project
- 2) Initiating events
 - definition of the initiating event categories
 - completeness of the categories

3) Initiating event frequencies

- estimation method
- validity of the data

4) Event trees

- core melt criteria
- success criteria of the safety functions

5) Sequence quantifications

- system failure criteria
- interpretation of most important minimum cut sets and components
- modelling of dependencies

6) Basic event probabilities

- estimation method
- common cause failures (CCFs)
- human errors.

The analyst identified uncertainties by interviewing the PRA-modellers and by studying PRA-reports including the failure mode and effect analyses (FMEA) performed for the systems modelled. On the other hand, the analyst had to get familiar with the functional behaviour and the structure of the plant where the Final Safety Analysis Report (FSAR) was an important document [9]. In addition to the TVO's documents, earlier PRA studies were useful material for comparing models and assumptions. The most important reference PRA was the Swedish Forsmark 1/2 safety analysis [10].

Identified uncertainties were documented on model forms (fig. 2). A model form contains the name of the submodel, participants in the uncertainty identification team, source documentations, description of the modelling methods and a list of assumptions. If an assumption was considered to be of minor importance with respect to the associated submodel, it was reasoned here.

Significant uncertainties were analyzed further in uncertainty forms (fig. 3) which were used in the documentation of rank and impact. Significance of an uncertainty was categorized as *large*, *moderate* or *small*, and the bias as *overestimating*, *unidentified* or *underestimating*. After the preceding notes room was reserved for presentation of the quantification methods and remarks about dependencies with other uncertainties.

3 Quantitative study

The object of the quantitative study was to assess comparable uncertainty measures so that a joint impact could be evaluated. Both sensitivity calculations and

TVO I-II/PRA		MODEL FORM
Code:3-LOCA		
Author(s)/Date:JHo/24.01.89		Participants:RPH, J.Fieandt
Model:LOCA initiating event frequencies		
Modelling method:The frequency estimates of pipe leakage or break in a study of TVO's pipings/ Fieandt, Rămö, "Pipe Leakage Frequencies in TVO I/II NPP in LOCA-classes". VTT/SAH Research Report 25/87./		
ASSUMPTIONS		
Description		Reference
1) Leakage freq. is constant per pipe length and time in each class.		3-LOCA-1
2) The LOCA class of a leakage is determined according to the pipe dimension. => Large LOCA = large leakage in main steam lines		3-LOCA-2
3) Only leakages in the primary loop (inside the containment) have been considered.		3-LOCA-3
Notes:		

Fig. 2 The model form

propagations of uncertainty distributions were performed.

3.1 Sensitivity studies

In sensitivity calculations the sensitivity of the models was studied by varying uncertain parameters and assumptions. Sensitivity studies involved

- selection of reasonable calculations,
- assessments of input data and model variations,
- requantification,
- calculations with reprocessed models, and
- interpretation of results.

First a ranked list of the topics to be studies was generated. It was mainly based on the qualitative part of the uncertainty study, partially on the Fussel-Vesely importance measures of the basic events and partially on the most important minimal cut sets.

TVO I-II/PRA

UNCERTAINTY FORM

Code:3-LOCA-1

Author(s)/Date:JHo/14.03.1989

Model:LOCA initiating event frequencies

Uncertainty:Pipe leakage frequency is constant per pipe length and time in each leakage class.

Contribution	Impact: small		Bias: overestimating	
	moderate	-	underestimating	-
	large	x	not identified	x

Description of the contribution:

Pipe aging, inspections, servicing and restorations are ignored.

- The most likely leakage places are pipe joints and components in pipings. Constant existence ratio is assumed for these places.
- Data reference plants are older.
- Only frequencies per time and piping are given in most of the references.
- There is a great variation between estimates of the used references.

Quantitative treatment:

- Uncertainties will be treated in the uncertainty distribution propagation
- The uncertainty distribution for each class will be assessed according to estimates in other PRA's. See 3-LOCA-2

Dependencies with other uncertainties:

3-LOCA-2

Fig. 3 Uncertainty form

The needs for data and model variations were identified in the qualitative part of the study. In addition to the realistic variation range of model and data, also risk increase and decrease were studied for the basic event probabilities 1 and 0, respectively. This variation showed the maximum benefit gained if the basic event is removed and the maximum risk increase if it always occurs.

The calculations were simple and straightforward. Three methods were used:

- the Fussel-Vesely importance measure,
- boundary changes of a basic event, and
- model variations.

The relative impact of the change of the probability of a basic event on the core melt probability was simply estimated based on the Fussel-Vesely importance measure:

$$\frac{\Delta f(CM)}{f_{nom}(CM)} = I_{f-v}(X_i) \cdot \frac{\Delta \Pr(X_i)}{\Pr(X_i)}, \quad (1)$$

where $\Pr(X_i)$ = nominal probability of event X_i ,
 $\Delta \Pr(X_i)$ = variation of the probability of event X_i ,
 $\quad = \Pr_{varied}(X_i) - \Pr(X_i)$,
 $I_{f-v}(X_i)$ = Fussel-Vesely importance measure of event X_i on the,
 \quad nominal probability $\Pr(X_i)$,
 $\quad = \sum \Pr(\text{min cut sets containing } X_i) / \sum \Pr(\text{all min cut sets})$,
 $f_{nom}(CM)$ = the nominal frequency of Core Melt
 $f_{new}(CM)$ = the varied frequency of Core Melt
 $\Delta f(CM) = f_{new}(CM) - f_{nom}(CM)$.

The impact of uncertain phenomena included in a basic event probability was estimated by removing/adding the frequency of conservatively/optimistically estimated phenomena from the initiating event frequencies. The relative impact on the core melt frequency is estimated as the ratio of f_{new} to f_{nom} . Event trees were modified in cases where the propagation of an event sequence was uncertain. In these cases complete event trees had to be requantified.

3.2 Uncertainty range propagation

The impact of the statistical uncertainties of the basic event parameters were demonstrated by the uncertainty range propagation. In this treatment the uncertainties are described with probability distributions (fig. 4). A fractile of a distribution characterize to which confidence we believe the parameter value to be below the fractile. The 0.05- and 0.95-fractiles are often used for describing the range of uncertainty. A common measure is the error factor (EF) originating from logarithmic normal distribution. The fraction of the upper fractile and the median of a logarithmic normal distribution equals the fraction of the median and lower fractile and it is called the error factor

$$\frac{\lambda_{50}}{\lambda_{05}} = \frac{\lambda_{95}}{\lambda_{50}} = EF, \quad (2)$$

where λ_{95} = 0.95-fractile, $\Pr(\lambda_{50} \leq \lambda) = 0.95$,

λ_{50} = median,

λ_{05} = 0.05-fractile.

Uncertainty ranges were propagated by Monte Carlo simulations like in the Forsmark 1/2 safety analysis [8]. Because the TVO's fault tree models contain

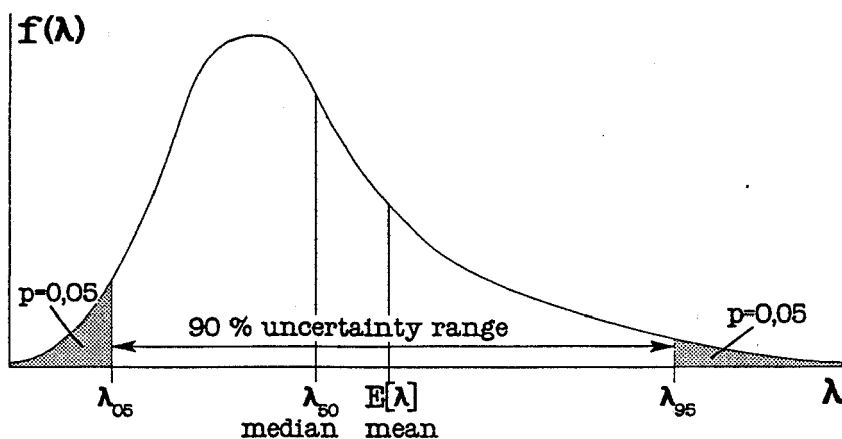


Fig. 4 Uncertainty distribution, its fractiles, mean and 90 % symmetric range

thousands of basic events, we could include only the most important minimal cut sets in the uncertainty range propagation which had the following phases:

- 1) Selection of the most important cut set in all event classes.
- 2) Coupling of state of knowledge dependent variables.
- 3) Assessment of the distributions.
- 4) Simulation runs.
- 5) Interpretation of the results.

One problem from the uncertainty quantification point of view was that the basic event probabilities were originally estimated as point values. Only in the case of the transient initiating event frequencies, a Bayesian approach had been applied. Therefore a simple strategy had to be developed in order to consistently generate uncertainty distributions for the rest of the basic event probabilities or parameters.

Firstly, a beta or lognormal distribution was selected as the uncertainty distribution type. Secondly, the mean value of the uncertainty distribution was set equal to the PRA's point value. Thirdly, the width of the distribution was subjectively defined by choosing a fixed distribution parameter (e.g. $EF = 3, 10$ or 30 for lognormal distribution).

The state of knowledge dependence was described as explicitly as possible. Only a total coupling was considered.

Simulations were performed by MONTEC-program [11] which runs in a micro-computer. We used the maximum allowed sample size, 16,000 laps, which seemed

to be enough at least for estimating the fractiles.

The modelling uncertainties studied individually by means of the sensitivity study were simulated as independent uncertainties, too. The following equation for the core melt frequency simulation was generated on the basis of the following equation

$$f(CM) = f_{nom}(CM) \cdot \prod_i E_i(\text{assumption } i_j), \quad (3)$$

where $E_i = f_{new}(\text{assumption } i_j)/f_{nom}$ is the random variable getting the values generated by the equation (1). The probability of each value of E_i is determined by the confidence $\text{Pr}(\text{assumption } i_j)$ which were assessed subjectively.

The resulting frequency in the equation (3) might be strongly biased due to the fact that the values of E_i s are dependent on each others. The dependency of importance measures on each other can be reduced by introducing the importance measures of component groups. However, in the case of complete event tree re-quantifications one should evaluate the varied event trees separately in order to properly treat their effect on the equation (3).

The aim of the simulation of the modelling uncertainties was mainly to obtain a coarse view of their impact in the total core melt frequency. As a consequence of very detailed fault and event tree models, explicit use of various minimal cut set equations would have exceeded the capacity of the simulation program without strong simplifications in the equations. Therefore, an approach based on the simulation of the equation (3) was adopted.

According to our experiences, the sensitivity studies provided the most useful information of the impact of identified uncertainties. Even though the uncertainty range propagations seem to be an attractive way to demonstrate the joint impact of the uncertainties, the difficulties to express the uncertainties coherently and exhaustively leave a lot of room for interpretation. Table 2 summarizes the benefits and limitations of the quantitative treatments of uncertainties.

4 Results

The sensitivity studies showed items in the procedures, where the assumed level of operator performance is adequate, but any reduction would lead to catastrophic increase of the core melt frequency. One example is the additional water to the Auxiliary Feed Water system (AFW) after the water in the containers has depleted. If the additional water supply always would succeed, the core melt probability

TABLE 2
Benefits and limitations of the quantitative treatments

<i>TREATMENT</i>	<i>BENEFITS</i>	<i>LIMITATIONS</i>
<i>Sensitivity studies</i>	<ul style="list-style-type: none"> + <i>simple</i> + <i>natural extension of qualitative study</i> 	<ul style="list-style-type: none"> - <i>suits only for studying single uncertainties</i> - <i>not necessarily based on estimation of upper and lower limits</i>
<i>Uncertainty range propagation</i>	<ul style="list-style-type: none"> + <i>attempts to display the joint impact of uncertainties</i> + <i>obeys the rules of probability calculus and statistics which makes it disciplinary</i> 	<ul style="list-style-type: none"> - <i>distribution is hard to understand for uncertainties are not only caused by randomness; distributions have both frequentist and subjectivist interpretation</i> - <i>difficult to model state of knowledge dependency</i>

would decrease only by 6 per cent. However, if the operators would never succeed, the core melt probability would increase by factor of several hundreds.

The estimation of the distribution of the modelling uncertainties allowed us to study the effect of conservative assumptions. Small probabilities were assessed to the normally conservative Final Safety Analysis success criteria as opposite to the success criteria used in PRA study. The resulting distribution was bimodal, since most of the distributions were discrete.

Although the results from the uncertainty range propagation showed that the uncertainty in e.g. the LOCA frequencies and in core melt after a LOCA was high — error factor even 100 — the final error factor due to statistical uncertainties for the core melt frequency was only 4. On the other hand the error factor due to modelling uncertainties was still smaller, less than 2. All in all, no major issue dominated as an uncertainty source because of the great detailness of the TVO's fault tree models.

5 Conclusions

The qualitative mapping out of the uncertainty factors turned out to be an effective way to generate a plan for an effective quantitative uncertainty analysis. At the same time it served as an internal review of the assumptions made in the PRA study. When performed for the almost finalized study it helped to correct coarse modelling errors and it forced the analysts to check the base of the assumptions and simplifications. The sensitivity studies were perhaps the most advantageous

part of the quantitative uncertainty analysis, because they allowed an individual analysis for the effect of each of the uncertainty sources identified.

The most significant uncertainties were those involved in modelling human interactions, dependencies and common cause failures (CCFs), loss of coolant accident (LOCA) frequencies and containment response. Common background for these models is the use of expert knowledge and subjective estimates due to a lack of proper data and plant experiences. The qualitative study of uncertainties gave a picture that statistical uncertainties would be negligible compared with uncertainties originated from modelling assumptions and the lack of knowledge. However, the number of those having significant impact on core melt frequency was very limited and it was possible to assess them by means of sensitivity studies. In the same context sensitivity study was used to compare alternatives of system modifications. A coarse simulation of the modelling uncertainties produced a more narrow distribution than that simulated from the statistical uncertainties.

Uncertainty study was found to be a suitable tool for a systematic and critical method of assessing uncertainties in a risk analysis. The usefulness of this study depends on the decision-maker (power company) since uncertainty study is primarily made to support decision making under uncertainty.

6 References

- [1] Reactor Safety Study: An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants, Rep. WASH-1400, NUREG-75/014, U.S. Nuclear Regulatory Commission, Office of Nuclear Regulatory Research, Washington D.C. (1975) App. II, pp. 39-47.
- [2] PRA Procedures Guide: A Guide to the Performance of Probabilistic Risk Assessments for Nuclear Power Plants, Final Report NUREG/CR-2300, U.S. Nuclear Regulatory Commission, Office of Nuclear Regulatory Research, Washington D.C. (1983) Ch. 12.
- [3] Reactor Risk Reference Document, Rep. NUREG-1150, U.S. Nuclear Regulatory Commission, Office of Nuclear Regulatory Research, Washington D.C. (1987) App. K.
- [4] Seabrook Station Probabilistic Safety Assessment, Rep. PLG-0300, Pickard, Lowe, Garrick, Inc., Rev. 2 (1983) Ch. 6 and App. A.
- [5] Oconee PRA: A Probabilistic Risk Assessment of Oconee Unit 3, Rep. NSAC-60, The Nuclear Analysis Centre, Electric Power Research Institute, California and Duke Power Company (1984) Ch. 4 and 12.3.

- [6] PÖRN, K., Analysis of Parametric Uncertainty in the PSA of Forsmark 1/2, Rep. Studsvik NP-88/46, App. G of the Forsmark 1/2 Probabilistic Safety Assessment, Vattenfall (1988) (In Swedish).
- [7] HIRSCHBERG, S., et.al., A Comparative Uncertainty and Sensitivity Analysis of an Accident Sequence, *Reliability Achievement: The Commercial Incentive*, ed. T. Aven (Proc. of the Symp. of the Society of Reliability Engineers, Scandinavian Chapter, Stavanger, Norway, 1989), Elsevier Applied Science, London (1989) 111-125.
- [8] PULKKINEN, U., KUHAOSKI, K., MANKAMO, T., Treatment of Uncertainties: Development of the Methodology fo TVO I/II PRA, Research Report VTT/SAH 14/88, Technical Research Centre of Finland, Espoo (1988) (In Finnish).
- [9] Final Safety Analysis Report (FSAR), Teollisuuden Voima Oy (TVO), Olkiluoto (1976, revised 1988) (unpublished).
- [10] Forsmark 1/2 Probabilistic Safety Assessment, Vattenfall (1988) (In Swedish).
- [11] KUHAOSKI, K., PULKKINEN, U., MONTEC Reference Manual, Research Report VTT/SAH 1/89, Technical Research Centre of Finland, Espoo (1989).

H. Pamme, RWE Energie AG, Essen

**Graphical tools for detection and modelling of time dependent
ageing behaviour in component data**

**OECD/BMU Workshop on "Special Issues of Level 1 PSA"
Köln 27.-29.5.91**

H. Pamme

RWE Energie AG, Essen

Graphical tools for detection and modelling of time dependent ageing behaviour in component data

1. Introduction

The "classical" approach within the PSA framework is to assume exponential i.e. constant ageing behaviour for basic events in fault or event tree analyses. The required statistical input data for these basic events are often derived from operating experience. These "raw data" however are mostly not analysed in depth concerning potential ageing informations. This step to check the validity of exponentiality is mostly (and often intentionally) neglected because the exponential model is easy in its application to estimate failure rates and to quantify fault or event tree structures.

This paper will describe a mainly graphical approach of life-time data analyses with the main aim to reveal non-constant ageing trends in data. This graphical approach is chosen because it allows a quick and comprehensive insight in data informations not only for the statistician but especially for the engineer as main user of statistical results.

2. Impacts of ageing effects

It is a trivial fact for engineers that a constant failure rate must be an oversimplification of the real failure behaviour of components. That becomes (at least implicitly)

obvious if engineers e.g. talk about "preventive maintenance or exchange activities", "problems with component wear out", "detection of material fatigue effects", "burn-in of electronic components before use in operation" or "increased spare parts provisioning due to observed higher part consumptions". All these problem areas would be irrelevant if the failure rates of affected parts were really constant.

Therefore the engineer using statistics (especially for safety predictions within the PSA-framework) or the involved statistician should somehow try to at least find a weak justification for exponentiality in data. The "classical" argument that the bathtub-shaped failure rate model is generally accepted but that only the flat part of the bathtub can be observed in (nuclear) operation is a weak hypothesis which can easily be disproved by many available data sets (see e.g. discussions in /1/ or /2/).

Beside the technical and economic aspects of ageing it must also be asked how a more realistic modelling of ageing behaviour might influence PSA-results. The exponential model will either over- or underestimate the real non-constant failure rate at a certain time point. The overall error in PSA-results however can be large (see e.g. /2/ for propagations of errors in fault tree quantifications).

3. Description of ageing properties

In technical applications the statistical ageing behaviour is mostly described by the failure rate $h(t) = f(t)/R(t)$ as quotient between distribution density $f(t)$ and survival function $R(t)$. $h(t) dt$ describes the conditional probability that a component which has survived until t will fail in the time interval $t+dt$.

For the exponential distribution $h(t)$ becomes a constant value.

Increasing failure rates (IFR) can formally be described by the differential condition $d h(t) / dt \geq 0$, decreasing failure rates (DFR) respectively by $d h(t) / dt \leq 0$ (see left side of figures 1 or 2).

"Trend changes" in the ageing behaviour are represented by failure rates with (at least) one local extreme in the time interval $0 < t < \infty$.

For example a bathtub-shaped failure rate can be characterized by one local minimum on $0 < t < \infty$ which describes the trend change from a strictly decreasing to an increasing failure rate.

It is the task of a statistical analysis to estimate the failure rate function (or any other measure statistically describing the informations contained in data).

4. Graphical tools for ageing analysis

The use of graphical representations in data analyses are beside the documentation function a valuable way of "communication" between statistician and engineer. Therefore it is meaningful to derive ageing informations not only by relatively abstract statistical methods (e.g. maximum-likelihood-estimation of distribution parameters and "proof" of fit by the Kolmogoroff-Smirnov-test).

This chapter shortly introduces some graphical representations which are useful to analyse the validity of or departure from the exponential model. These representations can be easily generated and allow a very quick and comprehensible assessment of the ageing informations in data.

A "naive" estimator $\hat{h}(t)$ for the failure rate could e.g. be defined by

$$\begin{aligned}\hat{h}(t) &= \hat{f}(t) / \hat{R}(t) = \hat{f}(t) / [n(t) / n] \\ &= n(t)^{-1} [n(t) - n(t + \delta t)] / \delta t ,\end{aligned}$$

where $n(t)$ denotes the number of components which survived t (with $n(0) = n$) and δt denotes a small time interval.

A graphical representation of $\hat{h}(t)$ over t however does not allow a profound analysis of the ageing trend as $\hat{h}(t)$ is an unsteady step function at each failure time t_j . Between successive failure times $\hat{h}(t)$ is constant.

Therefore other graphical representations which also allow the assessment of the ageing behaviour (and thus implicitly the failure rate) should be used for data analyses.

4.1 Empirical plot of cumulative distribution function

The empirical plot of the cumulative distribution function (CDF-plot) is widely used as one (and often only) representation of a data set (example of CDF-plot in figure 3).

Let t_1, \dots, t_n be an ordered sample of failure times of size n from a lifetime distribution $F(t)$. Then the graphical representation of $F_{\text{emp.}}(t)$

$$F_{\text{emp.}}(t) = \frac{\sum_{j=1}^n (t_j \leq t)}{n} \quad j = 1, \dots, n$$

is called empirical CDF-plot. Here " Σ " denotes the number of of failure times t_j less than or equal to t . $F_{emp.}(t)$ is a step-function with jumps over the j 'th ordered value of the sample. Very often however it is not represented as a step function, especially when the sample size is large.

The empirical CDF-plot provides an exhaustive graphical representation of a lifetime data set. For large samples $F_{emp.}(t)$ converges towards the true but unknown $F(t)$, the CDF of the underlying distribution.

The major advantages of the empirical CDF-plot are:

- the empirical CDF-plot is very easy to produce and gives an comprehensive overview concerning location and spread of data,
- it does not depend upon assumptions concerning an underlying parametric distribution model.

If the sample is sufficiently large (at least $n > 10$)

- it may provide a rough information concerning ageing classes in a data set; IFR-data will show an S-shape in the empirical CDF-plot whereas DFR-data will show a concave shape,
- it serves as a sensitive goodness-of-fit representation of $F_{emp.}(t)$ versus an assumed $F(t)$.

Some disadvantages are:

- the empirical CDF-plot does not allow a profound identification of parametric models (including the exponential distribution),

- because of the monotonically increasing behaviour of the empirical CDF-plot local variations in a data structure (e.g. trend changes in ageing) will tend to be masked,
- the informality rapidly decreases with small sample sizes.

Thus the empirical CDF-plot must be regarded as a more qualitative tool for documentation purposes of a data set and of the results of an analysis within a goodness-of-fit representation.

4.2 Probability plots

In practice it is often difficult to judge subjectively the goodness-of-fit between the (above described) empirical CDF-plot and a hypothesized distribution due to the shape of both curves. The probability plots transform this problem to a judgement concerning the deviation of a data set from a straight line. By suitably transforming (at least) the vertical scale of the empirical CDF-plot with respect to a hypothesized distribution, the data set will produce a straight line if it is a sample out of this distribution.

Within life time data analysis especially the probability plots based on the Weibull- and lognormal- distribution are widely spread.

Within these probability plots the slope of a (more or less straight) data "cloud" is a function of the shape parameter of a distribution. Thus these probability plots allow parameter estimation of the shape parameter (via the slope) and the scale parameter (via quantiles of $F_{emp.}(t)$).

4.2.1 Probability plot of the Weibull distribution

The Weibull-distribution with shape parameter β and scale parameter α has a CDF

$$F(t) = 1 - \exp[-(\alpha t)^\beta] \quad 0 \leq t \leq \infty \quad (*)$$

and a failure rate

$$h(t) = \beta \alpha^\beta t^{\beta-1} .$$

Obviously the exponential distribution is a special case of the Weibull-distribution for $\beta = 1$.

The probability plot of the Weibull-distribution is based on the following transformations:

Taking twice the logarithm of (*) provides:

$$\ln \ln (1 / (1 - F(t))) = \beta \ln t - \beta \ln (1/\alpha)$$

Let

$$y = \ln \ln (1 / (1 - F(t))) , \quad x = \ln t , \quad c = - \beta \ln (1/\alpha)$$

then the linear relation

$$y = \beta x + c$$

is obtained. Here the shape parameter β becomes the slope of the line. The time transformation $x = \ln t$ forms the horizontal axis of the probability plot.

To construct the vertical axis of the plot $F(t)$ is replaced by $F_{\text{emp.}}(t_j)$ which is e.g. estimated by

$$F_{\text{emp.}}(t_j) = (j - 0.3) / (n + 0.4) \quad j = 1, \dots, n$$

For further details (ranking theory) concerning the plotting position of $F_{\text{emp.}}(t)$ see e.g. /3/, /4/.

To estimate the scale parameter α in (*) the relation

$$F(t^{\wedge}) = 1 - \exp(-1) = 0.632$$

with $\alpha = 1 / t^{\wedge}$ is used. So an estimator of $1 / \alpha$ can be found on the logarithmic abscissa below the crossing of the data cloud (respectively the fitted line) with the horizontal axis of the 0.632-quantile. The fitting of straight lines can be done "manually" but also e.g. by using simple least squares regression.

The estimator of β can be found by defining a suitable vertical scale with a slope indication.

The Weibull-distribution is a very flexible distribution modelling IFR- (DFR-) behaviour for $\beta \geq 1$ ($\beta \leq 1$). For $\beta = 1$ the Weibull-distribution models the exponential distribution with constant failure rate α . Thus Weibull probability plots are widely spread in technical applications as they serve as a sensitive tool in discriminating between constant (exponential) and IFR-(respectively DFR-) ageing.

Convex shapes in a Weibull probability plot might indicate an underlying distribution with a trend change from DFR- to IFR-behaviour (bathtub-shaped failure rates). Concave shapes in a Weibull probability plot might indicate an underlying distribution with a trend change from IFR- to DFR-behaviour (inverse bathtub-shaped failure rates e.g. modelled by the lognormal distribution).

The major advantage of probability plots is the option for model identification by a relatively simple visual assessment whether a data set provides a linear trend in the corresponding plot. The identification is however restricted to one parametric distribution model in a plot. After identification of a suitable model the parameter estimation can be easily performed either by manually fitting a straight line or performing a regression analysis. Care must however be taken to avoid misidentifications due to the logarithmic scaling of the plots. It must be realized that the probability plots contain a graphical representation of the empirical CDF which is in general monotonically increasing. This increasing shape often "pretends" to be also linear on logarithmic paper. To reduce the risk of misidentifications especially the linearity of a data cloud at the left tail should be checked.

4.3 Mean residual life plots

The term "mean residual life" $m(t)$ describes the remaining life time expectation after survival up to the age t . Formally it can be written as the conditional expectation

$$m(t) = E [X-t \mid X > t] .$$

The mean residual life plot is achieved by plotting

$$m(t_i) = \sum_{j=i+1}^n t_j / (n-i) - t_i$$

over t_i , where t_i denotes the i -th failure with $i = 0, 1, \dots, n-1$. $m(0)$ is the life expectation of a new component. For further details see e.g. /5/ and /6/.

For the exponential distribution $m(t)$ is constant with $m(t) = 1/\alpha$ (α as failure rate of the exponential distribution). Thus the graphical representation of exponential data would produce a more or less horizontal plot. Increasing failure rates lead to a decreasing mean residual life whereas decreasing failure rates lead to an increasing mean residual life (see simplified correlation between failure rate and mean residual life in figure 1).

Bathtub-shaped failure rates show a first increasing then decreasing mean residual life function. Thus the data trend in a mean residual life plot is also a sensitive indication concerning the deviation from a constant ageing behaviour.

4.4 TTT-plots

Since Barlow and Campo /7/ presented their publication on the total time on test (TTT) transform and the empirical TTT-plot the TTT-concept has proven to be a valuable graphical tool in data analysis and model identification (especially departures from exponentiality).

Some introductory aspects to the TTT-transforms and plots (for details see e.g. /7/ or /8/) shall be mentioned here:

The TTT-transform of a CDF $F(t)$ is defined by

$$H^{-1}(u) = \int_0^{F^{-1}(u)} [1 - F(t)] dt \quad 0 \leq u \leq 1 .$$

$F^{-1}(u)$ means the inverse function of $u = F(t)$.

The expectation of a random lifetime X can be written as

$$E(X) = H^{-1}(1) .$$

The quotient

$$H(u) = H^{-1}(u) / H^{-1}(1)$$

is called scaled TTT-transform with $H(u) = 0$ for $u = 0$ and $H(u) = 1$ for $u = 1$.

The scaled TTT-transform of the exponential distribution provides $H(u) = u$. Thus the exponential distribution can graphically be represented as diagonal in a unit square (so called TTT-plots) of $H(u)$ over u (see figure 2).

The empiric counterpart of $H(u)$ allows the representation of data in a TTT-plot (for details see e.g. /8/). For a failure time t_j the empirical TTT-transform is defined by

$$U_j = \frac{\sum_{m=1}^j t_m + (n - j) t_j}{\sum_{m=1}^n t_m}$$

with $j = 1, \dots, n$ and $U_0 = 0, U_1 = 1$.

The correlation between the failure rate $h(t)$ and the TTT-transform is given by

$$\left. \frac{d}{du} H^{-1}_F(u) \right|_{u = F(t)} = 1 / h(t) \quad (**)$$

Thus the empirical TTT-plot (plotting U_j over j/n) can be used as a sensitive graphical instrument to identify deviations from a constant failure rate. TTT-plots are scale

invariant, monotonically increasing plots in a unit square with the diagonal representing the scaled TTT-transform of the exponential distribution family. Due to relation (**) TTT-plots above (below) the diagonal in the unit square indicate "increasing (decreasing) ageing properties" in a lifetime data set (see figure 2, for more details see again /7/ or /8/).

A bathtub-shaped failure rate is represented by a TTT-transform once crossing the diagonal in the unit square from below and having exactly one turning point on $0 < u < 1$.

5. Application to empirical data

The use of the above mentioned graphical tools shall be demonstrated at a set of data reflecting failure times of a (sufficiently homogeneous) group of condensate pumps (sample size $n = 32$). The first data set provides the times of the first external leakage, the second data set the survival times after this first failure until the next external leakage occurred. The empirical distribution function for both data sets is shown in figure 3.

It shall be analysed whether the life expectation or the ageing behaviour after the first repair is (statistically) the same as at the start of operation after the delivery from the manufacturer.

The scale-invariant TTT-plot for both data sets is shown in figure 4. The data of the first leakages provide a slight IFR-trend due to the nearly concave TTT-plot.

The data set of the survival times crosses the diagonal several times and stays then closely to the diagonal. An exponential behaviour for the survival data however seems to

be an incorrect assumption as the TTT-plot significantly lies above the diagonal for $H(x) < 0.3$. Thus the crossing with the diagonal from below and the change from a convex slope to a following IFR-behaviour might indicate a trend change from a nearly constant DFR-behaviour to an approximately IFR-ageing .

The use of any classical distribution (not especially discussed in this paper) such as Weibull, gamma or lognormal does not provide an acceptable fit to the relative survival data. Especially exponentiality as potential conclusion from the TTT-plot should be excluded due to graphical arguments. This is shown in figure 5 in Weibull-probability plots. The data provide a convex curve.

Therefore it is interesting to derive some more graphical results.

Figure 6 shows the mean residual life plots for both data sets.

This figure shows a decreasing trend of the mean residual life. So the plot would suggest an IFR-behaviour. The expectation of life after first repair $m(0) = 3114.22$ gives an indication that the life expectation has decreased after the first failure compared to a new component with $m(0) = 5016.28$.

5.2 Interpretation of results

A potential interpretation of the revealed non-constant failure rate from an engineering and statistical point of view is that some repairs of leakages did not provide a state of "as good as new" for the pumps. These pumps failed in an "infant mortality phase due to bad repair" shortly after

restart of operation providing a DFR-trend of the failure rate. Those pumps which were repaired successfully returned to their "inherent" ageing behaviour which is of IFR-character.

6. Summary and conclusion

The exponential ageing model plays a dominant statistical role in the PSA-framework. The experience with many data analyses however shows that the arbitrary and uncontrolled acceptance of this model might produce strongly biased or even meaningless statistical results (e.g. in fault tree quantifications). Therefore this paper has recommended some graphical "checks" which as well provide a data documentation and a validity assessment concerning constant ageing. The practical construction and interpretation of these graphical representations do not require a large amount of statistical theory. Therefore they can serve at least as basic analyses for further investigations and decisions if significant ageing properties were detected.

RWE intends to incorporate these graphical analysis options within a statistical software package for data analyses. These tools shall support the data analyses in PSA-studies and shall also serve as a decision support concerning technical or logistic activities.

7. Literature

- /1/ Safety aspects of nuclear power plant ageing
IAEA-TECDOC-540, Vienna 1990
- /2/ Vesely W.E.
Risk evaluations of aging phenomena: the linear
aging reliability model and extensions
NUREG/CR-4769, April 1987
- /3/ Lawless, J.F.
Statistical Models and Methods for Lifetime Data
Wiley, New York, 1977
- /4/ Härtler, G.
Statistische Methoden für die Zuverlässigkeitsanalyse
VEB Verlag Technik, Berlin, 1983
- /5/ Hall, W.J., Wellner, J.A.
Mean residual life
in: Statistics and Related Topics
Csörgö, M. et al. (Eds.)
North-Holland Publishing Company, 1981
- /6/ Guess, F., Hollander, M. Proschan, F.
Testing exponentiality versus a trend change
in mean residual life
The Annals of Statistics, Vol. 11,
No. 1, S. 1388-1398, 1986
- /7/ Barlow R.E., Campo R.
Total time on test processes and applications
to failure data analysis
in: Reliability and Fault Tree Analysis
SIAM, Philadelphia, S.451-481
- /8/ Bergman, B., Klefsjö, B.
The Total Time on Test Concept and Its Use in
Reliability Theory
Operations Research, Vol. 32, Nr. 3, 1984

8. Notation & Nomenclature

X	non-negative continuous random variable
$f(t)$	probability density function
$F(t)$	cumulative distribution function
$R(t)$	survival function, $1 - F(t)$
$h(t)$	$f(t)/R(t)$ failure (hazard) rate
$H^{-1}(u)$	total time on test transform of $F(t)$
t_1, t_2, \dots, t_n	ordered sample of size n
DFR (IFR)	decreasing (increasing) failure rate
\ln	natural logarithm
$\exp[t]$	exponential function e^t

Figure 1

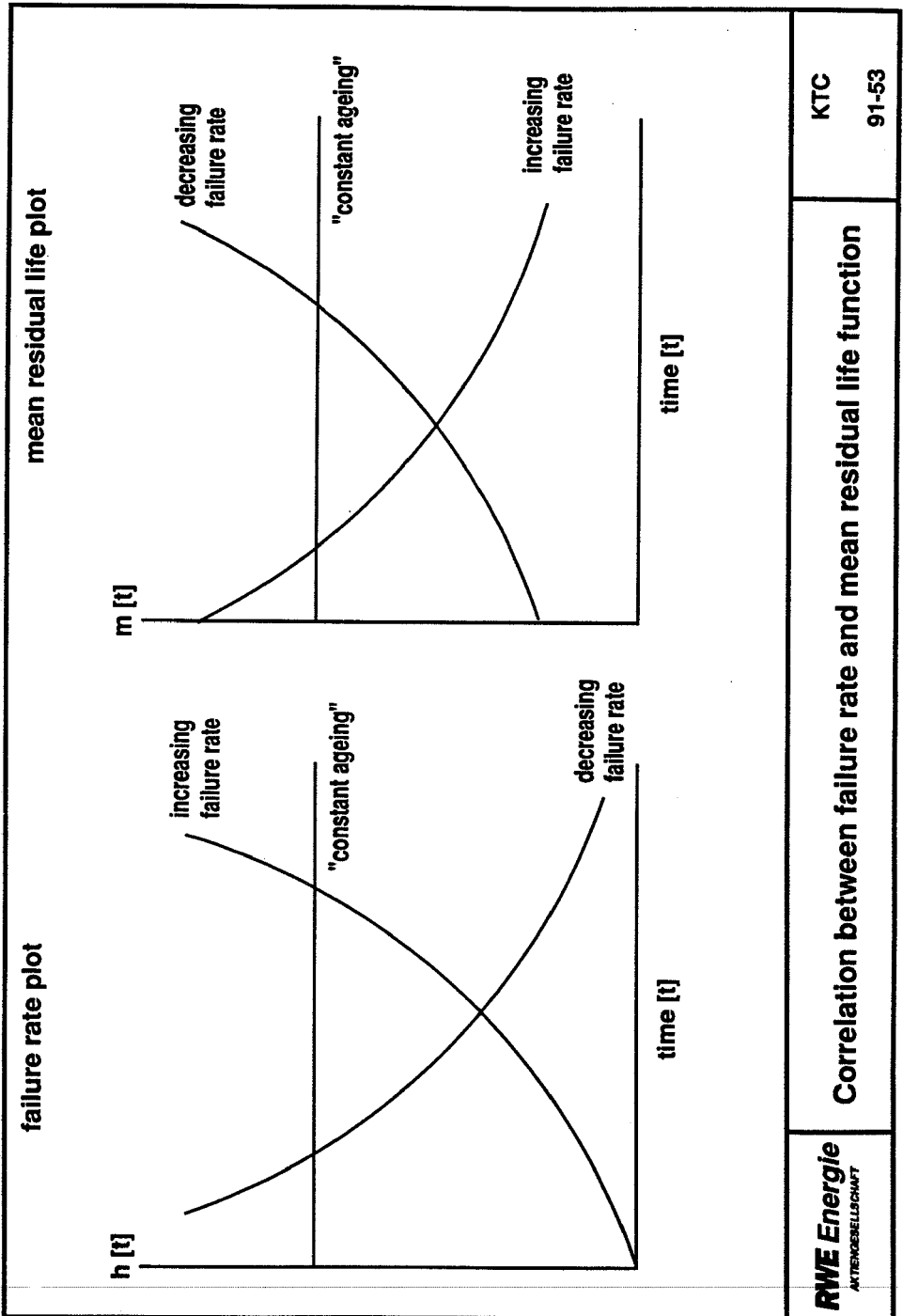


Figure 2

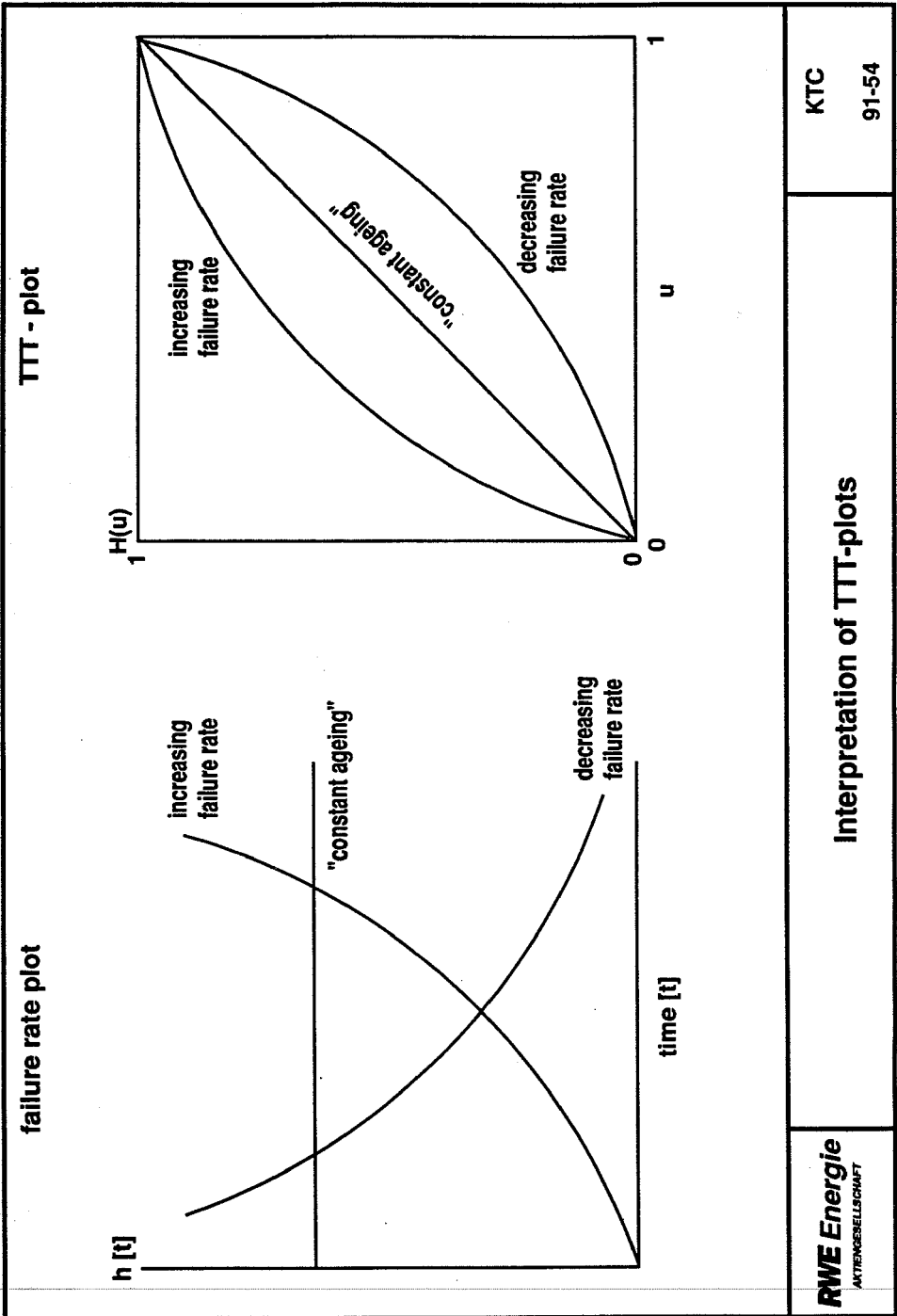


Figure 3

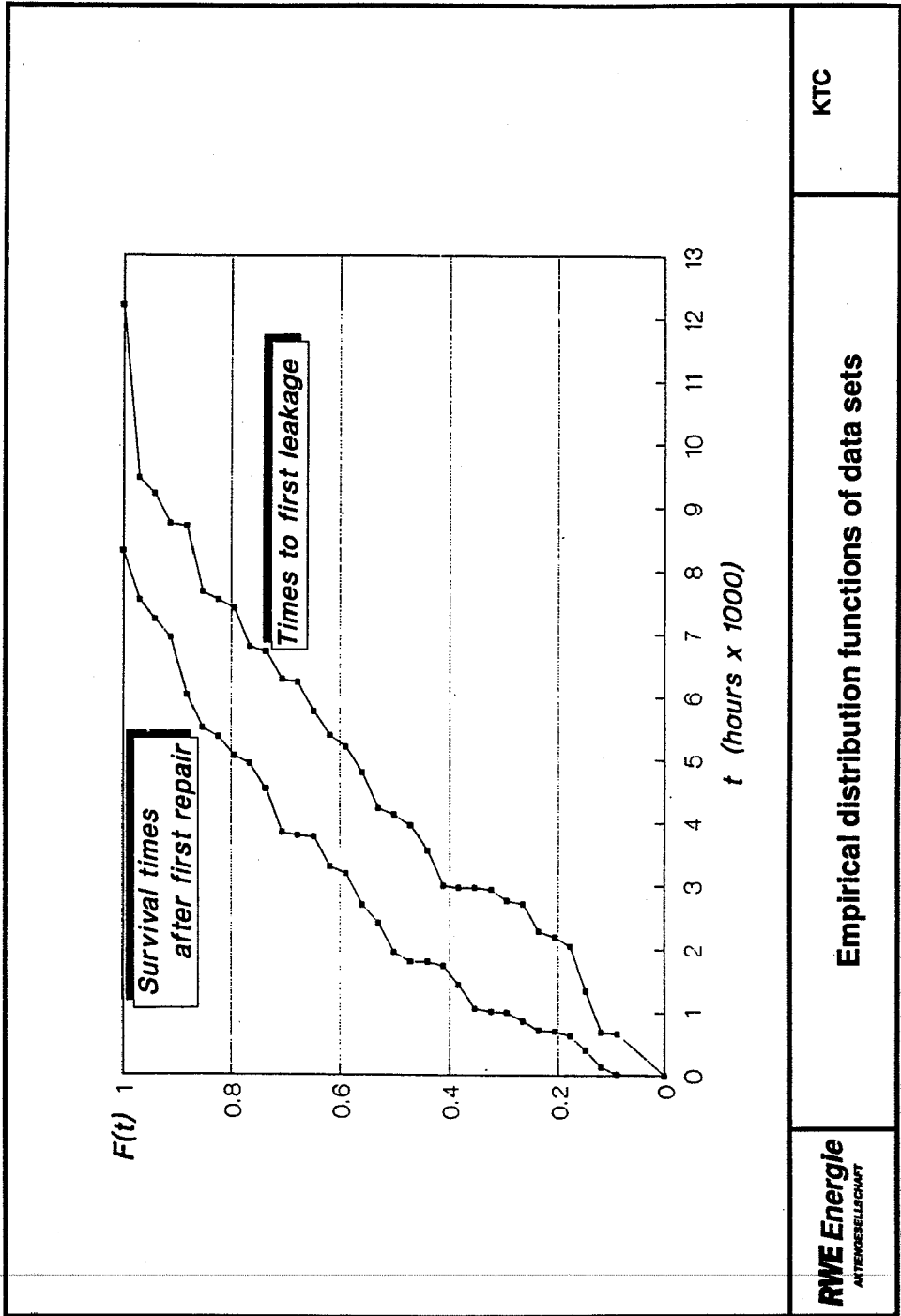


Figure 4

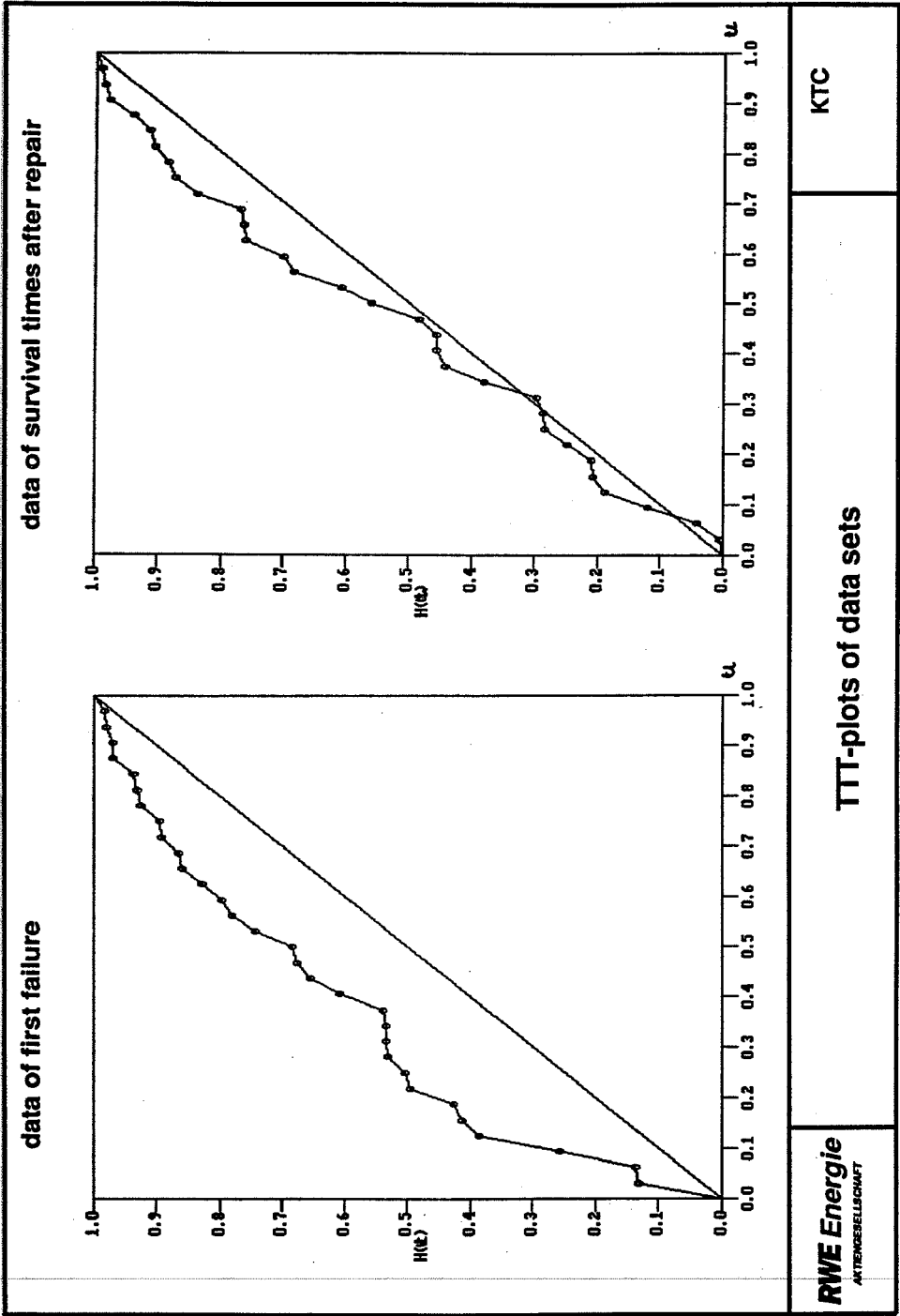
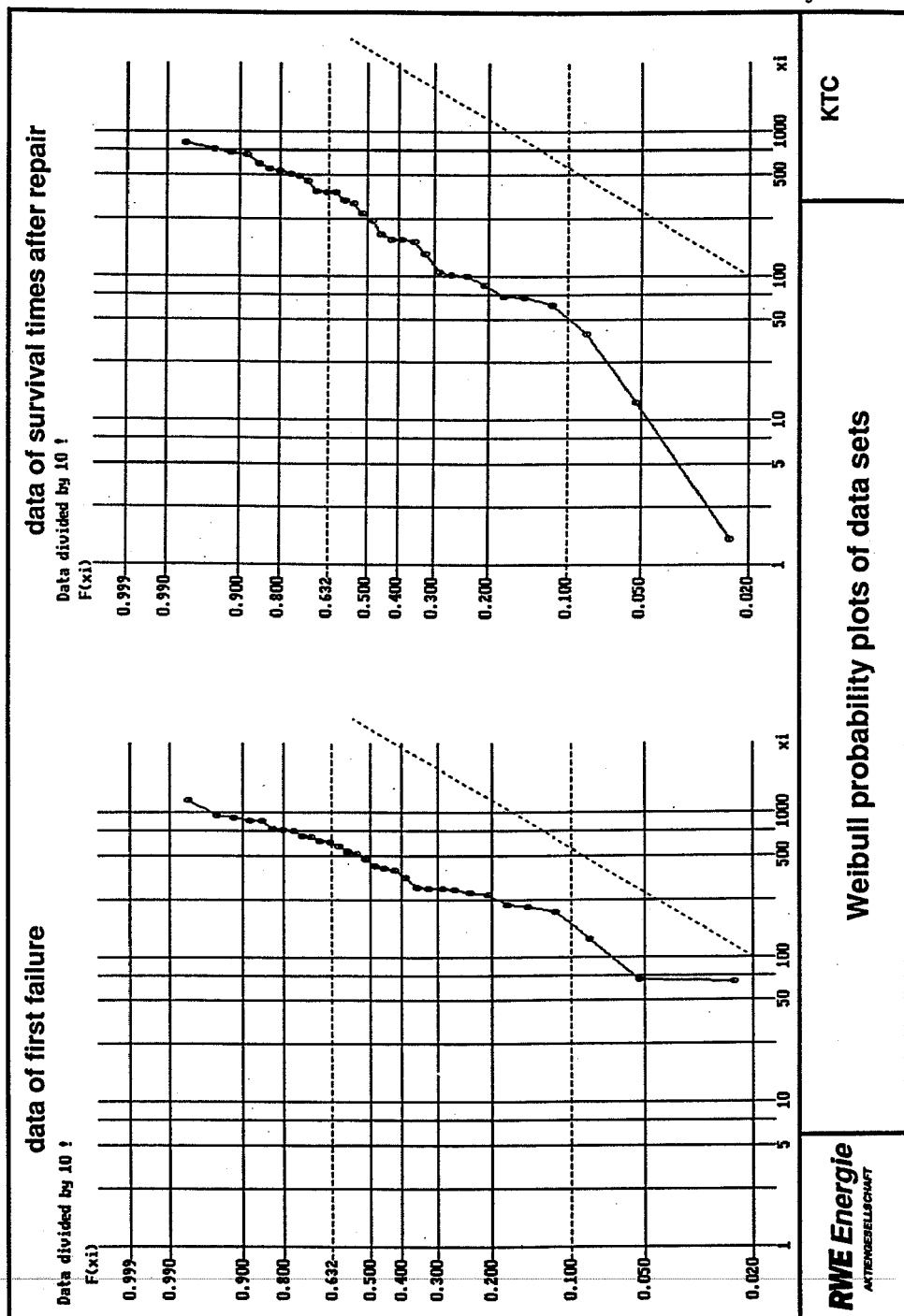


Figure 5



SKI

STATENS KÄRNKRAFTINSPEKTION
Swedish Nuclear Power Inspectorate

SKI/UA PROMEMORIA NR. 91:3

SKI/UA-PM 91:3
NKS/SIK-1 (91)6

April 2, 1991

Gunnar Johanson, Swedish Nuclear Power Inspectorate (Consultant)

DRAFT REPORT FOR COMMENTS:

NKS/SIK-1 PROJECT REPORT:

TIME DEPENDENCIES IN LPSA MODELS

The Nordic research project "Safety Evaluation, NKS/SIK-1" (1990-93),
Project report NKS/SIK-1 (91)6.

Distribution/DRAFT FOR COMMENTS:

Bo Litwång SKI, Lennart Carlsson SKI, Christer Karlsson SKI, Jan Holmberg VTT/SÄH, Kari Laakso VTT/SÄH, J Sandstedt
Relcon, U BERG Relcon, Ilkka Niemelä STUK, Lars Gunsell Vattenfall, Yngve Flodin Vattenfall, Tomas Eliasson Sydkraft,
Mauritz Gärdinge OKG, Mikael Landelius OKG, Kurt Pörn Studsvik, Tuomas Mankamo Avaplan.

ABSTRACT:

The objectives with this report are to describe the basic principles of time dependent modelling in LPSA. Practical recommendations has been generated on what to include in the models and how to avoid unnecessary model expansions. It is possible that detailed time dependency analyses require too much resources to be included in the standard PSA. Some of which are typical for Living PSA applications and must be included. It is foreseen that a LPSA model must treat time dependencies in a much more complete way than a conventional PSA model used for risk verification. Many important aspects on plant risk are time dependent. If the LPSA failure models are compatible with the operating experience this leads to a greater confidence of PSA results.

CONTENT:

ABSTRACT:	i
1 INTRODUCTION	1
2 TIME DEPENDENT FEATURES IN LPSA MODELS	1
2.1 <u>Time dependent failure rates.</u>	1
2.2 <u>Time dependent component unavailabilities.</u>	4
2.3 <u>Time dependent system unavailability (CCF models).</u>	8
2.4 <u>Time dependencies of accident sequences</u>	10
2.5 <u>The increase of statistical evidence.</u>	11
2.6 <u>Time dependent plant status knowledge.</u>	11
3 SUMMARY AND RECOMMENDATIONS	11 12
REFERENCES:	14

TIME DEPENDENCIES IN LPSA MODELS

1 INTRODUCTION

The objectives with this report are to describe the basic principles of time dependent modelling in LPSA. Further, practical recommendations has been generated on what to include in the models and how to avoid unnecessary model expansions.

A LPSA model must treat time dependencies in a much more complete way than a conventional PSA model used for risk verification. Many important aspects on plant risk are time dependent therefore is it necessary to include these aspects when developing the LPSA model to enable a more flexible use. If the failure models are compatible with the operating experience this leads to a greater confidence of PSA results.

The recommendations in this report discuss different development aspects, for models and codes, for further development in the SIK-1 project.

2 TIME DEPENDENT FEATURES IN LPSA MODELS

The basic features in LPSA models has been generated through a survey of a number of references dealing with this subject. The overall outline for this section is based on work done within the RAS-470 project (ref. 1). The outline has been expanded to take additional time related aspects into account. In Table 1 the overall outline is summarized.

2.1 Time dependent failure rates.

Time dependent failure rates has effects on the component failure probability and initiating event frequency.

Usually the time dependency of failure rates of individual components does not have a very strong impact on the core damage frequency, but the failure rates of a set of components may increase simultaneously which might strongly affect the final result.

The ageing mechanism (and the learning mechanism) can be monitored for components with short mean time between failures. Other components, e.g. piping, have rather long life length is much harder or impossible to monitor because the operational failure event experience is missing.

Different mechanisms can be identified in operational data analysis the main problem is to identify deteriorating components as early as possible.

Ageing.

The ageing process is slow (years) compared to other types of time dependencies in the LPSA. Operating experience and data trend analysis must be used to identify the failure mechanism. It is not necessary to treat this in the LPSA other than to give priorities to

Table 1 Time dependent categories.

TIME DEPENDENCY CATEGORY (ref. 1)	MODEL FEATURES	LPSA TREATMENT	PARAMETRIC MODEL /APPROACH	REMARKS
<u>Time dependent failure rates.</u> <ul style="list-style-type: none">- effects on the component failure probability and initiating event frequency- different for components with short and long life lengths- different learning mechanisms	1. Ageing.	The ageing process is slow (years) compared to other dependencies below.	.	Operating experience and data trend analysis. Lead diesel. Indicator and integrated use.
	2. Learning.	Considered for initiating events.	Exclusion of first year experience or 1-book methodology.	1-book methodology can also be used for other purposes.
<u>Time dependent component unavailabilities.</u> <ul style="list-style-type: none">- not always modelled in PSAs- effects also on CCF-probabilities- models rather complicated	1. Test interval dependencies.	Included in component model.	$q_0 + \lambda_{sb} \cdot t$ q_0 = Time independent start unavail. λ_{sb} = Stand-by fail. rate	Improved component models. T-book III data
	2. Test arrangement dependencies.	Test arrangement modelled in fault trees as a failure to by-pass the test arrangement in the case of a demand.	q_0 = The test override unavail. Prob. that the by-pass of the test arrangement fails in the case of a demand during the test.	In the case of system reconfiguration for test. Improved component models.
	3. Latent failures not revealed in tests.	Test efficiency can be expressed as a fraction of testable failures.	$q(t) = a_{eff}(q_0 + \lambda_{sb}(1-TD))$ a_{eff} = Test efficiency	No data for test efficiency modelling. RAS-450 RPC 89-69.
	4. Repair unavailabilities (critical failures).	Included in component model		Latent critical failures revealed at test and Monitored critical failures.
	5. Test introduced failures	Introduce a spec. failure mode	p_{tr} = The probability for a test caused failure.	
	6. Stand-by equipment operational failures.	Specification of mission time.	$\lambda_d \cdot t_m$ λ_d = Op. fail. rate t_m = mission time	
	7. Normally operating (non stand-by) equipment unavailabilities.	Monitored components treated as repairable.	$\lambda_d \cdot mtr$	Batteries, busbars etc.
<u>Time dependent system unavailability (CCF models).</u> <ul style="list-style-type: none">- not modelled in PSAs- requires code development	1. Test interval dependencies in CCF models.		See F1/2.	Three different CCF models suggested in PK-168-90. The problem is to avoid conservatism and to allow non symmetric test arrangements.
	2. Component status dependent CCF models.	Using quadruple model even if only three trains in operation ?		Factor 4 conservative error à la Gussell when doing nothing
	3. Test arrangement dependencies.	Test schemes represented in component models.	Time to first test.	
	4. Repair unavailabilities (non critical failures) according to LCO.	LCO represented in system models.	LCO represented with not logic in system models.	

TIME DEPENDENCY CATEGORY (ref. 1)	MODEL FEATURES	LPSA TREATMENT	PARAMETRIC MODEL /APPROACH	REMARKS
<u>Time dependencies of accident sequences</u> - effect both on level 1 and 2 PSA results - one of the uncertainties of PSA - different models exist - treatment with sensitivity studies	1. Time dependent success criteria.	Fased mission modelling.		Development area. Worst case event tree models (not TD). Long term success criterias as a function of residual heat.
	2. Timing of emergency system operation.	System timing modelled in ET. Sequence mission time affect component models.		Development area. Timing of recovery actions.
	3. Timing of operator actions.	Improved ET.		Development area. One approach is to model HI on ET level.
	4. Time dependence of operator error probabilities.	HI time windows.		
	5. Time dependent physical phenomena.	Residual heat dependencies.		
<u>The increase of statistical evidence.</u> - problem of living PSA - possibility to take several factors into account in PSA failure data	1. Time dependent operating experience evaluation. Time dependent trend follow up.	Importance or sensitivity analysis (ageing, learning).		Development area.
	2. Time dependent uncertainty estimate.	Decision under uncertainty. The process is slow (years) compared to other time dependencies.		As time dependent as the data source.
<u>Time dependent plant status knowledge.</u> - requires code development	1. Test interval dependencies.	Plant status model manipulator.	System or component specific setting of base line risk.	Development area. Model manipulator to introduce extra tests and real demands according to operations.
	2. Absolute representation of status information.		Absolute setting (0.1) of unavailable equipment.	Development area.

which components or set of components to monitor closely.

Differences in accumulated operational time, e.g. lead diesel, is one way to get early indications of a deteriorating trend.

Learning.

The learning process must in some cases be considered to eliminate conservatism in failure data or initiating events frequencies.

This has been the case for initiating event frequencies, e.g. in swedish PSAs exclusion of first year experience.

In a paper by J.K. Vaurio 1986 (ref. 2) an application example is given concerning learning from reactor accidents. In the I-book (ref. 3) initiating event data book, a baysian approach to handle the learning process has been developed based on the concept suggested by Vaurio. The I-book methodology can also be used for other purposes.

2.2 Time dependent component unavailabilities.

The modelling of time dependencies must not be too complicated and must be compatible with the available operating experience and failure data. The models depends on operational procedures (operation, testing, repair, maintenance) which also constitute a kind of time dependency.

Time dependencies has not always been modelled in PSAs the unavailability of stand-by components has usually been evaluated as mean unavailabilities. One important aspect on LPSA is the need to be exact (calendar) time dependent.

Time dependent component unavailabilities effects also on CCF-probabilities, this is further discussed in section 2.3.

One large problem are that time dependent models can become rather complicated one objective with this work is also to show how to simplify the models.

As a initial step in this model survey time dependent modeling in the Frantic code (ref. 4), component modeling for optimization of technical specifications (ref. 5) and the user manual for the Fault Tree code Risk Spectrum (ref. 6) has been studied. In Table 2 the time dependent modelling in these reports are summarized.

Test interval dependencies.

Test interval dependencies, Figure 1, are usually included in the component model which is even mean unavailability models are test interval dependent.

Table 2 Survey of component models.

Component models		Frankle	RAS-450 VTT 860	Risk spectrum/STUR PSA	SK-I TFSA recommendation
Constant unavailability components		$q = q_d$		$Q = q_d$	$Q = q_d$
Non-repairable components		$q(t) = 1 - \exp(-\lambda t) = \lambda t$		In operation, non-repairable $q(t) = q_d + 1 - \exp(-\lambda_d t) = q_d + \lambda_d t$ In operation defined mission time (t_m) $q(t) = q_d + 1 - \exp(-\lambda_d t_m) = q_d + \lambda_d t_m$	In operation, non-repairable $q(t) = q_d + 1 - \exp(-\lambda_d t)$ In operation defined mission time (t_m) $q(t) = q_d + 1 - \exp(-\lambda_d t_m)$
Monitored components		$Q = \lambda t / p_f (1 + \lambda t / p_f) = \lambda t / p_f$	$Q = \lambda t / p_f$ Monitored critical faults $T_r = T_{rw} + T_{ra}$ Monitored non-critical faults $T_r = T_{ra}$	In operation, repairable $Q = \lambda_d t / p_f (1 + \lambda_d t / p_f) = \lambda_d t / p_f$ $q(t) = \lambda_d t / p_f (1 + \lambda_d t / p_f) (1 - \exp(-\lambda_d t / p_f))$	For monitored critical faults $Q = \lambda t / p_f (1 + \lambda t / p_f) = \lambda t / p_f$ and $T_r = T_{rw} + T_{ra}$ for monitored non-critical faults are the same model used taking into account LCO and $T_r = T_{ra}$
Periodically tested components	Failure between test	$q(t) = \lambda t$ for the first test $q(t) = \lambda(t - \tau)$ for test $n+1$, $\tau_p > 1$ (τ_p is the time for test n (the previous test)) $Q_f = \lambda t / 2$	$Q = q_d / C + \lambda_d C / 2$	$q(t) = q_d + 1 - \exp(-\lambda_d t / C)$ $q(t) = q_d + \lambda_d t / C$	$q(t) = q_d + 1 - \exp(-\lambda_d t / C)$ $q(t) = q_d + \lambda_d t / C$
	Test period unavail.	$q_r = p_f + (1 - p_f) q_d + (1 - p_f) (1 - q_d) Q_f$ (1) p_f = The probability for a test caused failure. (2) q_d = The test override unavail. Prob. that the by-pass of the test arrangement fails in the case of a demand during the test. (3) Unavail due to failure between test $Q_f = q_d / 2$	$Q = 1 \times t / t_i$ $t_i = q_d$		Q_f must be considered if the test procedure requires so. $Q_f = (q_d + (1 - q_d)(q_d + \lambda_d p_f / 2) \tau / t_i)$ q_f (the probability for a test caused failure) has not been considered, have the same impact on the model as q_d
Repair period unavail.	Repair period unavail.	$q_r = p_f + (1 - p_f) Q_f + (1 - p_f) (1 - Q_f) \lambda / 2$ (1) p_f = The probability for a test caused failure. (2) Unavail due to failure between test (3) A failure during the repair period $Q_r = q_d / t_i$	$Q(t) = (q_d / C + \lambda_d C / 2) / t_i$ Latent critical faults $T_r = T_{rw} + T_{ra}$ Latent non-critical faults $T_r = T_{ra}$	$Q(t) = \lambda_d t / p_f$ According to Retiree manual, are probably correct in the code. $Q(t) = (q_d + \lambda_d p_f / 2) / t_i$	For latent critical faults $Q_r = (q_d + \lambda_d p_f / 2) / t_i$ and $T_r = T_{rw} + T_{ra}$ Failure during repair period neglected. For latent non-critical faults are the same model used taking into account LCO and $T_r = T_{ra}$
	Unstable stand-by failures				$q(t) = q_d + 1 - \exp(-\lambda_d t / C)$ all. $q(t) = q_d + \lambda_d t / C$ $q_{eff} = \text{Test efficiency}$

The recommended component model are:

$$q(t) = q_0 + (1 - \exp(-\lambda_{sb} * t))$$

where

q_0 Time independent start unavailability.

λ_{sb} Stand-by failure rate.

Improved component modelling, using this model, is now possible by using the new T-book III data (ref. 7)

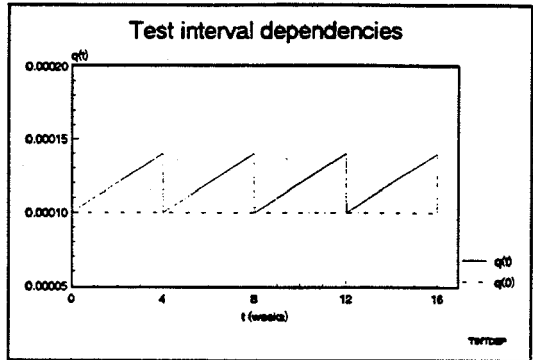


Figure 1 Test interval dependencies.

Test arrangement dependencies.

Test arrangement can be modelled in component models as a failure to by-pass the test arrangement in the case of a demand.

q_{io} The test override unavailability. The probability that the by-pass of the test arrangement fails in the case of a demand during the test.

If the tested system are reconfigured this parameter must be considered. As shown in (ref. 8) the test influence on systems and components are important and significant. The survey of test influence show that a number of test need reconfiguration with hand maneuvered test sequences that disallow automatic actuation of system or train function.

The test duration come into play as a contributing parameter in the case of reconfiguration of the tested component/train.

Handling of these aspects requires both model and code development. Available fault tree codes do not allow modelling of test override unavailability in a acceptable way. As shown in reference 8 the analysis work to identify the test influence are fairly large.

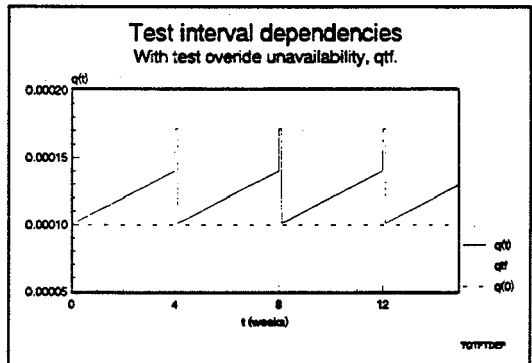


Figure 2 Test override unavailability

Latent failures not revealed at test.

Test efficiency can be expressed as a fraction of testable failures.

$$q(t) \approx a_{\text{eff}}(q_0 + \lambda_{sb}(t - TD))$$

a_{eff} Test efficiency

No data are available for test efficiency modelling (ref. 9), further analysis in the Diesel Generator pilot project (ref. 10) may result in test efficiency data for diesel-generators.

The time independent start unavailability, q_0 , presented in the T-book can be interpreted as partly an average measure of test efficiency.

Repair unavailabilities (critical failures).

Repair unavailabilities for critical failures are included in the basic component models, i.e. latent critical failures revealed at test and monitored critical failures (Risk spectrum will be corrected).

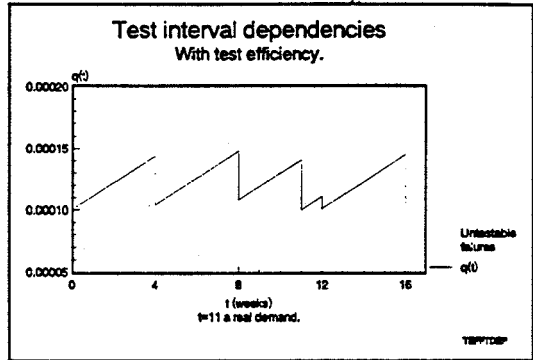


Figure 3 Test efficiency dependencies

Test introduced failures.

Model development with introduction of a specific failure mode

p_{tr} The probability for a test caused failure.

This failure mode have almost the same impact on the model as q_0 and may be excluded.?

Stand-by equipment operational failures.

Stand-by equipment operational failures can be treated as non-repairable failures with a specified mission time.

$$q(t) = 1 - \exp(-\lambda_d * t_m)$$

λ_d Operational failure rate

t_m Mission time

Normally operating (non stand-by) equipment unavailabilities and monitored stand by components.

Monitored components treated as repairable are included in the basic component models.

$$q(t) = 1 - \exp(-\lambda_d * mttr)$$

Batteries, busbars etc.

2.3 Time dependent system unavailability (CCF models).

Time dependent system unavailabilities (CCF models) are not modelled in conventional PSAs. The stand-by system unavailabilities are dependent on test arrangements this model aspect requires code development.

Test interval dependencies in CCF models.

Three different CCF models are suggested in Vattenfall Report PK-168/90 (ref. 11), Table 3. The problem is to avoid conservatism and to allow non symmetric test arrangements. Model 3 allow non-symmetric test arrangements but are not possible to use in the available fault tree codes. In the report "Optimization of test interval for 327 testing at O3" (ref. 12) a model approach is suggested which give a correct estimate of the mean unavailability for a time period considerably longer than the test interval. But for certain time points the unavailability estimate can be incorrect.

Table 3 Three CCF models.

Time dependent CCF-models (ref. PK-168/90)

CCF model	Parametric description	Features
<u>Arithmetic average model</u>	$Q_{CCF2} = (q_a(t) + q_b(t))(1/2)\beta$ $Q_{CCF3} = (q_a(t) + q_b(t) + q_c(t))(1/3)\beta\gamma$ $Q_{CCF4} = (q_a(t) + q_b(t) + q_c(t) + q_d(t))(1/4)\beta\gamma\delta$ Possible to model explicit in fault tree. This model is used in F1/2 and R1 PSA.	The model behave OK and can be used with small variations in failure data, but not when reaching extreme values such as 0 or 1. If one component fails the model become time independent (constant), as a result of the dominating contribution of the failed component.
<u>Geometric average model</u>	$Q_{CCF2} = (q_a(t) + q_b(t))(1/Q_{ind1})\beta$ $Q_{CCF3} = (q_a(t) + q_b(t) + q_c(t))(1/Q_{ind2})\beta\gamma$ $Q_{CCF4} = (q_a(t) + q_b(t) + q_c(t) + q_d(t))(1/Q_{ind3})\beta\gamma\delta$ Possible to model explicit in fault tree.	The model has a unstable behavior, it can be used with small variations in failure data, but not when reaching extreme values such as 0 or 1. If one component fails the result are approximately a factor of 10 higher compared to the other two models.
<u>Minimum common cause model</u>	$Q_{CCF2} = \min(q_a(t), q_b(t))\beta$ $Q_{CCF3} = \min(q_a(t), q_b(t), q_c(t))\beta\gamma$ $Q_{CCF4} = \min(q_a(t), q_b(t), q_c(t), q_d(t))\beta\gamma\delta$ Not possible to model explicit in fault tree, requires code development.	This model is probably most appropriate to reflect the reality. The model has a acceptable behavior, it can be used with both small and large variations in failure data. The results are always lower than the other two models.

Component status dependent CCF models.

To represent a failure situation correctly the CCF model must allow that one or more components are unavailable. (Using quadruple model even if only three trains in operation give a factor 4 conservative error.) The only model studied here that allow this in a correct manner is model 3 in reference 11.

Test arrangement dependencies.

Test arrangements and test schemes can easily be represented by introducing time to first test in the component model.

Repair unavailabilities (non critical failures) according to LCO.

Repair unavailabilities generated from non critical failures, Table 4, must be considered in accordance to Limiting Conditions for Operation (LCO). LCO can be represented in system fault tree models with not logic. Table 4 give definitions of functional failure modes of stand-by component (ref. 13).

Table 4 Failure criticality categorization.

Revealability Component state at fault occurrence /detection	Functional consequence	
	Critical Prevent component operation directly	Non-critical Prevent operation only under active repair
Failure during operation Normally operating	Failure to operate, critical (FC)	Failure during operation, non-critical (FN) Repairable according to LCO
Failure during operation Mission period operation	Failure to operate, critical (FC)	(Non repairable in LPSA model)
Monitored failure in stand-by, failure detected via instrumentation, walkarounds, etc	Monitored critical (MC)	Monitored non-critical (MN). Repairable according to LCO
Latent failure in stand-by, detected via test	Testable latent critical (LC)	Latent non-critical (LN) Repairable according to LCO
Latent failure in stand-by, detected only at real demands	Un-testable latent critical (UC)	(Non repairable in LPSA model)
Failure (in stand-by) introduced at test	Test related, critical (TC)	(Non repairable in LPSA model)

2.4 Time dependencies of accident sequences

Currently worst case event tree models, not time dependent, are presented in the PSAs. Treatment of success criteria as a time dependent function of residual heat generation are only considered in a simplistic manner. This effects both level 1 and 2 PSA results and contribute both to the uncertainties and to the conservatism of a PSA. Sensitivity studies has been used to estimate the impact of these limitations and to identify areas for model improvements.

Time dependent success criteria.

Phased mission modelling, Mankamo 86 (ref. 14), discuss various approaches in which also operational decisions can be included. Further, some quantification approaches are suggested based on conditional unavailabilities or projected unavailabilities.

Long term success criteria as a time dependent function of residual heat generation are only considered in a simplistic manner. This type of time dependency are considered as a development area and will be further analyzed within the SIK-1 project.

Timing of emergency system operation.

System timing are modelled in event trees but are dependent on the degree of detail in the event trees. A model improvement within this area are related to phased mission modelling, to enable a more detailed sequence model. Sequence mission time affect component models and are today handled by mission time specification within the component model, but in the case of a sequence dependent variation of the mission time the models use are not dynamic enough.

Timing of operator actions.

Different conditions for operator action during accident scenarios can be defined more clearly by improved event tree modeling. One approach are to develop event trees that only use operator objectives/actions in the event tree headings and consider hardware event only as support to the operator objectives/actions. This type of development should require extensive model work but should address the operator situation much better, e.g. timing of recovery actions.

Time dependence of operator error probabilities.

The operator error probabilities are dependent on the time available for the operator to understand the situation and take necessary measures. In PSA this is handled by definition of human interaction time windows which are evaluated using time-reliability curves and so called cognitive reliability models.

Time dependent physical phenomena.

Phenomena that come into account are those how can aggravate the situation after a certain time or after certain conditions are fulfilled. One example is the back-flush operation in older ABB BWR design.

2.5 The increase of statistical evidence.

A problem and use of LPSA is to give a support in decision making using relevant background data and experience. The LPSA allow the possibility to take several factors into account such as failure experience, plant operations, design e.t.c.. This experience change/grow as time pass on and this time dependency must be treated to a certain extent. The process is slow (years) compared to other time dependencies but many small changes can accumulate and become significant.

Time dependent operating experience evaluation. Time dependent trend follow up.

As suggested in section 2.1 operating experience and data trend analysis must be used to identify time dependent failure mechanism. It is not necessary model these mechanism explicit in the LPSA but to give priorities to which components or set of components to monitor using importance or sensitivity analysis.

Time dependent uncertainty estimate.

It is essential to structure a given decision situation by identifying decision alternatives and model limitations at the same time. With a relevant decision model available, decision making under uncertainty is possible. With this as a background the decision model will also emphasize the most significant limitations in models and data, and time dependent uncertainty estimates will come into account.

2.6 Time dependent plant status knowledge.

Failure modes can be categorized into a few classes which are treated differently depending on our knowledge (ref. 15). In current PSAs the plant status is represented by probabilities and test intervals. By using these parameter one can express an average risk for mainly risk verification purposes. When trying to expand the PSA model into risk follow up and risk monitoring the need for an more flexible way to represent plant status increase, e.g. due to the fact that you just know that a component works after performing an extra test.

The main categories are evident and hidden events. The state of an evident event are known but the state for a hidden event could be uncertain and represent what we usually model as basic events in PSA.

Knowledge categories:

- evident
- hidden

events.

Test interval dependencies.

A plant model manipulator that allow system or component specific settings of extra tests and real demands according to operations.

Absolute representation of status information.

Absolute setting (0,1) of evident events, available or unavailable equipment.

SUMMARY AND RECOMMENDATIONS

It is possible that detailed time dependency analyses require too much resources to be included in the standard PSA. However, a detailed review of PSAs can lead to recommendation to include time dependency analyses of some specific issues. Some of which are typical for Living PSA applications. A LPSA model must treat time dependencies in a much more complete way than a conventional PSA model used for risk verification. Many important aspects on plant risk are time dependent. If the failure models are compatible with the operating experience this leads to a greater confidence of PSA results.

Different mechanisms can be identified in operational data analysis the main problem is to identify deteriorating components as early as possible. Differences in accumulated operational time, e.g. lead diesel, is one way to get early indications of a deteriorating trend. In the I-book initiating event data book, a bayesian approach to handle the learning process has been developed based on the concept suggested by Vaurio. The I-book methodology can also be used for other purposes.

Test interval dependent component modelling is possible by using the new T-book III data. Test arrangement can be modelled in component models as a failure to by-pass the test arrangement in the case of a demand.

The time independent start unavailability, q_0 , presented in the T-book can be interpreted as partly an average measure of test efficiency.

The probability for a test caused failure, p_{tf} , have almost the same impact on the model as q_0 and may be excluded.

To model test interval dependencies in CCF models, the problem is to avoid conservatism and to allow non symmetric test arrangements. Model 3 allow non-symmetric test arrangements but are not possible to use in the available fault tree codes.

Component status dependent CCF models are required to represent a failure situation correctly and must allow that one or more components are unavailable.

Limiting Conditions for Operation can be represented in system fault tree models using not logic in the system modelling.

Time dependent success criteria can be modelled using phased mission modelling various approaches can be used in which also operational decisions can be included. Timing of emergency system operation requires model improvements that are related to phased mission modelling.

Timing of operator actions can be defined more clearly by improved event tree modeling, by developing event trees that only use operator objectives/actions in the event tree headings and consider hardware event only as support to the operator objectives/actions.

Time dependent uncertainty estimate. With a relevant decision model available decision making under uncertainty is possible. Such model will also reveal the most significant limitations in models and data and time dependent uncertainty estimates will come into account.

Treatment of time dependent plant status knowledge requires that failure modes can be categorized into classes which are treated differently, i.e. evident and hidden events. The state of an evident event are known but the state for a hidden event could be uncertain. A plant model manipulator are required to allow system or component specific settings of extra tests and real demands according to operations. Further, this manipulator must allow absolute setting (0,1) of the evident events, i.e. the test outcome (available or unavailable equipment).

REFERENCES:

1. S. Hirschberg et. al.. Dependencies, Human Interaction and Uncertainties in probabilistic Safety Assessment. NKA/RAS-470, April 1990.
2. Vaurio, J.K.. Application of a New Reliability Growth Model that Fits Data. Scandinavian Reliability Engineers Symposium, Otaniemi, Finland, October 14-16, 1986.
3. Blomquist R., Pörn K.. Initiating Event Data Book. Studsvik, To be Published.
4. US NRC. The FRANTIC Code Manual. NUREG-0193. Mars 1977.
5. Laakso K., et al. Optimization of Technical Specifications by use of Probabilistic Methods. NKA RAS-450, 1990.
6. Berg U. Risk Spectrum user Manual. Relcon. To be Published.
7. Pörn K., Skagerman S.. T-Book III - Reliability Data Book for Components in Swedish and Finish Nuclear Power Plants, third edition. To be published 1991.
8. Schwartz F.. Verifiering av säkerhetsfunktioner för O3, Steg 1. OKG, 3-710/90, 901102.
9. Knochenhauer M.. Development of a Time Dependent Failure Model for Motor Operated Valves Based on Analysis of Failure Data and Testing. ABB-Atom, RPC 89-69, 890920.
10. Björe S., et. al.. Defences against CCF and Generation of CCF Data, Pilot Study for Diesel Generators. SKI Research Program, To be published.
11. Erhardsson U-K. Test av några tidsberoende CCF-modeller. Vattenfall, PK-168/90, 901123.
12. Landelius M..Optimering av provningsintervall för 327-pumprokning i O3. OKG, 3-518/89, 891116.

Landelius M.. English translation, Letter Report. Time Dependent Component Modelling Including Common Cause Failures for Components subject to Staggered Testing. 910301.
13. Mankamo T., Pulkkinen U.. Test interval of standby equipment, VTT 892, September 1988.
14. Mankamo T.. Phased Mission Reliability - A New Approach Based on Event Sequence Modelling. Scandinavian Reliability Engineering Symposium, Otaniemi, Finland, October 14-16 1986.
15. Holmberg J.. Principles of the Risk Assessment of Operating Experience by PSA. VTT/SÄH, Finland, NKS/SIK-1(91)2, 910123, Draft report.

Human Error

Chairman: J. Mertens

KFA-Forschungszentrum Jülich GmbH
Institut für Sicherheitsforschung und Reaktortechnik (ISR)
Dr. J. Mertens 27.03.1991

ISSUE PAPER

Subject: Human Errors

1) Problem description

The safety of Nuclear Power Plants is influenced by human errors in various manner, as operating experiences and real accidents have shown. Therefore an adequate consideration of human errors in Probabilistic Safety Analyses (PSA) is essential. On the other side the specific possibilities of the operators - compared to safety systems - cause specific PSA-problems, as well regarding completeness as in respect to quantitative assesement.

2) Documents stating the state of the art

- Comparison and Application of Quantitative Human Reliability Analysis Methods for the Risk Program (RMIEP)
NUREG/CR 4835, 1989
- A.D. Swain
Comparative Evaluation of Methods for Human Reliability Analysis
GRS-71, April 1989, ISBN 3-293875 21-5
- Models and Data Requirements for Human Reliability Analysis
IAEA-Tecdoc-499, 1989
- P. Humphreys (Editor)
Human Reliability Assessors Guide, SRD, RTS-88/95 Q,
Oct. 1988
- Poucet, A.
Human Factors Reliability Benchmark Exercise (HF-RBE), Final Report I; summary of results and conclusions
P.E.R. 1482/88; Commission of the European Communities,
Joint Research Centre Ispra, 21020 Ispra (Va), Italy, 1988

- Reliability Engineering and System Safety (Special Issue on Human Reliability Analysis)
Vol. 29, No. 3, 1990

3) Areas with well established and validated methodology

Strictly spoken there is no PSA-relevant area concerning human factors for which the methods are established and validated (compared for instance with the methodology of failure trees). In respect to both the qualitative and quantitative assessment of operator actions, the identification of possible human failures in the course of planned actions (that means during normal plant operation and accident control) seems to be relatively practicable. Indications of such error-likely situations are essentially a result of the systematic procedures which a PSA generally makes use of.

4) Areas where improvements are necessary

Compared with the identification of error-likely situations in the course of planned operator actions the frequency quantification of operator errors is less validated. Even the great number of operator models is a clear indication of methodological deficiencies. Often these models include only partial aspects of human reliability, and none of the models covers all of them. On the other side there is a lack of sufficiently validated reliability data regarding to operator actions. Even though basic data are available, there is still the problem to quantify so-called performance shaping factors which depend on specific situations. These deficiencies cannot be redressed easily by simulator experiments; the main reason is that simulators not reflect the real world conditions, and the raw data from training simulators have to be modified. Another method, expert judgement, has often a relative characteristic and needs calibrations using 'hard' data. Therefore it is necessary to collect such data furthermore (at the best by evaluation of operating experiences) and to develop criteria for comparison and transference.

An additional and essential problem lies in the subjectivity of the analysts using operator models. The related uncertainty margins are in the same order of magnitude than those caused by the application of different models. Possibly this situation can be improved by using expert systems which standardize the model application and make the decision process verifiable.

Analyses of beyond-design accident sequences (including accident management measures) have shown substantial deficiencies regarding the assessment of necessary operator actions. These problems of qualitative quantitative assessment are caused mainly by the unsufficient knowledge about the specific accident situation. Therefore the operating crew has to recognize and decide in a stronger extent than in the course of exactly planned action. In addition there may exist possibilities of diverging goals. In such cases the range of action which have to be identified and assessed is relatively wide, and there is a need to develop criteria for identification of risk-relevant situations, to formulate performance shaping factors and to quantify such factors. This seems not possible without using psychological approaches.

In view of the need for improvements the following issues should be discussed:

- How can operating experiences used to provide a better data base?
- How can rough data from training simulators be modified to reflect real accident situations?
- What is the best way to diminish the subjectivity of analysts?
- If current operator models do not sufficiently address the cognitive and psychological aspects specific to human operators, what is a practicable way to get improvements?

Annex 1

Problem Description

The safety of nuclear power plants depends in various ways on the human factors related to plant design, construction and operation. During operation human errors can influence the plant safety

- as initiators of unwanted events
- as an incorrect accident control action
- by turning a trivial sequence into one with serious consequences
- latent as errors during maintenance of stand-by components, surveillance tests and calibrations.

Therefore human errors have to be considered in Probabilistic Safety Analyses, and from previous experience human errors contribute essentially to the unavailability of systems and to the overall plant risk.

Related to the quantitative assessment, failure during design and construction are included in reliability data of components and systems.

Concerning the identification and quantitative assessment of operator action during operation, a classification into 'planned' and 'unplanned' seems to be useful. Planned actions are expected to be carried out by the operators during safe operation and in the course of accident control; therefore planned actions have been written down (such as test- and maintenance procedures or measurements during design basis accidents). Planned actions are associated with rule- or skill-based behaviour.

In opposition to this, a desired human action can be called 'unplanned', if there is a need peculiar for cognition and decision making in the case of an accident (knowledge-based behaviour).

Regarding to the quantitative assessment of human errors needed in PSA's, the knowledge of all relevant influences on human reliability is important. Typical 'performance shaping factors' are training, control room quality and design, stress, available time, personal redundancy, dependencies between different tasks and personal dependencies.

There are several models for human reliability analysis (HRA) which have been used in PSA/PRA mainly concerning planned actions. Such HRA methods provide useful techniques to identify the potential for important human errors and to design complex systems considering human factors.

In view of the quantification of error probabilities the uncertainties are still extensive, and the possibilities to consider all relevant aspects of human behaviour (especially the cognitive and psychological aspects) are under discussion.

Annex 2

References

- Swain, A.D., Accident sequence evaluation program reliability analysis procedure. US Nuclear Regulatory Commission, Washington, DC, 1987.
- Comer, M.K., Seaver, D.A., Stillwell, W.G. & Gaddy, C.D., Generating human reliability estimates using expert judgement, Vol. 1, Main Report. NUREG/CR-3688, US Nuclear Regulatory Commission, Washington, DC, 1984.
- Hannaman, G.W., Spurgin, A.J. & Lukic, Y.D., Human cognitive reliability model for PRA analysis. Draft NUS-4531, NUS Corp., San Diego, CA, 1984.
- Kopstein, F.F. & Wolf, J.J., Maintenance personnel performance simulation (MAPPS) model: User's manual. NUREG/CR-3634, US Nuclear Regulatory Commission, Washington, DC, 1985.
- Wreathall, J., Operator Action Trees: An Approach to Quantifying Operator Error Probability During Accident Sequences. NUS-4159, NUS Corp., Gaithersburg, MD, 1982.
- Dougherty, Jr, E.M. & Fragola, J.R., Human Reliability Analysis: A Systems Engineering Approach with Nuclear Power Plant Applications, Wiley, NY, 1988.
- Hannaman, G.W. & Spurgin, A.J., Systematic Human Action Reliability Procedures (SHARP), EPRI NP-3583, Electric Power Research Inst., Palo Alto, CA, 1984.
- Embrey, D.E., Humphreys, P., Rosa, E.A., Kirwan, B. & Rea, K., SLIM-MAUD: An Approach to Assessing Human Error Probabilities Using Structured Expert Judgement. Vol. I: Overview of SLIM-MAUD, NUREG/CR-3518, US Nuclear Regulatory Commission, Washington, DC, 1984.
- Swain, A.D. & Guttman, H.E., Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications. NUREG/CR-1278, US Nuclear Regulatory Commission, Washington, DC, 1983.
- Reliability Engineering and System Safety (Special Volume on 'Accident Sequence Modeling: Human Actions, System Response, Intelligent Decision Support'), Vol. 22, Nos. 1-4, 1988.

- Dougherty, E.M.; Fragola, J.R.: Human Reliability Analysis, New York, Wiley, 1988.
- Seaver, D.A.; Stillwell, W.G.; Procedures for Using Expert Judgement NUREG/CR-2743, 1983.
- Hannaman, G.W.; Spurgin, A.J.; Lukic, Y.D.; Human Cognitive Reliability Model for PRA Analysis, Draft Report NUS-4531, EPRI Project RP2170-3, Electric Power Research Institute, Palo Alto, CA, 1984.
- Weston, L.M.; Whitehead, D.W.; Graves, N.L.; Recovery Actions in PRA for the Risk Methods Integration and Evaluation Program (RMIEP), Volume 1: Development of the Data-Based Method, NUREG/CR-4834, Volume 1, US Nuclear Regulatory Commission, Washington, DC, 1987.
- Whitehead, D.W.; Recovery Actions in PRA for the Risk Methods Integration and Evaluation Program (RMIEP), Vol. 2: Application of the Data-Based Method, NUREG-4834, Vol. 2: US Nuclear Regulatory Commission, Washington, DC, 1987
- Beare, A.N.; Dorris, R.E.; Kozinsky, E.J.; Manning, J.J.; Haas, P.M.; Criteria for Safety-Related Nuclear Power Plant Operator Actions: Initial Simulator to Field Data Calibration, General Physics Corporation and Oak Ridge National Laboratory, NUREG/CR-3092, US Nuclear Regulatory Commission, Washington, DC, 1983
- Swain, A.D.
Accident Sequence Evaluation Program Human Reliability Analysis Procedure NUREG/CR-4772, Sand 86-1996, Febr. 1987
- Rasmussen, J.
Information Processing and Human-Machine Interaction: An Approach to Cognitive Engineering, North-Holland, New York, 1986

SÄTEILYTURVAKESKUS
(STUK) - Strålsäkerhetscentralen
Finnish Centre for Radiation and
Nuclear Safety - Helsinki Finland
Lasse Reiman

OECD/CSNI Workshop
on Special Issues
of Level 1 PSA
Cologne, May 1991

A SLIM-BASED APPROACH IN ANALYZING OPERATOR COGNITIVE ACTIONS

1 Introduction

1.1 A pre-study

A study is in progress in STUK to analyze most important human actions identified in level 1 PSAs. A pre-study was first made to prepare for the actual analysis. It included a review of the existing methods used in HRA. Another part of the pre-study was an interview of six shift supervisors from both the TVO and Loviisa nuclear power plants aiming at recognizing the most contributing factors to the behavior of control room operators in disturbance and accident situations. Other issues dealt with in the pre-study are described in Ref. 1.

1.2 Selection of methods

A wide range of techniques exists for quantitative human reliability assessment. The validity and the qualitative usefulness of the method were considered the most important criteria in evaluating the methods. Qualitative usefulness was rated high because of the large uncertainties still present in quantitative results and also because qualitative results can be used to further enhance the safety of the plant. The effective use of resources was not regarded critical because only selected operator actions are studied. Instead, in comparing different methods based on expert judgment the acceptability to the experts was regarded an important factor.

Because of the sparsity of relevant empirical data, expert opinion is frequently used in HRA to assess frequencies of

human failures. The use of expert judgment in probability assessment has been widely studied. In Ref. 2 a thorough review of subjective probability assessment and psychological scaling methods is presented. One recommendation is that the event to be judged must be completely defined and structured. Also training of experts is stressed. The study presented in Ref. 3 critically reviews several representative applications of expert opinion in the field of risk analysis. One of the key findings is that when unaided by formal methods, people are poor processors of information. In spite of many negative findings, the authors state that they have found several efforts confirming that expert opinion can in fact be used well in practical settings.

Based on review and comparison of methods it was decided to use SLIM- and TRC-based methods in the quantitative part of the analysis. This paper deals with the analysis of operator cognitive actions at TVO plant using a SLIM-based approach. A detailed description of the methods used and the results is presented in Ref. 4.

2 SLIM-based analysis

2.1 Success Likelihood Index Methodology

Multi-Attribute Utility Theory (MAUT) provides a formal basis for Success Likelihood Index Methodology (SLIM). The rationale underlying SLIM is that the likelihood of an error occurring in a particular situation depends on the combined effects of a relatively small set of performance shaping factors (PSF). SLIM assumes that the Success Likelihood Index is a sum of the products of the normalized PSF weights and ratings /5/.

2.2 Selection and training of experts

Four experts were chosen for the first session. Two of them were from STUK, one from the VTT and one from the utility. Different fields of expertise were covered. All the experts

have a long working experience on nuclear field and are well-known specialist on their own fields. In the second session three experts from STUK took part.

The Success Likelihood Index Method was described to the experts at the beginning of the session using some earlier studies as examples. A procedure had been prepared and given to the experts earlier in which the scales of weight and rating assessments were explained and guidance was given concerning the use of these scales. The definitions of PSFs were also presented in the procedure.

A number of biases have been observed in the expert judgments. Training of the experts has in some studies been observed to improve the quality of the judgments. For this purpose a summary of different types of errors affecting subjective judgments was prepared and presented at the beginning of the session. The summary was based on References 6 and 7. For example, to avoid overconfidence in their judgments, the experts were asked to try to actively search for evidence contrary to their original opinion.

One of the most difficult issues in analyzing operator actions in an accident situation is the evaluation of stress and its effects on operator behavior. Only very few studies exist concerning the stress in particular of nuclear power plant operators in emergency situation. At the beginning of the first session the chairman (the author) presented a brief review of Ch. 17 of the Handbook /8/ which deals with stress. Also, a summary of References 9 and 10 was presented.

2.3 Qualitative analysis

A very important part of the analysis is a thorough qualitative analysis of the operator actions in question. This was done by first studying the plant behavior based on accident analysis. In some cases new analyses had to be done. The operator actions were preliminary modelled based on plant

behavior and symptom-based EOPs of the plant. Descriptions of event sequences were written where main plant parameters and supposed operator actions were presented.

These event sequences were then discussed with six shift supervisors of the plant. This was done in connection with the pre-study interviews described in Ch. 1.1. Each shift supervisor evaluated the sequences using a talk-through and a walk-through method. For some actions an execution time was measured for quantification purposes.

2.4 Selection of PSFs

In this study the human factors analyst made a preliminary selection of the PSFs based on a literature review and the pre-study. A detailed definition of each factor was formulated. In the session this selection was presented to the experts who accepted it for use in the assessment. In the second session two least important factors were left out for practical purposes. The factors used in the second session were quality of information on plant state, diagnosis complexity, decision making burden, stress, training/experience and emergency operating procedures. The two additional factors in the first session were task complexity and organizational factors.

2.5 Expert session

The first expert session was held at the power plant. After the training described earlier, the session chairman described the accident sequence and the particular operator action to be evaluated. The related EOPs were then presented and discussed. The accident sequence and the execution of all the related operator actions was then demonstrated to the experts in the main control room. The positions of different measuring and control equipment were also shown to the experts. Different error possibilities were discussed during this walk-

through. The assessment of this particular operator action was done right after this demonstration.

Nominal Groups Technique (NGT) was adopted for the first session. When the first estimates of weights and ratings were drawn up, each expert briefly went through his assessment giving some basis for it. After that the experts had a possibility to make questions to each other. Finally, the assessments were revised without any subsequent discussion.

2.6 Weight assessment by AHP

In the first session weights were determined using the original method of SLIM. It is stated in Ref. 11 that the decomposed weights are relatively uniformly distributed across the attributes, whereas the optimal statistical weights are much more heavily concentrated on but a few factors. A subjective evaluation of the results of the first session indicates that possibly too much weight had been given to some less important PSFs in some cases.

New methods to evaluate weights were searched to improve the weight assessment and the Analytic Hierarchy Process (AHP) of Saaty was taken in use in the second session. The AHP is a pairwise comparison method developed for modelling unstructured problems in the economic, social and management sciences. A scale of numbers from 1 to 9 is introduced with qualitative explanations for pairwise comparisons [12/.

If we denote by w_1, \dots, w_n the weights of the factors the pairwise comparisons may be represented by a matrix which has positive entries $a_{ij} = w_i/w_j$. If A is a $n \times n$ matrix of pairwise comparisons, in order to find the priority vector, we must find a vector w which satisfies $Aw = \lambda_{\max} w$, where λ_{\max} is the largest eigenvalue of the matrix A . A is consistent if and only if $\lambda_{\max} = n$. Since small changes in a_{ij} imply a small change in λ_{\max} , the deviation of the latter from n is

a measure of consistency. The consistency index is defined as $(\lambda_{\max} - n)/(n-1)$.

In the second session three experts from STUK evaluated, using AHP for weight assessment, the same operator actions that had earlier been evaluated with the original SLIM. Two of the experts had taken part also in the first session. The third expert was the human factors analyst, who had also made the assessments using the original SLIM, but not presented them in the session. The results obtained by of these three experts were compared when using these two methods and this comparison is presented in Ch. 3.2.

2.7 Conversion of SLIs to Probabilities

The SLIs generated in SLIM-session are relative measures of the likelihood of success of each task considered in the session. In order to transform these to human error probabilities, it is necessary to calibrate the SLI scale for the tasks considered. In SLIM the calibration is based on a logarithmic relationship between SLIs and human error probabilities. In this study concerning the TVO plant the calibration was done using the HCR/ORE correlation /13/, Swain screening model or by expert judgment in the cases of high stress. Although the calibration is quite essential in SLIM it is not dealt with in detail because the main focus of this paper is on the method used to produce the SLI estimates.

3 Evaluation of assessment procedure

3.1 Group assessment methods

SLIM was found a practical method to analyze nuclear power plant operator actions. It was used to analyze the cognitive actions in six accident sequences at the TVO plant. Only four of these sequences were totally separate from each other and the results presented are based only on those four. The

average SLI values with their standard errors produced in the two sessions are presented in Table 1.

In aggregating individual judgments a NGT type interaction was used. Some experts expressed afterwards satisfaction with the method. The effect of this group process was to improve the consistency of the weight assessments as is discussed in Ch. 3.2. Also some important qualitative observations came up in this phase. In the second session a Delphi type interaction was used.

Based on this study a group interaction like the NGT seems to be useful but time consuming. Some way to gather qualitative findings of the experts should be organized, if this kind of method is not used.

3.2 The assessment of weights and ratings

In the second session the AHP was used in weight assessment as described earlier. For each matrix the largest eigenvalue, the consistency index and the consistency ratio were calculated. The largest consistency ratio produced in this study was 0.10. According to Ref. 12 this value is still acceptable.

To compare the two ways of assessing weights, the Kendall coefficient of concordance W was calculated for different cases. To calculate the coefficient the values of different variables are replaced with their ranks. The value of W can be calculated from the formula presented in Ref. 14.

In the first session all the values of W are significant at least at the 5 per cent confidence level showing that the judges are applying essentially the same standard in ranking the objects. In the second session all the values of W except for the case 3 are also significant at the 5 per cent level. The Kendall coefficient of concordance W was also calculated for the first session without the two least important factors

that were left out in the second session. In this case the values of the second session are clearly higher except for the case 4.

The Kendall coefficient of concordance can also be used to see how the consistency of weight assessments improved when using the NGT method in the first session. In Table 2 the values of W are shown for the first and second estimates of weights for different cases. The effect of the structured group process can be clearly observed in the first three cases.

In some studies the weights have been assessed only once and used for all the operator actions analyzed. Looking at the average weights across experts clearly shows that weights should be evaluated for each case separately.

To compare the SLI-values achieved by the two methods Table 3 was produced. It shows the SLIs of the three experts, who used both methods in all the four cases. It is interesting to note that differences between the highest and lowest values are slightly larger while using the AHP. The distinction is, however, not statistically significant.

3.3 Interjudge consistency

The consistency across experts was examined also by a two-way analysis of variance (ANOVA). An ANOVA was conducted for the SLI-values of the two sessions. The results of these analyses are presented in Table 4. In both sessions, the effects of both events and judges are significant when the ANOVA is conducted for SLI-values, but at different levels of confidence.

It is suggested in Ref. 15 that the interjudge consistency should be evaluated by carrying out an ANOVA using the individual log HEPs as the dependent variable. This was also

done for the results of both sessions, and the results indicated that the effect for judges was not significant.

4 Some quantitative results

The first cognitive action analyzed was an ATWS-situation related with a loss of condenser transient. The failure of the reactor hydraulic scram was postulated to be caused by a common-mode failure of relays in the reactor protection system. In this situation the operators have the possibility to trip the reactor by initiating the hydraulic scram by some manual actions at the relay cabinets. The total available time is 5 min and the manipulation time 2 min provided that the actions in the relay cabinets are done before the actuation of the boron system (or simultaneously).

The second operator action was a refilling of the tank from where the auxiliary feedwater system takes its suction. This is necessary in some medium LOCA sequences, where either reactor depressurization is not possible or the low pressure emergency cooling system is not available. After the low level alarm of the tank there is about one hour's time to initiate the refilling, which is done by the fire brigade using the fire fighting system.

The third action analyzed was the initiation of manual reactor depressurization. In the accident sequence that was analyzed in the SLIM session one of the safety relief valves of the reactor was stuck open (case 3.1). The SLI values obtained this way were used also in the base case where all safety relief valves function as designed (case 3). The initiator of the accident sequence was a loss of all the main feedwater pumps because of a low suction pressure. A common-mode failure in the auxiliary feedwater system prevented its use. The times available for the initiation of manual depressurization are 37 min and 25 min in the two cases, respectively. They are based on analyses made in STUK using a RELAP code /16/.

The manual depressurization of the reactor was later tested at the simulator by the utility and the times of initiation were measured for all crews. On the basis of these measurements, no changes were necessary in the manipulation times assessed in the qualitative analysis. Only a small correction was made in the diagnosis time based on expert judgment.

The fourth operator action analyzed is related to a station black-out sequence, where none of the diesel generators have started but at the neighbouring unit at least three of them are running. In this situation there is a possibility to 'loan' one of the diesel generators of the other unit.

In all these four cases only the cognitive part of operator action was analyzed. Operator failure probabilities based on the first session are presented in Table 5. The results are calculated as a geometric mean of human error probabilities based on SLI values of each expert.

In Ref. 15 uncertainty bounds are determined based on the variances of the log HEP estimates across judges. In this study ± 2 s.e. uncertainty bounds were given to SLI values and an EF = 10 was assumed for the boundary conditions used in the calibration. The results indicate that the uncertainty is to large extent caused by the uncertainties related with the boundary conditions of the calibration.

6 References

1. L.Reiman. Analyzing activities of nuclear power plant operators. A pre-study. (Draft). Finnish Centre for Radiation and Nuclear Safety. Helsinki. 2.5.1991.
2. W.G.Stillwell, D.A.Seaver, J.P.Schwartz. Expert Estimation of Human Error Probabilities in Nuclear Power Plant Operations: A Review of Probability Assessment and Scaling. NUREG/CR-2255. Decision Science Consortium, Inc., May 1982.

3. A.Mosleh, V.M.Bier, G.Apostolakis. Methods for the Elicitation and Use of Expert Opinion in Risk Assessment. NUREG/CR-4962. Pickard Lowe and Garrick, Inc., August 1987.
4. L.Reiman. Analysis of operator cognitive actions at TVO nuclear power plant using a SLIM-based approach. (Draft). Finnish Centre for Radiation and Nuclear Safety, 6.5.1991.
5. D.E.Embrey, P.Humphreys, E.A.Rosa, B.Kirvan, K.Rea. SLIM-MAUD, An Approach to Assessing Human Error Probabilities Using Structured Expert Judgement. Vol. 1. Overview of SLIM-MAUD. NUREG/CR-3518. Brookhaven National Laboratory, March 1984.
6. A.Tversky, D.Kahnemann. Judgement under uncertainty: Heuristics and biases. Science, 185, 1974.
7. D. von Winterfeldt. Some sources of incoherent judgments in decision analysis. Decision Science Consortium, Inc., November 1980.
8. A.D.Swain, H.E.Guttman. Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications. NUREG/CR-1278. Scandia National Laboratories, August 1983.
9. S.Baker, E.Marshall. Stress and Control Room Operator Performance - A Summarised Literature Review. HPR-332, December 1987.
10. D.I.Gertman, L.N.Haney, J.P.Jenkins, H.S.Blackman. Operational Decisionmaking and Action Selection Under Psychological Stress in Nuclear Power Plants. NUREG/CR-4040. Idaho National Engineering Laboratory, May 1985.
11. G.W.Fischer. Experimental Applications of Multi-Attribute Utility Models. In: Utility, Probability and Human Decision Making, D. Reidel Publishing Company, 1975.

12. T.L.Saaty. The Analytic Hierarchy Proses. McGraw-Hill, 1980.
13. P.Moiemi, G.W.Parry, S.J.Spurgin. A Human Reliability Analysis Approach Using Measurements for Individual Plant Examination. NUS-5191, Electric Power Research Institute, July 1989.
14. S.Siegel. Nonparametric statistics for the behavioral sciences. Book Company, Inc., Tokyo, 1956.
15. D.E.Embrey, P.Humphreys, E.A.Rosa, B.Kirvan, K.Rea. SLIM-MAUD: An Approach to Assessing Human Error Probabilities Using Structured Expert Judgement. Vol. II. Detailed Analysis of the Technical Issues. NUREG/CR-3518. Brookhaven National Laboratory, March 1984.
16. J.Hyvärinen. RELAP 5 analysis for a stuck-open safety relief valve in case of a total loss of feedwater at TVO plant (in Finnish). Finnish Centre for Radiation and Nuclear Safety. 9.5.1990.

Table 1. Average SLI values

The first session		The second session (AHP)
Case 1	6,14 ± 0,34	5,95 ± 0,18
Case 2	5,33 ± 0,49	3,59 ± 0,22
Case 3	6,43 ± 0,45	6,16 ± 0,19
Case 4	5,63 ± 0,46	5,24 ± 0,38

Table 2. The effect of NGT on W in the first session

Case	First estimate	Second estimate
1	0.62	0.76
2	0.60	0.70
3	0.49	0.64
4	0.98	0.98

Table 3. Comparison of the SLI values using the two methods

		Case 1	Case 2	Case 3	Case 4
J3	Session 1	5.25	4.33	5.88	4.49
	Session 2	5.60	3.47	5.83	4.55
J4	Session 1	6.03	4.66	6.04	5.95
	Session 2	6.04	4.01	6.47	5.87
J5	Session 1	5.98	4.27	6.31	5.44
	Session 2	6.20	3.28	6.19	5.29

Table 4. ANOVA results

Sources of Variation	Sums of Squares	Degree of Freedom	Mean Square	F-ratio
<u>First session</u>				
Events	2.99	3	1.00	4.0 (5 %)
Judges	6.96	3	2.32	9.3 (1 %)
Residual	2.25	9	0.25	
<u>Second session</u>				
Events	12.26	3	4.09	51.1 (0.1 %)
Judges	1.08	2	0.54	6.8 (5 %)
Residual	0.48	6	0.08	

Table 5. Operator error probabilities (first session)

Case	HEP	Remarks
Case 1	8.0 E-2	Two response patterns combined
Case 2.a	3.6 E-2	Base case
Case 2.b	5.7 E-3	Calibration: Swain screening model
Case 3	4.6 E-2	Base case
Case 3.1	1.9 E-1	Safety relief valve stuck open
Case 4	9.5 E-2	Base case

**AN APPROACH TO THE ANALYSIS OF OPERATING
CREW RESPONSES USING SIMULATOR EXERCISES
FOR USE IN PSAs**

by

Gareth W. Parry
Halliburton NUS Environmental Corporation
910 Clopper Road
Gaithersburg, Maryland 20877
USA

Avtar Singh
Electric Power Research Institute
3412 Hillview Avenue
Palo Alto, California 94303
USA

Anthony Spurgin and Parviz Moieni
Accident Prevention Group
16980 Via Tazon
San Diego, California 92127
USA

Arthur Beare
General Physics Corporation
6700 Alexander Bell
Columbia, MD 21046

**Presented at the OECD/BMU Workshop on
Special Issues of Level 1 PSA,
Cologne, FRG**

May 28th, 1991

Abstract: This paper describes an approach to the estimation of the probability of non-response in the detection, diagnosis, and decision making phase of operating crew interactions following a plant trip. The approach is based on the results of the EPRI funded Operator Reliability Experiments project, and employs two complementary methods. The first uses response time data to generate response time probability distributions. The second uses a cause based decomposition as a framework for subjective estimation.

1.0 INTRODUCTION

The Electric Power Research Institute (EPRI), as part of an effort to advance the state-of-the-art in Human Reliability Analysis (HRA) and its applications, launched a human reliability program in 1982. A major component of this program was the Operator Reliability Experiments (ORE) project⁽¹⁾. The primary purpose of the ORE project was to collect and analyze data on operating crew responses from full-scale nuclear power plant control room simulators. The data was to be used to test the hypotheses behind the Human Cognitive Reliability (HCR) Correlation⁽²⁾, conceptualized in 1984 as a means to estimate operating crew reliability for use in PSAs. In addition, guidance was to be formulated for the application to the evaluation and reduction of risk during plant operation of the HCR model and other lessons learned from the ORE data analysis. This paper discusses the application of the results of the ORE project to PSAs, and in particular, the use of data, from simulator exercises similar to those carried out under the ORE project, for the estimation of human error probabilities.

A PSA will include many human error events, and they may be classified into three main groups⁽³⁾. Type A events represent human errors that occur before the initiating event and whose effect is to leave equipment in an (unrevealed) unavailable state. Type B events relate to the initiating events themselves. Type C events represent human errors or failures that occur after the initiating

event. Motivated by the differences in approach to quantification, Reference 3 further subdivided them into two groups; type CP, which represent failures in procedure guided actions, and type CR, which represent failures to perform scenario specific, non-procedure driven innovative recovery actions. Since simulator exercises are primarily focused on in-control room procedure based operator actions, the domain of applicability to a PSA of the data that can be collected is the modeling of operating crew responses following a plant disturbance, or the type CP events. Other aspects, such as the analysis of ex-control room actions, maintenance errors, and the integration of an HRA into the PSA, are addressed elsewhere in the EPRI program.

The paper discusses the approach, formulated on the basis of the results of the ORE program, for using simulator data to quantify human error probabilities. There are two complementary methods. The first relies on curve fitting to represent the distribution of crew response times and using this fit to evaluate non-response in a specified time. While this approach has some appealing properties, it is clear that it is not, in itself, sufficient, since it relies heavily on an extrapolation technique, which cannot have unlimited applicability. Therefore, a complementary approach is proposed, to identify the possibility, and estimate the probability, on a scenario specific basis, of failure to initiate correct responses that result from causes that are expected to occur rather infrequently. This approach is strongly influenced by the analysis of errors detected in the ORE program, and consists of identifying various modes and causes of error, and constructing, for each mode, a decision tree that identifies the factors that influence the likelihood of that error mode. Because of the lack of applicable data, the estimation process is necessarily subjective. Therefore, the approach is tailored to provide structure to the process and provide a means of documenting the assumptions made.

Simulator exercises can provide much more information than mere numerical results. For example, in addition to measuring crew response times, the ORE program, as indicated above, also collected observations on crew errors, their impacts, and their causes. In this way, simulator exercises can help in the identification of potential weaknesses with EOPs from both the structural point of view and from the point of view of their ease of interpretation, and can point to potential improvements in training, human factors and man-machine interface aspects. Consequently, it is strongly believed that the worth of simulator exercises should not be measured on the basis of providing the response time data alone.

An overview of the approach to the estimation of type CP event probabilities is presented in Section 2. Section 3 describes the method for using simulator data, and Section 4, the complimentary method. Section 5 is a summary.

2.0 OVERVIEW OF AN APPROACH TO QUANTIFICATION OF TYPE CP EVENT PROBABILITIES

This section presents an overview of the approach to the quantification of type CP logic model HI event probabilities. Current PSA practice is generally to construct the plant logic model in such a way that accident sequences are developed to represent the consequences of performing a type CP interaction correctly, and also the consequences of not performing it at all. However, what the crew might have done instead, i.e., an error of commission, is not often modeled. Hence, type CP HI logic model events generally are modeled as if they were errors of omission. However, their probabilities are taken to include all the ways in which the crew might fail to perform the required function and this includes both true errors of omission and all errors of commission, and thus may be characterized as probabilities of incorrect response.

Because its major objective was to validate the HRC correlation⁽²⁾, the focus of the ORE program was on the cognitive aspect of the

operating crew response. To reflect this, the contributions to the probability of incorrect response is separated into those from failure to initiate timely correct response, and those from failure to execute the required response correctly.

This representation (Figure 1) is, in principle, similar to the expanded operator action tree presented in Reference 2, and the OAT approach⁽⁴⁾, in that the human interaction is subdivided into a cognitive (detection, diagnosis and decision making) part, and a response, or manipulative, part. An earlier version of this representation⁽³⁾ identified two specific mechanisms by which a correct response might not be initiated, namely, a failure to formulate the correct response, and taking too long to initiate the response. However, as discussed below, making a clear distinction between these mechanisms, and therefore, between the parameters p_1 and p_2 of the representation given in Reference 3, which parameterize these two failure modes, is difficult.

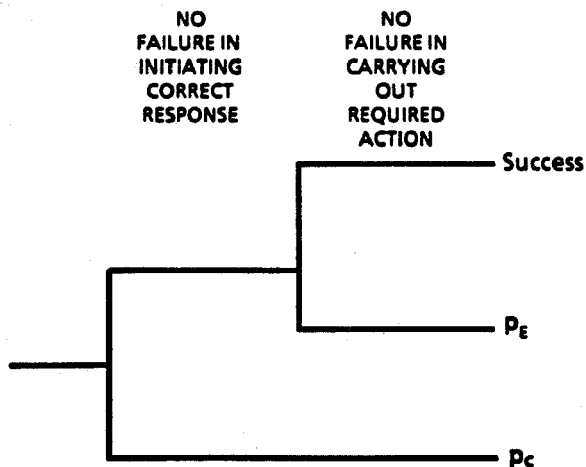


Figure 1. Representation of Type CP HIs.

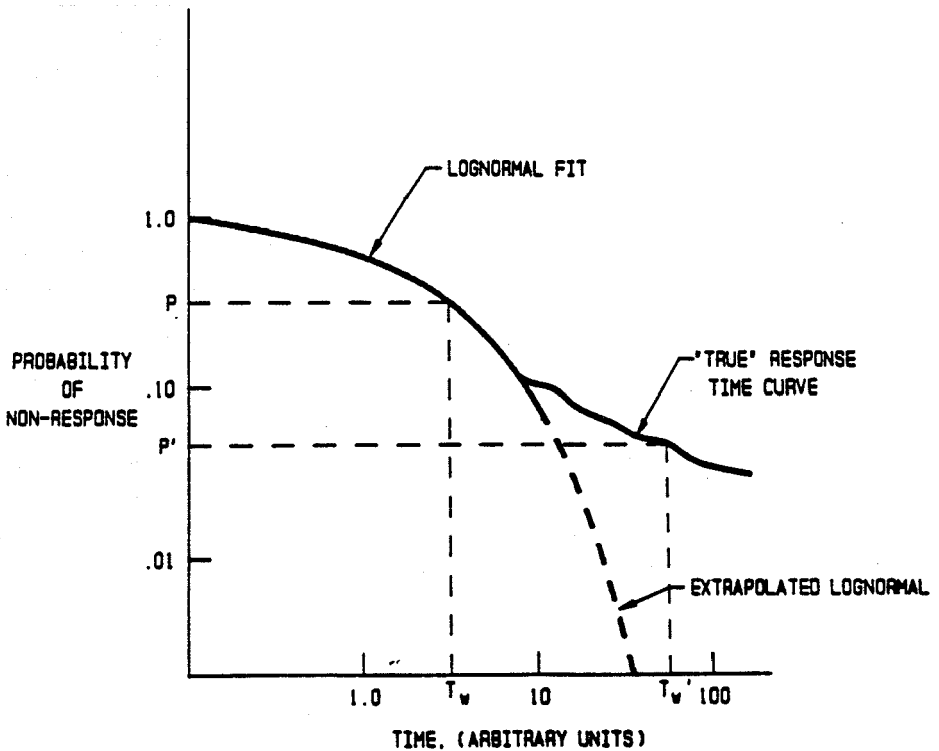


Figure 2. Conceptual Representation of Complementary Response Time Probability Distribution

2.1 The Probability of Failure to Initiate Timely Correct Response

For most of the Type CP HIs modeled, there is a time window within which the required function must be completed. Thus, time is an important element in the analysis of many human interactions. As implied above, untimely initiation of the response may arise because of slow cognitive processing, or of errors on the part of the crew, such as failing to choose the correct procedure. It is stressed that the term error is not intended to imply that the operators are necessarily at fault; in many cases, the situational factors conspire to produce errors.

The ORE experiments showed that crew response times, measured up to the point of initiation of correct action are, not suprisingly, variable, and given there is no outlier behavior, i.e., one or more crews responding considerably earlier or later than the others, the variability can be adequately represented by a lognormal distribution. The causes of, and the factors that determine, the variability were not determined, but it is not unreasonable to suppose that some of it may be due to errors that are made initially, but recovered in a timely manner. In this way, the response-time curve, fitted to a set of response times, would potentially already account for the effect of some errors. However, what the ORE program also showed was that there was a possibility of outlier behavior, which prevented a smooth monotonic fit to the response data in some cases. While some outlier behavior could be interpreted as arising from significant errors which were not recovered in the time available, in other cases, it could be interpreted as being due to crew specific problems, such as slow reading. Thus, the impact on response time of errors, and of variability in the rate of cognitive processing, are not clearly separable, at least in part because of the dynamic nature of human interactions which allows mid-course corrections to be made by the operators as time passes. These effects conspire to produce a response time curve, a conceptual picture of which, drawn as a complementary distribution, is given in Figure 2.

In principle, the probability required for the PRA model can be estimated by determining the abscissa of the response-time curve, Figure 2, at the value of the argument corresponding to the maximum time allowable. When there is no outlier behavior in a sample of response times, it is tempting to use the HCR/ORE lognormal distribution fitted to these data as the representation of the response time distribution. In some certain circumstances, this method of estimating the probability entails extrapolating the fitted curve to a significant extent, and can result in very low estimated probabilities. This is illustrated by the second of the two cases, in Figure 2, where the allowable time is T'_w . This is

to be contrasted with the first case where the time window is T_u . However, as discussed above, there exists the possibility that some response times could be very long, albeit at a low enough probability, that in the small sample obtained, they have not been observed. In this case, the extrapolation using the lognormal curve could be extremely optimistic as illustrated by the case of the time window T_u' in Figure 2. Therefore, while the main thrust of the EPRI approach is to use fitted response time curves (the HCR/ORE correlations) to estimate the probability of failure to initiate response, it is supplemented by the complementary approach, described in Section 4.

In keeping with standard PRA methodology, the parameter p_c is intended to predict the 'average' crew behavior. In the same way that PRA methods are not intended to identify poor performance for a specific pump in a population of like pumps, the method discussed here is not intended to identify crew specific problems. As discussed elsewhere⁽¹⁾, the use of simulator exercises, however, does facilitate this and is, perhaps, as strong a motivation for performing these exercises as is their usefulness for PRA purposes.

2.2 The Probability of Failure to Execute the Required Response

The second parameter of the representation of Figure 1, p_e , represents the probability that the crew makes an error in execution which is not recovered in the available time. The ORE program did not address this issue in detail. Approaches such as THERP⁽⁶⁾ are proposed for its evaluation. There is an important consideration that directly impacts the estimation of p_c , however, and that is that if the time needed to execute the response is significant, it will impact the time available for the detection, diagnosis, and decision making phase, which is a critical parameter.

3.0 ESTIMATION OF THE PARAMETER p_c USING SIMULATOR DATA

In Reference 2, the HCR correlation was proposed as a way of characterizing the operator response time distribution. The HCR correlation was expressed as a function of normalized time, a dimensionless unit which is the ratio of real time to the median crew response time. The form of the correlation was chosen to be a Weibull, with the shape parameter being a function of whether the type of cognitive processing could be classified as being skill, rule, or knowledge based, and other performance shaping factors were assumed to modify the median response time, but not the shape parameter.

As discussed in Reference 1, the ORE program did not support the original HCR hypothesis that normalized time response curves fell into one of these three categories. However, it was demonstrated that for individual human interactions, the response time data could be fitted by a lognormal distribution, which has two parameters, $T_{1/2}$, the median response time, and σ , the logarithmic standard deviation of normalized time. With these two parameters, the probability of crew non-response in a time T is given as:

$$p_c = \text{Prob}(T_r > T_y) = 1 - \Phi \left[\frac{\ln(T_y/T_{1/2})}{\sigma} \right] \quad -1$$

where $\Phi(\cdot)$ is standard normal cumulative distribution, T_y is the allowable time window, and T_r is the time of response. This curve will be referenced to henceforth as the HCR/ORE correlation. The appropriate time window, T_y , is the time window for detection, diagnosis, and making a decision. It will, therefore, generally be different from a time window based on thermal hydraulics consideration which will include the time to both identify and perform the action.

As with the original HCR formulation, it was felt that it would be advantageous if the correlations for the different HIs could be

grouped in some way, so that a small number of correlations could be established, with the different HIs within each group being distinguished by variations in the $T_{1/2}$ parameter. An approach based on the cue-response structure⁽³⁾ showed some systematic differences between the average σ values for the different cue-response types, but with considerable overlap of the distribution of σ within a type. It would appear, therefore, that while one factor in determining σ has been identified, there are other, HI specific factors, which have not. In the absence of such predictability, it is strongly recommended that HI specific data be gathered whenever possible.

3.1 Estimation of the Parameters $T_{1/2}$, σ of the HCR/ORE Correlation

Three different approaches are proposed in order of preference. The first is the use of simulator exercises to gather data on response times. This has the major advantage that the impact of many of the principal performance shaping factors will be implicit in the collected response times. In addition, by designing the simulator exercise, the analysts can obtain data which matches as closely as possible the scenario developed in the PRA.

In situations where it is not possible, or convenient, to perform the necessary experiments, structured interviews with instructors, operators, and other knowledgeable persons can be a valuable alternative to obtaining estimates of $T_{1/2}$ and σ . The purpose of performing the interviews is to get either direct or indirect estimates of ranges of response times. It is unlikely that, except for a few prompt actions, such as placing the mode switch in shutdown, plant personnel will have a reliable feel for the time taken directly. However, it is likely that, for one or two key plant parameters, they may have a very good idea of the range of values within which they might act. This will probably be particularly true of training personnel who are focused on these key parameters. The ranges of values can be converted into ranges

of times using the same thermo-hydraulic calculational tools that were used to estimate the time windows.

The third alternative is to use a generic data compilation. The ORE project has collected data on more than 40 scenarios, resulting in about 1,100 data points associated with more than 100 HIs. That is an average of about 10 data points per HI. The data can be used in several different ways. The most appropriate way is to choose a data set that most closely matches the scenario specification and HI definition of interest. Another factor of importance is that, to be completely compatible, the plant design and operational practices should also match as closely as possible. It is possible to determine the former from the information in the ORE report⁽¹⁾. It may not, however, be so easy to compare designs, or particularly operational practices, particularly as the plants from which the data are collected are not identified. An alternative then is to use aggregated data as discussed in Reference 3.

4.0 A COMPLEMENTARY CAUSE-BASED APPROACH TO THE ESTIMATION OF p_c

The approach involves the identification of situation-specific error conducive factors, and was guided by an analysis of errors observed in the ORE and elsewhere. The approach is one of decomposition, consisting of identifying potential error-causing mechanisms and, for each mechanism, evaluating the impact of certain performance shaping factors on an HI-specific basis, and also allowing for potential recovery mechanisms. This is essentially an analytical approach, as opposed to the empirical approach represented by the use of HCR/ORE curves. Available time is considered primarily in the application of the recovery factors, whose impact is considered to be time dependent.

4.1 Decomposition

To facilitate the identification of the potential causes of error, a decomposition is first made into two high-level failure modes which can be characterized as:

- 1 - Errors associated with the plant information-operator, and
- 2 - Errors associated with the operator-procedure interface.

Each of the high-level failure modes may, in turn, be decomposed into contributions from several distinct error-causing mechanisms.

The way in which this decomposition is made is clearly subjective and to some extent, arbitrary. It depends on the analyst's experience and biases as to what he thinks are the most important mechanisms. The decomposition developed by the authors of this report is summarized below.

Failure Mode 1: Failures of the Plant Information-Operator Interface: Four mechanisms are identified for this failure mode.

- p_ca. The required data are physically not available to the control room operators.
- p_cb. The data are available, but are not attended to.
- p_cc. The data are available, but are misread or miscommunicated.
- p_cd. The available information is misleading.

Failure Mode 2: Failure in the Procedure-Crew Interface: Given that the existence of a possible cue state has been recognized, four ways have been identified in which the crew may fail to reach the correct interpretation (for Type CP HIs, "correct interpretation" means execute an action or proceed to the next appropriate instruction as contingent on the cue state).

- p_ce. The relevant step in the procedure is skipped.
- p_cf. An error is made in interpreting the instruction.

$p_{c,g}$. An error is made in interpreting the diagnostic logic (this is a subset of $p_{c,f}$, but is treated separately for convenience).

$p_{c,h}$. The crew decides to deliberately violate the procedure.

This particular decomposition is based on an assumption that the procedures are, in their intent, correct. However, incorrect procedures could clearly be a cause for failure.

The approach proposed for the evaluation of p_c is, for each failure mechanism, to construct a decision tree, which incorporates questions concerning the principal factors that are felt to influence its probability of occurrence. Two example trees that were constructed as part of the work reported here are presented in Figures 3 and 4.

The decision trees presented here are not intended to be definitive, either in the choice of branch points or in the probabilities used. They are provided as a demonstration of the application of the thought process. Individual analysts are encouraged to bring their own judgement to bear on what are the important issues, and how to assess the probabilities. However, it should be stressed that the establishment of the trees and the elemental probabilities must be done at the outset of the HRA, so that all the type CP HI events are evaluated consistently.

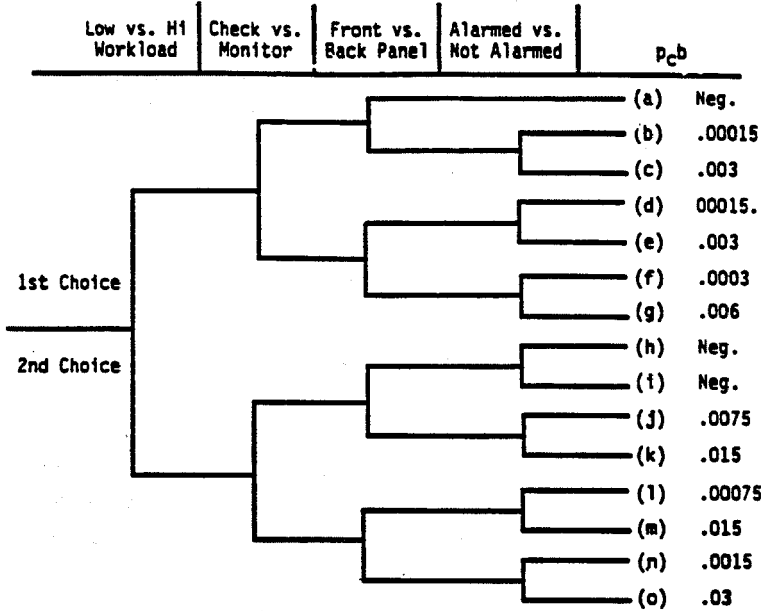
Given that an initial estimate of the probabilities of each mechanism has been obtained, the possibility of recovering from that mechanism, within the time allowable (T_y) is allowed for by correcting the initial estimates of the $p_{c,a}$ through $p_{c,h}$.

4.2 Recovery Analysis

The failure mechanisms embodied in the decision trees can be partitioned into two categories on the basis of the predominant levels of cognitive processing that influence the outcomes.

Figure 3. Decision Tree Representation of $p_{c,b}$, Failure of Attention

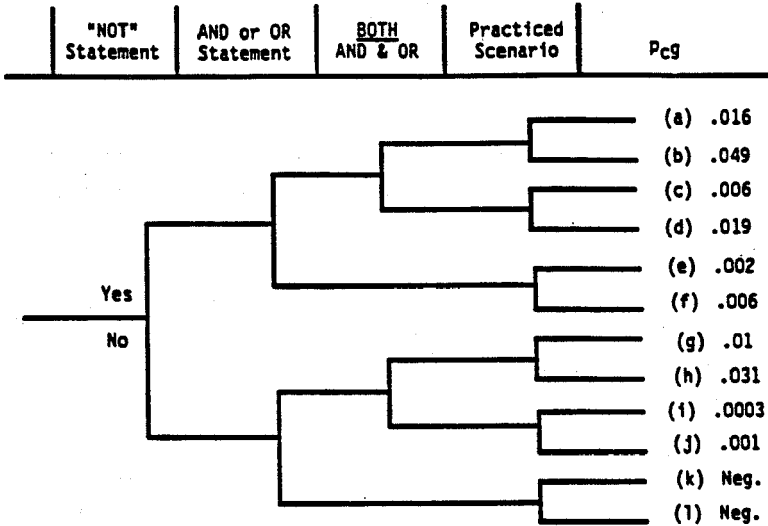
Failure Mechanism b. Data not attended to



1. Low vs. HI Workload. Do the cues critical to the HI occur at a time of high workload or distraction? Workload or distraction leading to a lapse of attention (omission of an intended check) is the basic failure mechanism for $p_{c,b}$, and it interacts with the next two factors.
2. Check vs. Monitor. Is the operator required to perform a one-time check of a parameter, or is he required to monitor it until some specified value is reached or approached. The relatively high probabilities of failure for the monitor branches are included to indicate a failure to monitor frequently enough to catch the required trigger value prior to its being exceeded, rather than complete failure to check the parameter occasionally.
3. Front vs. Back Panel. Is the indicator to be checked displayed on the front panels of the main control area, or does the operator have to leave the main control area to read the indications? If so, he is more likely to be distracted or to simply decide that other matters are more pressing, and not go to look at the cue immediately. Any postponement in attending to the cue increases the probability that it will be forgotten.
4. Alarmed vs. Not Alarmed. Is the critical value of the cue signaled by an annunciator? If so, the operator is more likely to allow himself to check it, and the alarm acts as a preexisting recovery mechanism or added safety factor. For parameters that trigger action when a certain value is approached or exceeded (type CP-2 and CP-3 HIs), these branches should only be used if the alarm setpoint is close to but anticipates the critical value of interest; where the alarm comes in long before the value of interest is reached, it will probably be silenced and thus not effective as a recovery mechanism.

Figure 4. Decision Tree Representation of P_{cg} , Misinterpret Decision Logic

Failure Mechanism a. Error in Interpreting Logic



1. "NOT" Statement. Does the step contain the word "not"?
2. AND or OR Statement. Does the procedure step present diagnostic logic in which more than one condition is combined to determine the outcome?
3. Both AND & OR. Does the step contain a complex logic involving a combination of ANDed and ORed terms?
4. Practiced Scenario. Has the crew practiced executing this step in a scenario similar to this one in a simulator?

Failure mechanisms a, d, f, and g are strongly influenced by the operators' training (specific knowledge) and his ability to draw on it to solve problems, whereas mechanisms b, c, and e are more completely determined by easily observable physical aspects of the situation with which he is dealing, and the errors involved may be categorized as slips or lapses rather than errors of understanding or intention. Deliberate violations of the procedure, p_h, do not fall into either of the above categories, but are assumed to be recoverable if the crew so chooses.

For both kinds of errors, the basic recovery mechanism is revisitation, either by the individual who committed the error, or by a second party. For the individual, this mechanism is much more effective in the case of slips than it is in the case of failures of interpretation or memory, largely because the latter reflect a characteristic of the individual instead of a more or less random occurrence that is potentiated by situational characteristics that may be momentary (e.g., workload or distraction).

Examination of the recovery factors identified makes it clear that recovery potential is also a function of time, because the factors proposed require time to come into play. In this way, the value of p_c is not fixed at its initial value, but is itself a decreasing function of time, providing a different slope (or a stair-step slope) to the curve describing the probability of non-success, rather than a clearly demarcated asymptotic value.

4.3 Synthesis

The probability of non-response, taking all this into account, may be written as:

$$p_c = \sum_{i=1,2} \sum_j p_{ij} p_{nr}^{ji}$$

Where p_{ij} is the probability of mechanism j of the mode i occurring initially for the HI, and the p_{nr}^{ij} is the probability of non-recovery from mechanism j in mode i . This formalism recognizes the fact that different error mechanisms may have different recovery or compensating factors. The formula, representing the value of p_e as the sum of the probabilities of an error resulting from each of the constituent mechanisms implies that the mechanisms are considered to be independent. This is a conservative assumption.

5.0 SUMMARY

This paper has presented an approach to the estimation of the probability of failure of an operating crew to make a timely, correct response as required by emergency or abnormal operating procedures. The work reported here has concentrated on the detection, diagnosis, and decision making phase of the response rather than the execution phase. This is largely for the historical reason that the current work has grown out of the ORE project, where the focus was on that first phase of response. To accommodate this, the failure mode is split into two contributions, the failure of the operators to initiate correct, timely response, and the failure to execute the response correctly, as discussed in Section 2.

The use of simulator exercises to provide both qualitative and quantitative data on operating crew response is recommended. In this way, as long as the simulator is a faithful representation of the control room and provides a faithful representation of the plant response, many of the important performance shaping factors are implicitly addressed. Of course there can be arguments about whether the stress in the simulator is comparable to that in a real accident. However, the use of simulators undoubtedly provides a basis for assessment that is more firmly anchored in reality than arbitrary theoretical models.

A type of time reliability correlation, called the HCR/ORE correlation is proposed to use response time data for the evaluation of the probability of failure to initiate timely action. The use of plant specific data to calibrate the correlation data is clearly to be preferred, but as an alternative, the data collected in the ORE project⁽¹⁾ can be used.

The use of the time-reliability curves to estimate the probability of untimely response requires in many cases that the HCR/ORE correlation be extrapolated into a region far beyond where response time data was collected. In this case, since there is no theoretical basis for the functional form of the response time curve, extrapolation is suspect. Furthermore, the approach does not immediately lend itself to identifying the causes of failure, which may be important if corrective actions are warranted as a result of the PSA evaluation. Therefore, an alternate complementary approach to the evaluation of the probability is proposed. The approach proposed is based on identifying significant failure mechanisms, and, for each failure mechanism, constructing a decision tree whose branches represent the most important influence factors, to help subjectively assign failure probabilities. Recovery is also allowed as the scenario permits.

While an example decomposition is presented in this paper, it should be realized that this is only one of many possible decompositions, and is almost certainly not complete. For example, while the particular decomposition may help identify the potential for outlier behavior that results from situational or procedural factors, it will not, in its present form, identify specific crew behavioral problems nor indeed is it intended to, as discussed in Section 2.

The approach is, however, an ideal format for representing the basis for an HRA analyst's assessments, making the assumptions visible in such a way that the analysis can be easily reviewed.

This approach also enforces a degree of self consistency which would not be so easy to achieve with less formal or less systematic approaches.

REFERENCES

1. Spurgin, A.J. et. al., Operation Reliability Experiments Using Power Plant Simulations, EPRI NP-6937, Volume 1, Executive Summary July 1990, Volume 2, Technical Report, July 1990, Volume 3, Appendices, December 1990.
2. Hannaman, G.W., A.J. Spurgin, and Y.D. Lukic, Human Cognitive Reliability Model for PRA Analysis, NUS-4531, Electric Power Research Institute, 1984a.
3. Moieni, P., G.W. Parry, A.J. Spurgin, A. Singh, The Use of Simulator Data in Human Reliability Analysis: Results from the EPRI Operator Reliability Experiments Program, "Proceedings of Probabilistic Safety Assessment and Management", Beverly Hills, CA, February 1991, Elsevier.
4. Hall, R.E., J.R. Fragola, and J. Wreathall, Post Event Human Decision Errors: Operator Action Tree/Time Reliability Correlation, NUREG/CR-3010 USNRC, 1982.
5. Beare, A., C.D. Gaddy, G.W. Parry and A. Singh, An Approach for Assessment of the Reliability of Cognitive Response for Nuclear Power Plant Operating Crews, "Proceedings of Probabilistic Safety and Management", Beverly Hills, CA, February 1991, Elsevier.
6. Swain, A.D., and H.E. Guttman, Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications, NUREG/CR-1278, SAND80-0200, 1983.

An Assessment of the Risk Significance
of Human Errors in Selected PSAs
and Operating Events

Robert L. Palla, Jr.
Adel El-Bassioni
Risk Applications Branch
Office of Nuclear Reactor Regulation
U.S. Nuclear Regulatory Commission

James Higgins
Department of Nuclear Energy
Brookhaven National Laboratory

ABSTRACT

Sensitivity studies based on Probabilistic Safety Assessments (PSAs) for a pressurized water reactor and a boiling water reactor are described. In each case, human errors modeled in the PSAs were categorized according to such factors as error type, location, timing, and plant personnel involved. Sensitivity studies were then conducted by varying the error rates in each category and evaluating the corresponding change in total core damage frequency and accident sequence frequency. Insights obtained are discussed and reasons for differences in risk sensitivity between plants are explored. A separate investigation into the role of human error in risk-important operating events is also described. This investigation involved the analysis of data from the U.S. Nuclear Regulatory Commission (NRC) Accident Sequence Precursor program to determine the effect of operator-initiated events on accident precursor trends, and to determine whether improved training can be correlated to current trends. The findings of this study are also presented.

INTRODUCTION

In recent years it has become increasingly clear that the risk associated with nuclear power is strongly influenced by human performance. Although human errors have contributed heavily to the two core melt events that have occurred at power reactors, effective performance during an event can also prevent a degraded situation from progressing to a more serious accident, as repeatedly shown in the U.S. operating experience. Two studies were sponsored by the NRC over the last three years in an attempt to quantify the potential impact of human performance on risk and to derive insights on how to limit risk. The first study investigated the sensitivity of risk to human error using the probabilistic safety assessments for several nuclear power plants. The second study involved an analysis of recent risk-significant operating events in U.S. reactors to determine the role of human error in these events and to identify whether improved training can be correlated to current safety trends. The results of these studies are the subject of this paper. While significantly different in character, the findings of both studies confirm the importance of human error, and support a regulatory strategy of reducing human errors and improving the likelihood of success for recovery actions through increased emphasis on emergency operating procedures, accident management preparation, and operator training.

SENSITIVITY STUDIES

Background

In 1980, Brookhaven National Laboratory performed a study for the NRC on the sensitivity of risk parameters to human error rates using the WASH-1400 model for the Surry plant (Westinghouse pressurized water reactor). This model included treatment of approximately 100 human errors, most of which were pre-accident errors, e.g., calibration errors and failure to properly reposition valves. The study confirmed the risk significance of human error and provided additional insights into risk important sequences and categories of human actions at Surry (Reference 1).

The insights from the Surry study were considered by the NRC to be of potential value in guiding licensing and inspection activities. The results, however, were plant-specific and influenced by assumptions and level of detail in the human reliability analysis (HRA). Notably, this early PSA did not model operator recovery actions. Accordingly, an effort was initiated in 1987 to update and expand the insights from the original study to reflect advances in HRA techniques and additional nuclear steam supply system designs. The program involved the conduct of extensive analyses of the sensitivity of risk to human error based on the PSA for a pressurized water reactor (PWR), followed by similar analyses using a PSA for a boiling water reactor (BWR). These studies are described in detail in References 2 and 3, respectively. Most recently, similar sensitivity analyses have also been performed by the NRC for several of the plants studied in NUREG-1150. These analyses are not discussed in this paper.

Approach

The level 1 portions of the PSAs for Oconee, Unit 3 (Babcock & Wilcox PWR) and LaSalle, Unit 1 (General Electric BWR/5) were selected as the basis for detailed sensitivity studies. The Oconee PSA was performed by the Electric Power Research Institute for Oconee, Unit 3 and published as NSAC-60 in 1984 (Reference 4). This PSA was selected because it included the most detailed treatment of human error in a PWR study at that time. As an example, the Oconee PSA includes over 500 individual human errors, of which over 200 remained after truncation. The LaSalle PSA used was a 1988 the NRC Risk Methods Integration and Evaluation Program. The LaSalle study was selected for analysis because it was considered to be a state-of-the-art BWR study and unique in its extensive use of simulator-based human error rate data.

A human error categorization scheme was developed to allow insights to be drawn from the sensitivity studies. Human errors modelled in the respective PSAs were then categorized according to such factors as timing (pre-accident or during-accident), location (inside or outside control room), and personnel involved (e.g., licensed reactor operator, non-licensed operator, and maintenance personnel). A profile of the types of human errors in each PSA is presented in Figure 1. Major differences are (1) a larger number of human errors in the Oconee PSA, due in part to the representation of numerous individual human errors in the LaSalle study by "generic" errors, and (2) the presence of only a limited number of pre-accident

errors in the screened cutsets of the LaSalle PSA in contrast to a nearly equal number of pre-accident and during-accident errors in Oconee.

Sensitivity calculations were conducted by varying the human error probabilities (HEPs) for all errors and for individual categories of errors, and investigating the corresponding changes in total core damage frequency (CDF) and accident sequence frequency. HEPs were generally varied by multiplicative factors over ranges which depended on the type of error. The largest range extended from 1/30 up to 30 times the base case value of the HEP (without exceeding a maximum HEP of 1.0). Such variations in HEPs on a global basis are considered hypothetical, and for practical purposes, smaller variations around the base case probabilities may be of more interest. A summary of the more significant results are provided below.

Sensitivity of Total Core Damage Frequency

Total core damage frequency for both Oconee and LaSalle was found to vary significantly as all HEPs were varied simultaneously over their full range (Figure 2). The Oconee CDF variation is over four orders of magnitude, compared to less than two orders of magnitude for LaSalle. For both plants, the bulk of the change in CDF occurs within a factor of 3 to 10 from the base case.

The large difference in sensitivity between Oconee and LaSalle was investigated and was found to be due to a combination of factors, the most important of which include: (1) the presence of multiple HEs in cutsets of the dominant sequences of Oconee, (2) a larger number of HEs in the Oconee PSA, and (3) higher base case HEPs in the LaSalle PSA. Both plant design differences (such as a Standby Shutdown Facility and an Emergency Feedwater System at Oconee which require manual actions) and PSA/HRA modelling differences (such as a decision to not include calibration errors in the LaSalle PSA) contribute to these factors. The significance of multiple human errors in the dominant cutsets is illustrated in Figure 3, which shows that by only doubling the HEPs, cutsets with multiple human errors begin to dominate the risk profile.

Sensitivity of Accident Sequence Frequency

Certain sequences are dominated by cutsets involving multiple human errors and exhibit strong sensitivity to changes in HEPs. An example for Oconee is the loss of instrument air sequence which includes a failure to provide feedwater within 30 minutes combined with a failure to recover instrument air in one hour. Other sequences are hardware dominated and less sensitive to changes in human error rates, such as large break LOCAs that progress rapidly and provide little opportunity for operator intervention. The sensitivity of the dominant sequences for Oconee is depicted in Figure 4. The curve for total core damage frequency is influenced by different sequences at each extreme. As HEPs are increased, sequences dominated by human actions define the curve, whereas when HEPs are reduced, the curve is defined by hardware-dominated sequences.

Pre-Accident Versus During-Accident Errors

Sensitivity analyses for both Oconee and LaSalle suggest that actions taken during the course of an accident (e.g., operator errors and recovery actions) have far greater impact on risk than errors made prior to an event (e.g., failure to restore a valve to the proper position after maintenance). Results for Oconee are shown in Figure 5 and are similar to those for LaSalle. While consistent with intuition, these results should be interpreted cautiously, recognizing that PSAs do not offer a complete treatment of pre-accident activities and errors, and that the sensitivity analysis did not explore the impact of human error on initiating event frequency. Nevertheless, the sensitivity evaluation highlights the importance of emergency operating procedures and training in mitigating important accident sequences.

Personnel Type

Calculations were also performed to investigate the sensitivity of core damage frequency to errors committed by various categories of personnel. Results of these evaluations indicate that core damage frequency is most sensitive to activities (and associated errors) which are the primary responsibility of the licensed reactor operator. Due to the significance of during-accident errors and the licensed reactor operator, additional evaluations were conducted for those actions involving coordination between the licensed reactor operator and other personnel, and those actions carried out solely by the reactor operator. Results of these analyses (Figure 6) indicate that actions involving coordination between the licensed reactor operator and non-licensed operator have a greater influence on core damage frequency than actions involving any other categories of personnel. These results point out the importance of communications, team training, and the non-licensed operators themselves.

Simulator-Based Human Error Probabilities

Approximately 70 percent of the human errors represented in the LaSalle PSA were quantified using data collected on the LaSalle plant-specific full scope simulator. This included essentially all of the errors associated with activities in the control room. As shown in Figure 7, despite the extensive use of simulator data, "simulator-based" human errors did not have a dominant effect on core damage frequency. Instead, core damage frequency for LaSalle was found to be most strongly influenced by human actions/errors which would be taken outside the control room and which could not be readily simulated. In particular, these errors were associated with recovery of offsite AC power and repair of the emergency diesel generator. This sensitivity evaluation illustrates that not all important human actions can be simulated in a standard control room simulator, and that for such errors alternative types of training may be beneficial. The potential role of training in reducing the incidence of human error was investigated in a separate study as discussed below.

ROLE OF HUMAN ERROR AND TRAINING IN RECENT OPERATING EVENTS

Background

The Accident Sequence Precursor (ASP) program at the NRC is an ongoing activity in which operational events that occur at light water reactors are screened for

precursors to more significant accidents based on risk significance. The results from the ASP program, including estimated conditional core damage probabilities for accident sequences of interest, are used to identify potential problem areas and emerging trends in the incidence and severity of precursor events.

In 1990, the NRC undertook a study of the ASP data to determine the effect of operator-initiated events on the general trends identified in the ASP program, and in particular, to identify whether improved training can be correlated to the current improving trends in the risk significance of precursor events. A summary of the approach and findings is provided below.

Approach

The NRC staff, supported by Brookhaven National Laboratory, reviewed the licensee event reports (LERs) for all precursor events during 1984 through 1989 and identified and characterized human errors that occurred in these events. Recognizing that the classification of a human action as an error can involve a significant amount of judgment, the validity of this assessment was confirmed by comparison with the human error classifications reported in the annual ASP status reports (Reference 5). To provide additional verification, a human error identification protocol was applied to precursor events for 1989. This protocol is currently undergoing further development for systematically searching the computerized nuclear documents database (NUDOCS) for LERs involving human error.

Each identified human error was evaluated by a three-member panel to determine whether nuclear power plant training programs should be effective in preventing the error. Specifically, for each error the panel determined whether "training, as it exists today in the nuclear industry and as it would reasonably be expected to develop over the next few years, could be effective in preventing the error." However, while the panel may have determined that training could be effective in preventing a specific error, such a determination does not indicate that training would absolutely prevent an error from occurring. Many factors can contribute to an error, and training is but one.

Finally, this additional information was sorted in various ways to identify any correlations between improving trends in the ASP data and major improvements in industry training programs implemented over the 6-year period; specifically, the INPO-managed accreditation of utility training programs and implementation of plant-specific or plant-referenced control room simulators required by 10 CFR 55.45(b).

Results

Of the 184 precursor events reviewed, 93 involved one or more human errors. The 93 LERs with human errors had a total of 165 human errors; about half of these errors occurred prior to the event, about 25% initiated the event, and the remaining 25% occurred during the response to the event. Of the 93 events involving human error, 57 (slightly more than half) were judged to be affected by training programs. (A precursor event was considered to be affected by training if at least one of the human errors occurring in the event was judged to be affected by training.)

Figure 8 shows the distribution of the events involving human error over the 6-year period in terms of the number of LERs and cumulative conditional core damage probability (CCDP). On average, nearly half of the cumulative CCDP is due to events involving human error. The risk that is associated with those events related to human error and training appears to be decreasing slightly by visual examination, however, this trend is not statistically significant.

Human-initiated events account for about 20 percent of the ASP events, with nearly equal contributions from licensed operators, non-licensed operators, and maintenance technicians. The number of human-initiated events has remained relatively constant from 1985 to 1989. With the exception of the Davis-Besse event in 1985, these events did not contribute appreciably to the cumulative CCDP.

In Figure 9a, the total number of human errors occurring in the ASP events is presented broken down by personnel type. The types of personnel considered are control room operators and senior reactor operators (CROs/SROs); non-licensed operators (NLOs); electrical maintenance, instrumentation and control, and mechanical maintenance technicians (EMTs/ICTs/MMTs); and technical staff and management (TSM). No significant trends in the number of errors committed by any of the four personnel types are apparent. However, an interesting pattern emerges when the effect of training on the types of errors committed by each category of personnel is considered. As shown in Figure 9b, most of the errors committed by licensed operators could have been affected by training and, therefore, might be further reduced through improved training programs. Figure 9c presents the opposite trend for technical staff and management, where most of the errors occurred in procedure writing and other areas not easily rectified through technical training. Results for non-licensed operators and maintenance technicians (Figures 9c and 9d) are between those for operators and the management/technical staff, and indicate that training can affect slightly more than half the errors committed by these personnel.

The strongest argument for a link between industry training programs and precursor data trends is provided by comparing the frequency of operator errors in the precursor events as a function of the status of the licensee's operator training program and the availability of a plant-referenced simulator at the time of each event. Table 1 provides the results of this assessment for control room operators and senior reactor operators. These results indicate a notably lower frequency of training-sensitive errors at plants that have both an accredited training program and a plant-referenced simulator.

Caution should be used in interpreting and applying the results of this assessment because of the limited nature of the precursor database and the multiplicity of factors that influence the observed trends.

CONCLUSIONS

The sensitivity evaluations performed for Oconee and LaSalle and the analyses of accident sequence precursor events together provide valuable insights into the role of the human in plant risk and means by which risk might be reduced. Most importantly, the sensitivity studies confirm the significance of actions taken

by operators in response to an event, and the importance of activities which involve coordination between licensed reactor operators (inside the control room) and non-licensed operators outside the control room. These findings support a regulatory strategy of reducing human errors and improving the likelihood of success for recovery actions through continued emphasis on emergency operating procedures, accident management preparation, and operator training.

The reduced frequency of operator errors at plants with both accredited training programs and plant simulators provides evidence that training may reduce the incidence of error and that this strategy is already paying off. As the sensitivity evaluations indicate, however, control room simulation cannot address all important events and recovery actions, and training for certain actions may need to be accomplished through other means. Accordingly, this is an area that will be specifically addressed in future activities under the accident management program.

REFERENCES

1. NUREG/CR-1879, "Sensitivity of Risk Parameters to Human Errors in Reactor Safety Study for a PWR", Brookhaven National Laboratory, January 1981
2. NUREG/CR-5319, "Risk Sensitivity to Human Error", Brookhaven National Laboratory, April 1989
3. NUREG/CR-5527, "Risk Sensitivity to Human Error in the LaSalle PRA", Brookhaven National Laboratory, March 1990
4. NSAC-60, "Oconee PRA: A Probabilistic Risk Assessment of Oconee Unit 3", NSAC-EPRI, June 1984
5. NUREG/CR-4674, "Precursors to Potential Severe Core Damage Accidents", Oak Ridge National Laboratory

Table 1. Correlation Between CRO/SRO Errors and Training/Simulator Status

Training/Simulator Status at Time of Event	No. of CRO/SRO Errors Affected by Training per 100 Reactor Years*
1. No accredited CRO/SRO training; no plant-referenced simulator	17.8
2. No accredited CRO/SRO training; plant-referenced simulator	5.6
3. Accredited CRO/SRO training; no plant-referenced simulator	4.8
4. Accredited CRO/SRO training; plant-referenced simulator	5.4

*Normalized to reflect the number of operating reactors in each training/simulator status category in the year of the event

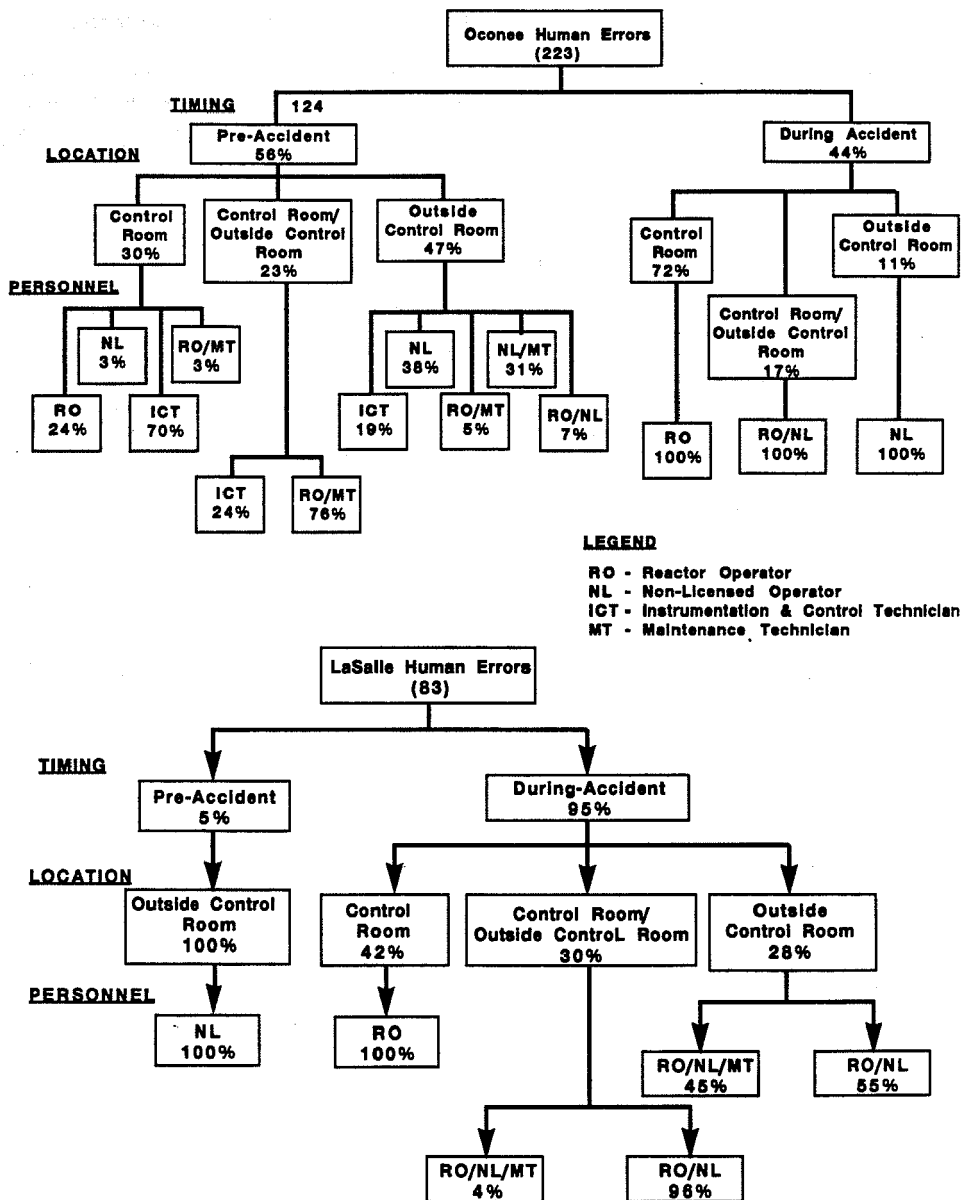


Figure 1 Breakdown of Human Errors in the Oconee and LaSalle PSAs

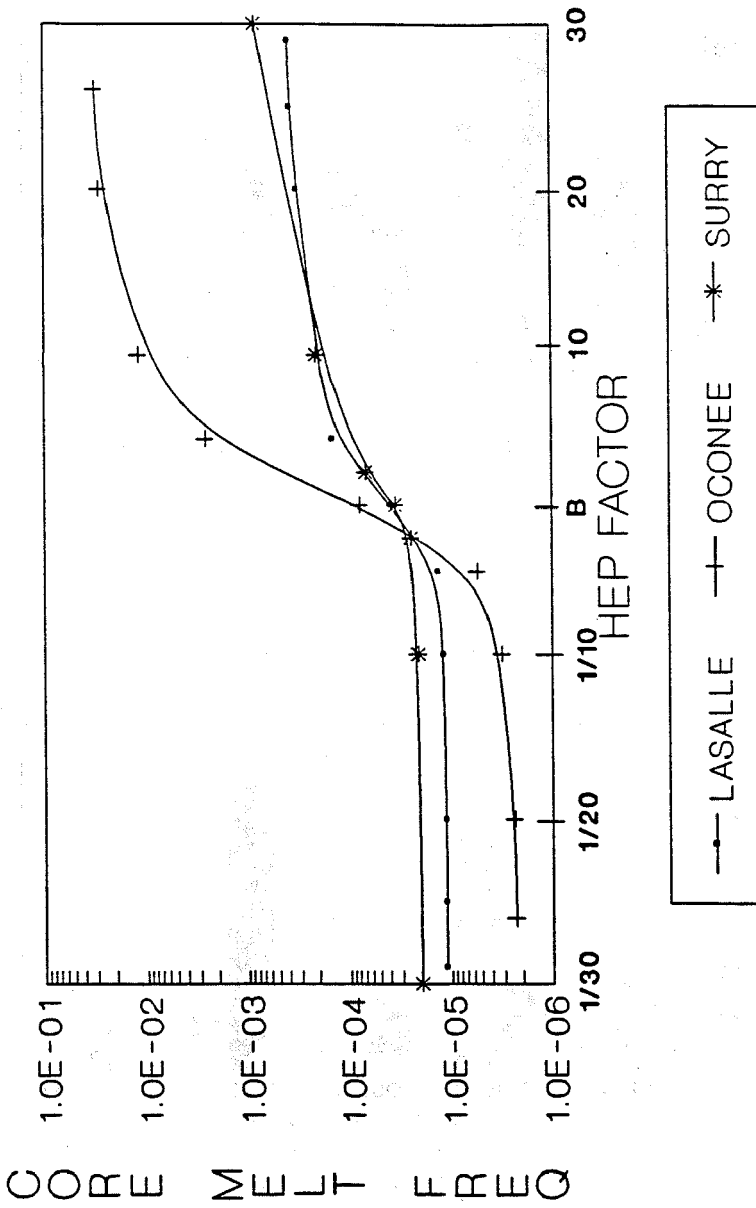
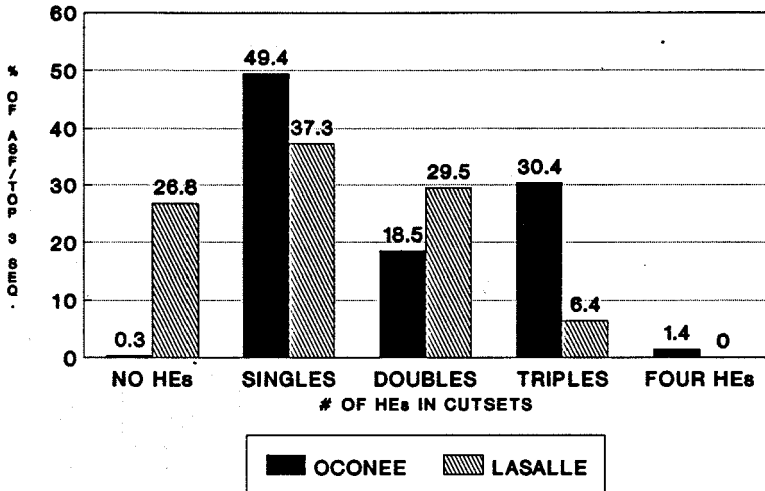


FIGURE 2 - Sensitivity to Simultaneous Variation of All HEPs

HEPs at Base Case



HEPs Doubled

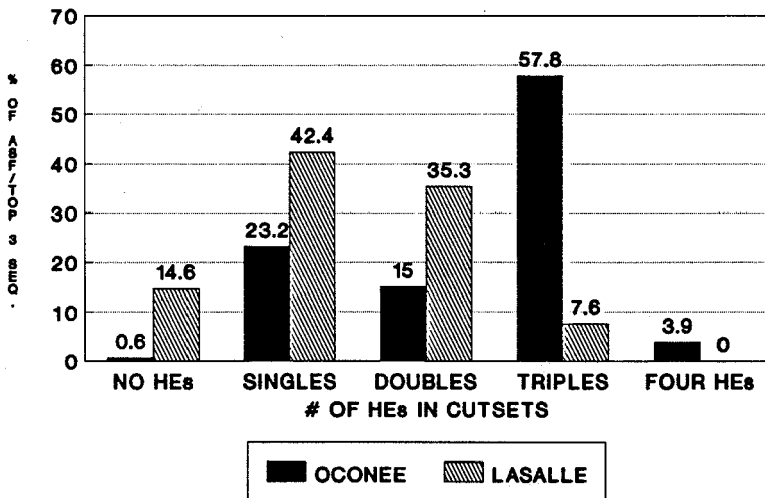


FIGURE 3 - Effect of Doubling Human Error Probabilities on Cutset Distribution

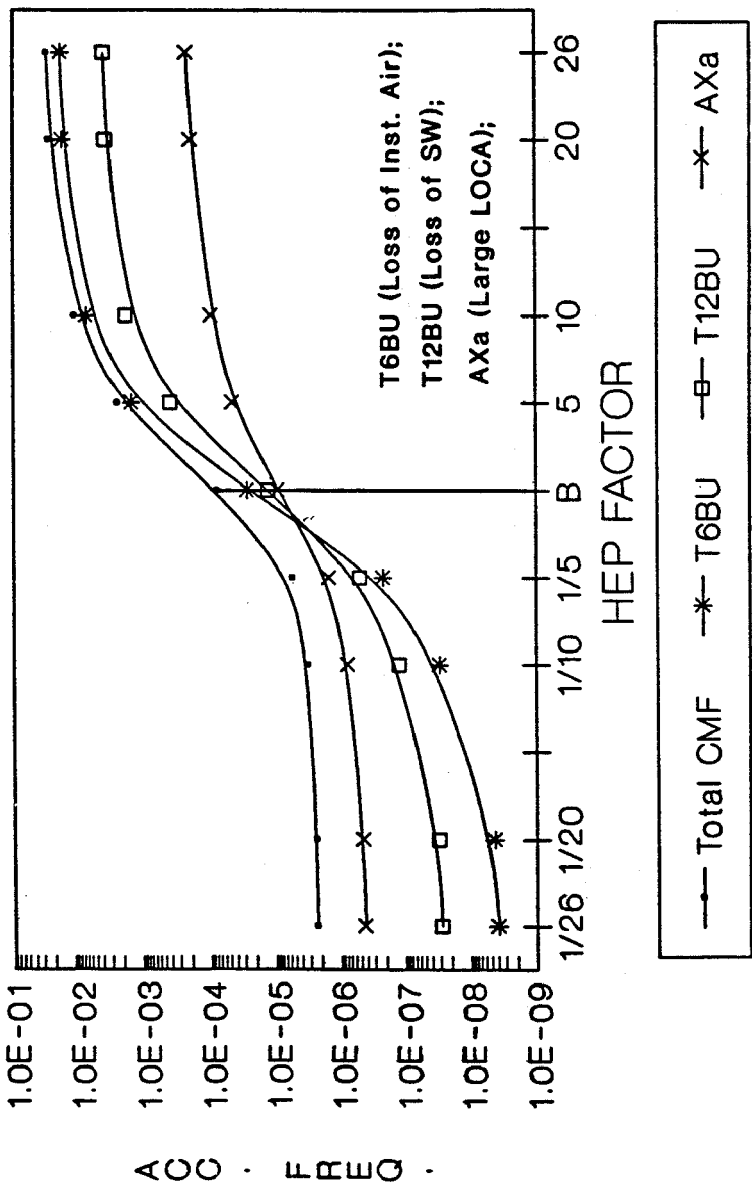


FIGURE 4 - Sensitivity of Dominant Sequences in 0cone to Simultaneous Variation of All HEPs

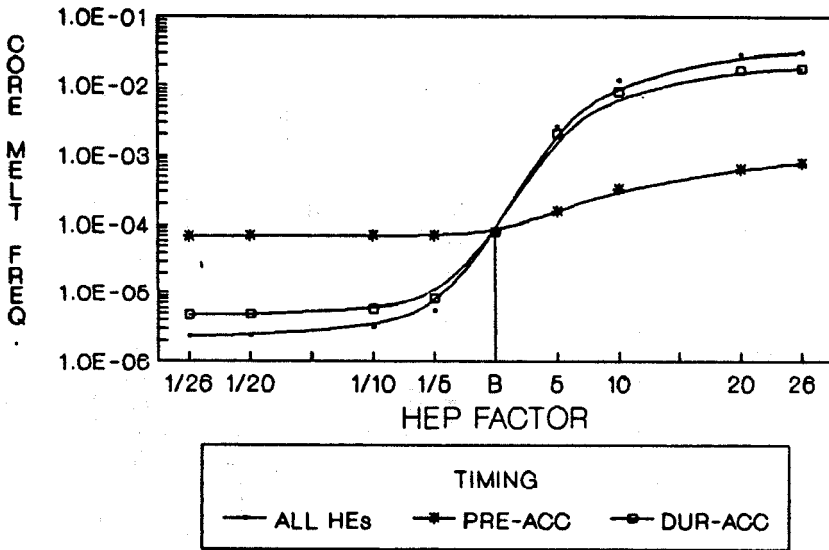


FIGURE 5 - Sensitivity to Pre-accident and During-accident Errors for Oconee

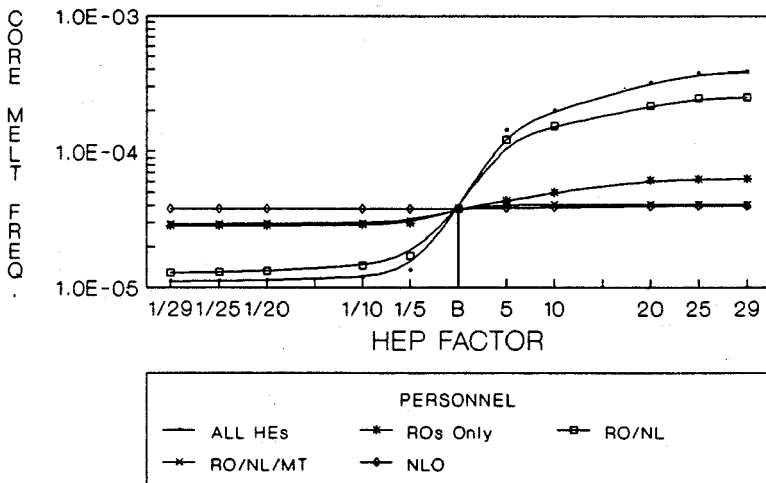


FIGURE 6 - Sensitivity to Personnel Type and RO Interactions for LaSalle

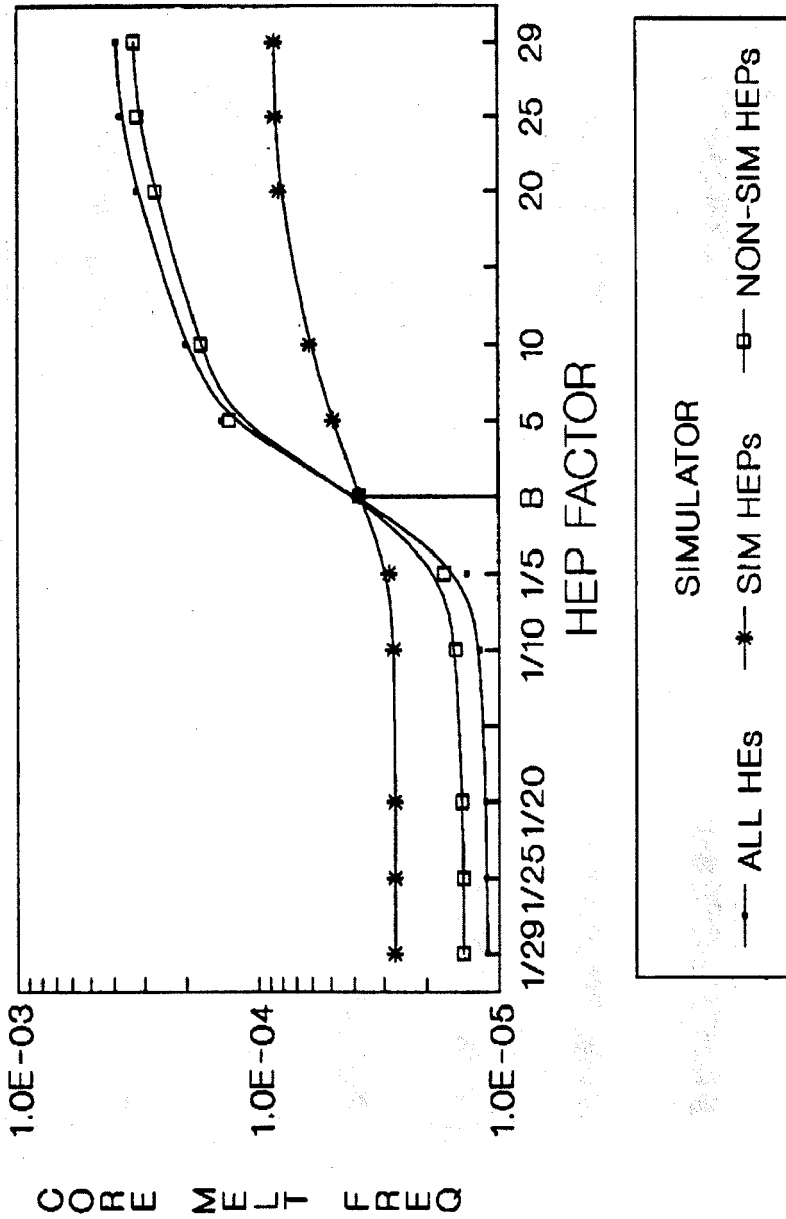


FIGURE 7 - Sensitivity to HEPs Based on Simulator Data for LaSalle

Number of LERs

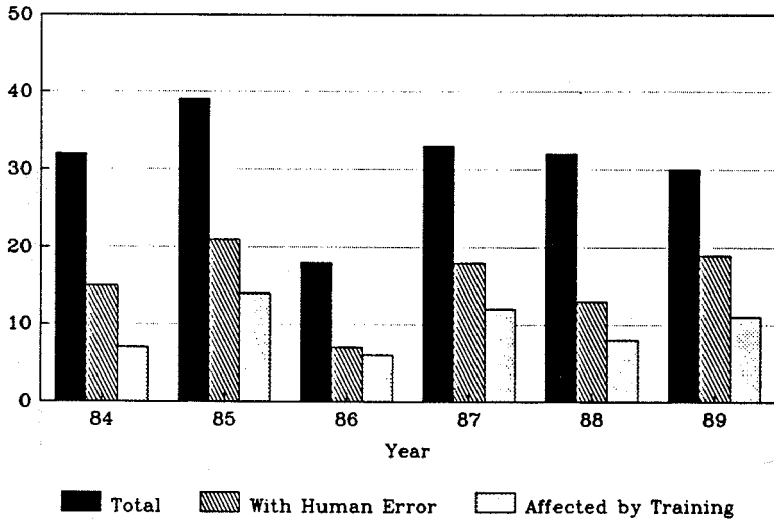


FIGURE 8.a - Number of LERs Involving Human Error

Cumulative CCDP

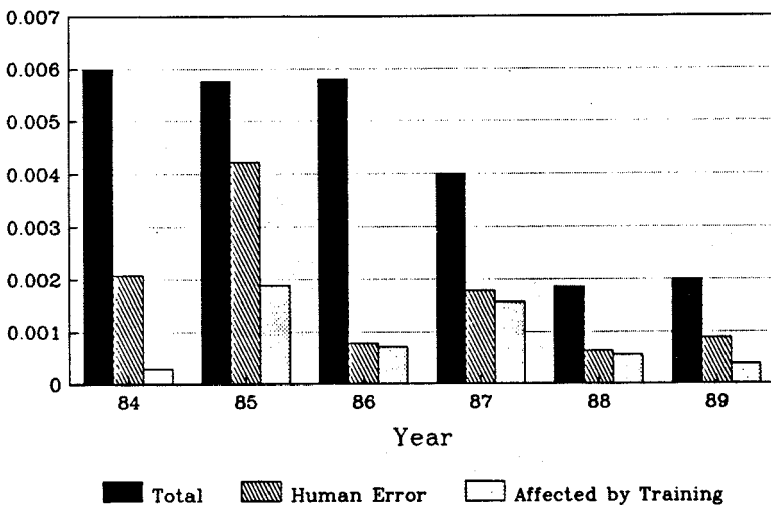


FIGURE 8.b - Cumulative CCDP for LERs Involving Human Error, Excluding 1985 Incident at Davis Besse

Number of Human Errors

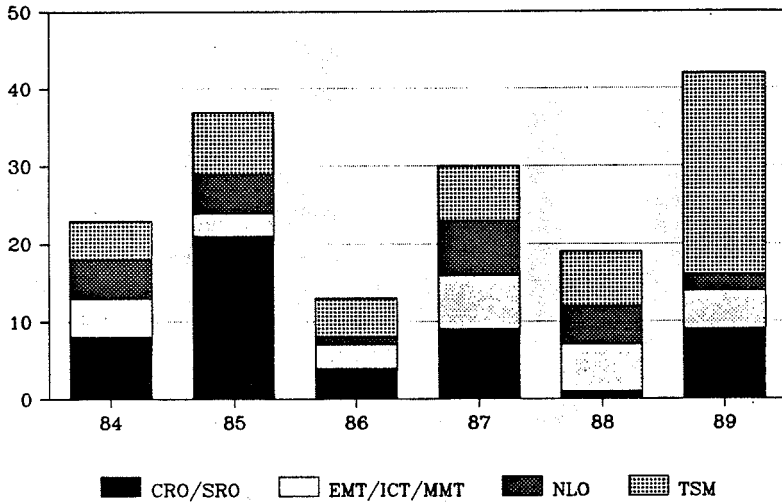


FIGURE 9.a - Number of HEs in ASP Events, by Personnel Type

Human Errors for CRO/SRO

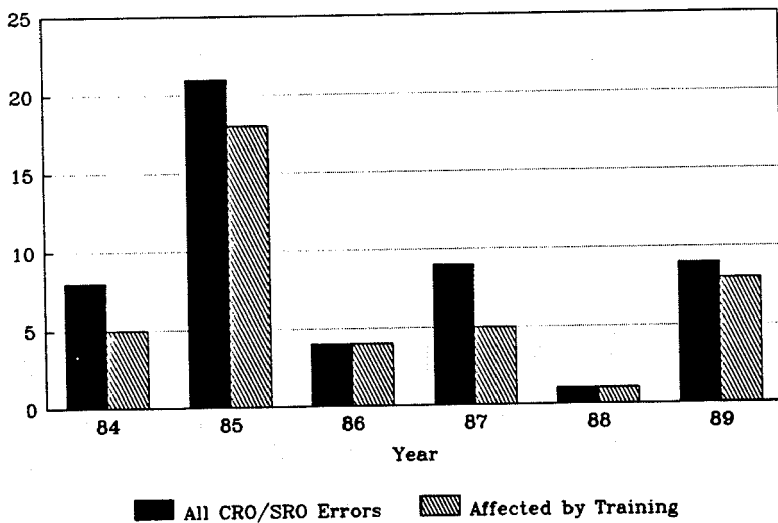


FIGURE 9.b - Number of CRO/SRO Errors Affected by Training

Human Errors for NLO

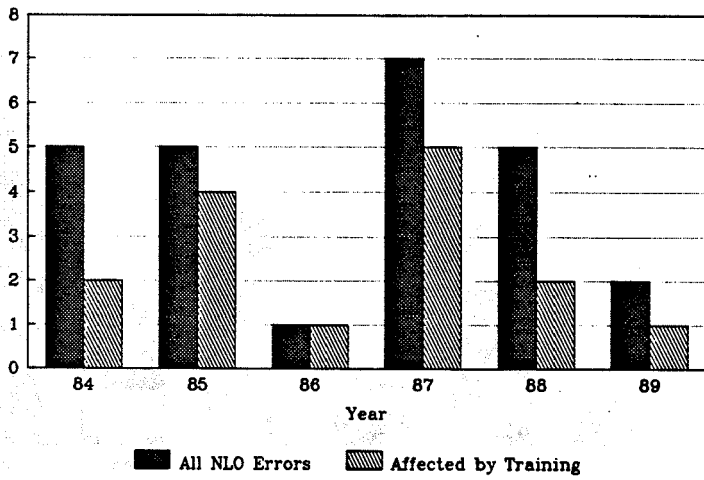


FIGURE 9.c - Number of NLO Errors Affected by Training

Human Errors: EMT/ICT/MMT

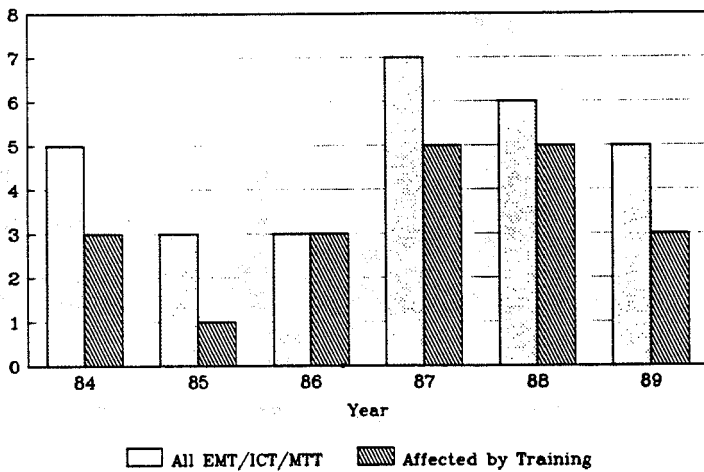


FIGURE 9.d - Number of EMT/ICT/MMT Errors Affected by Training

Human Errors for TSM

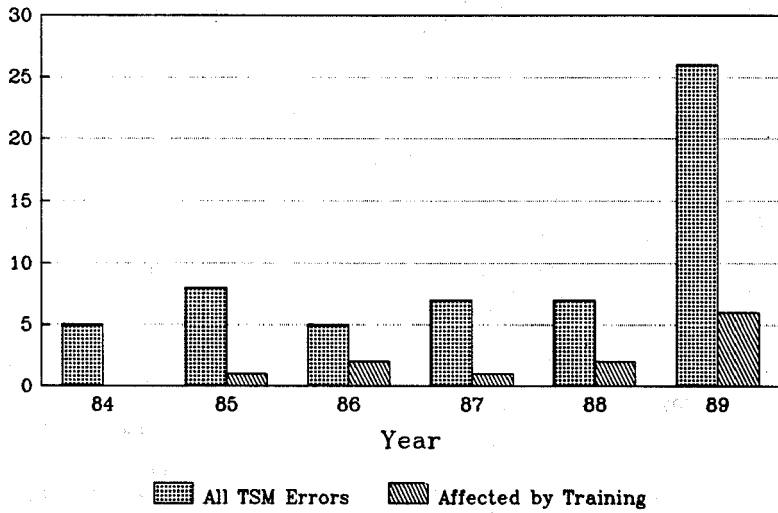


FIGURE 9.e - Number of TSM Errors Affected by Training

Session II-B ; Human Errors

QUANTIFICATION OF HUMAN ERRORS IN LEVEL-1
PSA STUDIES IN NUPEC/JINS

M.Hirano, M.Hirose, M.Sugawara and T.Hashiba
Japan Institute of Nuclear Safety (JINS)
Nuclear Power Engineering Center (NUPEC)
Tokyo, Japan

ABSTRACT

This paper presents the human error evaluation method which is applied to level-1 PSA of typical Japanese NPPs by NUPEC/JINS. THERP method is mainly adopted to evaluate the pre-accident and post-accident human error rates. Performance shaping factors are derived by taking Japanese operational practice into account. Several examples of human error rates with calculational procedures are presented. The important human interventions of typical Japanese NPPs are also presented.

1. Introduction

NUPEC/JINS has been conducting, sponsored by the Ministry of International Trade and Industry (MITI), level-1 and level-2 PSAs for typical Boiling Water Reactors (BWRs) and Pressurized Water Reactors (PWRs) with an aim to provide the regulatory authorities with the useful probabilistic information. We are mainly assessing both 1,100 MWe-class BWR-5, MARK II type plant and 1,100MWe-class 4-loop, PCCV type PWR plant as the typical Japanese commercial power generating plants.

The human error probabilities of level -1 PSA studies are basically assessed by means of THERP method⁽¹⁾. It may be convenient to use ASEP human error data, but THERP method is useful in case the detailed analyses of human interventions are indispensable to investigate their nature and effects

on PSA.

2. Human Factors of NPPs

The human error factors of nuclear power plants are categorized in pre-accident ones and post-accident ones. Typical examples are as follows:

(1) Pre-accident Human Errors

- Miscalibration of instrumentations
- Failures to restore the equipments following maintenance outage/ test

(2) Post-accident Human Errors

Typical human errors are associated with following manual operations.

a) BWR

- Start of standby liquid control system (SLCS)
- Manual depressurization (DEP) at transients
- PCV venting
- Switch of cooling water sources at LOCA
- Change of the operating modes of residual heat removal system (RHR)

b) PWR

- Primary feed and bleed operation
- Secondary cooling through MSRVs
- Isolation of ruptured SG
- Isolation of AFW from broken side SG
- Emergency boration

3. Human Error Evaluation Method

THERP (Technique for Human Error Rate Prediction) method was developed by A.D.Swain and applied to Rasmussen

Report (WASH-1400). This method has been updated and applied to many PSAs. The manual of THERP (NUREG/CR-1278) contains comprehensive and detailed explanations of human reliability analyses.

So, THERP method is useful in case the detailed analyses are indispensable to investigate the nature and effects of human intervention on PSA.

THERP procedure is outlined in Fig.1. The procedure is composed of 4 phases as follows:

Phase 1:
Review plant information and identify human factors important to PSA.

Phase 2:
Clarify the operational procedure and develop HRA(Human Reliability Analysis) event tree.

Phase 3:
Assign nominal HEPs, estimate the relative effects of PSFs (Performance Shaping Factors) and calculate the total HEPs.

Phase 4:
Incorporate the total HEPs to event tree or fault tree.

4. Assumptions to Evaluate HEPs

4.1 Treatment of Diagnosis HEPs

Diagnosis is operator judgement precedent to operator actions to counteract the post-accident plant behavior.

Diagnosis HEPs are derived using the time dependent diagnosis error curve (Swain curve) as shown in Fig.2. The curve is composed of three elements, namely upper bound, lower bound and nominal.

Guideline to use the curve is as follows:

- (1) Use upper bound if:
 - (a) the event is not covered in training.

or

- (b) the event is covered but not practiced except in initial training of operators for becoming licensed,

or

- (c) not all the operators know the pattern of stimuli associated with the event.

- (2) Use lower bound if:

- (a) the event is well-recognized classic (e.g., TMI-2 incident) and the operators have practiced the event in the simulator requalification exercises,

and

- (b) all the operators have a good verbal recognition of the relevant stimulus patterns and know what to do or which written procedures to follow.

- (3) Use nominal HEP if:

- (a) the only practice of the event is in simulator requalification exercises and all operators have had this experience,

or

- (b) none of the rules for use of upper or lower bound apply.

Operators are well trained and passed the stringent qualification test. So, we use the lower bound as a median value except some dynamic diagnoses in very rare accident sequences such as PCV venting after large LOCA and interfacing system LOCA (ISLOCA).

Allowable diagnosis time is mainly obtained from the thermal hydraulic analysis.

4.2 Determination of PSFs

In assessing total HEP for human intervention, various kind of factors such as experience level, stress level are taken into consideration to determine PSFs. PSFs are applied to pickup HEP for each operator action from THERP data base and evaluate total HEP.

The PSFs considered are following levels and dependencies listed in Section 4.3.

(1) Experience Level of Operators

The experience level of operators are classified into two categories, i.e. "skill" and "novice". All operators are assumed to be skill because of good and stringent operator education and training system.

(2) Stress Level of Operators

The stress level of operators are classified into four categories as follows.

- Very low
- Optimum
- Moderately high
- Extremely high

Following stress levels are selected.

- "Optimum" for pre-accident HEPs
- "Moderately high" for post-accident HEPs

(3) Task Level

The type of task is classified into step-by-step task and dynamic task in accordance with the complexity of required operational procedure.

All the pre-accident tasks are deemed to be step-by-step tasks.

The post-accident tasks that require higher degree of man-machine interaction such as decision-making and controlling several functions are

classified into dynamic tasks. PCV venting of BWR and some operator procedures to mitigate ISLOCA fall into this category.

Other post-accident tasks that are routine and procedurally guided tasks are classified into step-by-step tasks.

Estimated HEPs are modified by considering the effect of stress, experience and task levels as shown in Table 1.

(4) Tagging Level

Three levels of tagging are considered as follows.

• Level 1:

A specifically numbered tag is issued for each job. A record is kept of each tag. This record is checked every shift by the shift supervisor. An operator is assigned the job of tagging controller. For restoration, the numbers on the removal tags are checked against the item numbers in the records. (Use lower UCBs -- Uncertainty Bounds)

• Level 2:

Tags are not accounted for individually -- the operator may take an unspecified number and use them as required. In such a case, the number of tags in his possession does not provide any cues as to the number of items remaining to be tagged. For restoration, the record keeping does not provide a thorough checking for errors of commission or selection. Even if an operator is assigned as tagging controller, the position is rotated among operators too frequently for them to maintain adequately controlled tags and records. (Use nominal UCBs)

• Level 3:

Tags are used, but record keeping is inadequate to provide the shift supervisor with positive knowledge of every items that should be tagged or restored. No tagging controller

is assigned.
(Use upper UCBs)

We assess that the tagging level is level-1 because of good operation and maintenance management. The lower UCBs are used as median values.

4.3 Treatment of Dependencies

(1) Dependencies Within Operating Personnel

The level of dependencies within operating personnel are classified into 5 levels and the conditional failure equations on Task "N", given the failure (HEP) on previous Task "N-1" are presented as follows:

- ZD : Zero Dependence
 $F = \text{HEP}$
- LD : Low Dependence
 $F = (1 + 19 \times \text{HEP}) / 20$
- MD : Moderate Dependence
 $F = (1 + 6 \times \text{HEP}) / 7$
- HD : High Dependence
 $F = (1 + \text{HEP}) / 2$
- CD : Complete Dependence
 $F = 1.0$

A shift supervisor, an assistant shift supervisor and several operators are necessary to operate the plant in the control room. Each operator is usually assigned specific tasks. There is no hierarchy within them. So, the dependencies are limited within a shift supervisor, an assistant shift supervisor and an operator. We assessed the level of dependencies within them as follows:

- HD between operator and assistant shift supervisor:

The cooperation between them are routine. So, HD is assumed.
- MD between shift supervisor and

operator/assistant shift supervisor:

The shift supervisor involves in operation only when abnormal situation occurs. So, MD is assumed.

(2) Dependencies within Tasks

The level of dependencies within tasks are classified into 5 levels, which is just the same as those within operating personnel. We assessed the dependencies within tasks as follows:

(a) Pre-accident Human Error

- MD within Miscalibration of Redundant Instrumentations:

The nature of task is to calibrate the sensors that measure the same process variables and are used for the same purposes. The task is performed by one maintainer or one group of maintainers. The miscalibration HEP of first sensor is independent from other task. The miscalibration HEPs of remaining sensors depend upon the miscalibration HEP of the first sensor. The task is step-by-step in accordance with the calibration manual under optimum stress level. So, the dependencies are assessed to be MD.

- ZD for Failure to Restore After Maintenance/Test:

The typical task is represented as to re-open the pump inlet and outlet valves that were previously closed. Both valves should successfully be restored. So, ZD is assumed for conservative purpose.

(b) Post-accident Human Error

Post-accident human interventions are classified into the task performed in series and the task performed in parallel. Success criteria of the task performed in series is "All the tasks should be accomplished to attain the

objectives". Success criteria of the task performed in parallel is "At least one of the redundant tasks should be accomplished to attain the objectives".

We conservatively assume ZD within the tasks performed in series. Most of all tasks fall into this category.

The dependencies within the tasks performed in parallel are assumed to be CD. The tasks that fall into this category is the diagnosis to start the systems manually that are simultaneously failed to start automatically due to the failure of the common initiating signal.

Typical example for BWR is the diagnosis to manually start the high pressure core spray system (HPCS) and reactor core isolation cooling system (RCIC) when reactor water low (L2) signal failed to generate.

Typical example for PWR is the diagnosis to manually start the high pressure injection system (HPI) and low pressure injection system (LPI) when safety injection (SI) signal failed to actuate these systems.

4.4 Recovery of Human Error

Even if an operator fails to operate, recovery actions by other operating personnel in the control room can be expected. (Note that the recovery of diagnosis error is not applicable, because the time dependent diagnosis error curve--Swain curve-- represents the diagnosis error of all the operating personnel in the control room.)

(1) Recovery of Pre-accident Human Error

The recovery model by the inspection checker is applied. The inspection items and activities are as follows:

- Miscalibration of Instrumentation:
Functional tests are performed after the calibration in order to detect

miscalibration.

- Failure to Restore After Maintenance /Test
The status of equipments such as valves are examined by a checker.

(2) Recovery of Post-accident Operating Action Error

The recovery of operator action error by an assistant shift supervisor and a shift supervisor is considered. The recovery model (conditional equation) is the same as that described in dependence model.

4.5 Derivation of HEP Mean Values and Error Factors (EFs)

The HEP data in THERP hand book are median. So, mean values are derived by considering corresponding EFs. We obtain point estimate total HEP mean values firstly, then obtain corresponding EFs by referring to Table 2.

5. Typical HEP Values

Pre-accident HEPs and post-accident HEPs are derived by applying above-mentioned method and assumptions. Typical pre-accident and post-accident HEPs are shown in Table 3 and Table 4.

The detailed calculational procedure of the following HEPs are presented in the calculation sheet.

- Instrument calibration error (BWR)
- Failure to initiate reactor depressurization at transient events (BWR)
- Failure to initiate primary feed and bleed operation (PWR)

6. Important Human Interventions

PSA results show that following human interventions are important to minimize core damage frequencies.

BWR (1,100 MWe, Mark II PCV)

- Reactor depressurization at transient events.

This human error causes the failure of core cooling by low pressure ECCS.

- Initiation of residual heat removal system
- PCV venting

PWR (1,100 MWe, 4-loop, PCCV)

- Calibration of RWSP (Refueling Water Storage Pit) level sensors.

This human error causes the failure to transfer from the emergency core cooling injection mode to the recirculation mode.

- Isolation of auxiliary feedwater to the broken side SG.
- Primary feed and bleed.

7. Conclusion

Human error probabilities are derived based on THERP by taking Japanese operational practice into account. Typical examples are presented. Also presented are important human interventions to minimize core damage frequencies for typical BWR and PWR.

HRAs of important human interventions with THERP method provide us with useful informations regarding to the following items.

(a) Pre-accident Human Intervention.

Importance and effects of the error by the maintainer, recovery by the checker and the operator.

(b) Post-accident Human Intervention.

Importance and effects of diagnosis error, operation error and recovery by the assistant shift supervisor and

the shift supervisor.

These informations are useful for the maintenance management and operator training.

Both governmental research institute and nuclear power industry are conducting human factor research. We are going to update our PSA by applying these outputs in a timely manner.

REFERENCES

- (1) A.D. Swain, et al., "Handbook of human Reliability Analysis with emphasis on Nuclear Power Plant Applications", Sandia National Laboratories, NUREG/CR-1278, August 1983.

Table 1. Modifications of estimated HEPs for the effects of task, stress and experience levels

Human intervention	Task level	Stress level	Modification for mean HEPs	
			Skilled (Note 1)	Novice (Note 1)
• Test • Maintenance • Calibration	Step-by-step (Note 2)	Optimum	HEP × 1	—
• Operations at accidents	Step-by-step (Note 2)	Moderately high	HEP × 2	—
• PCV venting at other than large LOCA	Dynamic (Note 3)	Moderately high	HEP × 5	—
• PCV venting at large LOCA	Dynamic diagnosis	Extremely high	0.22 (EF=5) (Note 4)	—
• Operation at ISLOCA	Dynamic diagnosis	Extremely high	—	0.3 (EF=5) (Note 5)

(Note 1) A skilled person is one with 6 months or more experience in the tasks being assessed. A novice is one with less than 6 months or less experience. Both levels have the required licencing or certificates.

(Note 2) Step-by-step tasks are routine, procedurally guided tasks, such as carrying out written calibration procedures.

(Note 3) Dynamic tasks require a higher degree of man-machine interaction, such as decision-making, keeping track of several functions, controlling several functions, or any combination of these.

(Note 4) This is the actual HEPs and NOT modifiers, and different from THERP table. Namely, the total mean HEPs for all control room personnel are presented including diagnosis error rates.

(Note 5) Same as above except for the experience level. Novice is selected because operators are not trained to counteract ISLOCA by using plant simulator.

Table 2. General guideline for estimating uncertainty bounds for estimated HEPs

Human intervention	Task procedure and circumstances	Stress level	Estimated HEP value (Mean)	Error Factor
• Test • Maintenance • Calibration	Step-by-step procedure conducted under routine circumstances	Optimum	HEP < 0.001	10
			$0.001 \leq \text{HEP} \leq 0.01$	3
			HEP > 0.01	5
• Operation at accidents	Step-by-step procedure conducted under nonroutine circumstances	Moderately high	HEP < 0.001	10
			HEP \geq 0.001	5
• PCV venting at large LOCA • Operation at ISLOCA	Any task performed under extremely high stress circumstances	Extremely high	HEP \geq 0.2 (Note)	5

(Note) This value is smaller than that in THERP table in order to include HEP for "PCV venting at large LOCA" within this range.

Table 3. Typical pre-accident human error probabilities (total HEPs)

Human intervention		B W R		P W R	
		HEP	EF	HEP	EF
Restoration of one manual operation valve		6.7×10^{-5}	10	6.7×10^{-5}	10
Restoration of one motor operated valve (MOV) (manual position holding is not required)		4.4×10^{-5}	10	4.4×10^{-5}	10
Instrument calibration	Single Instrument	6.4×10^{-4} (Analog type)	10	2.3×10^{-4} (Digital type)	10
	Parallel Instruments (1 out of 2) twice logic	1.8×10^{-4} (1 out of 2) twice logic	10	1.8×10^{-5} (2 out of 4) logic	10

Table 4-a Typical post-accident human error probabilities (total HEPs)
(BWR)

Initiating event and mitigating operation	Allowable diagnosis time	Total HEP (Diagnosis error)	E F
1) At small LOCA and transients • Depressurization	20 min	2.8×10^{-3} (2.7×10^{-3})	5
2) At ATWS • Manual SLCS start	10 min	2.8×10^{-2} (2.7×10^{-2})	5
3) At residual heat removal stage			
a) RHR mode			
• Transfer from LPCI mode to SPCS mode at LOCA and transients	12 ~ 24 hr	8.8×10^{-4} (Negligible)	10
• Start SPCS mode at transients	12 ~ 24 hr	1.4×10^{-3} (Negligible)	5
b) PCV venting			
• PCV venting at large LOCA	2 hr	0.22 (0.2)	5
• PCV venting at intermediate/small LOCA and transients	24 hr	2.2×10^{-2} (Negligible)	5

Table 4-b Typical post-accident human error probabilities (total HEPs)
(PWR)

Initiating event and mitigating operation	Allowable diagnosis time	Total HEP (Diagnosis error)	E F
1) At medium LOCA			
• Secondary cooling through MSRVs	30 min	6.8×10^{-4} (2.7×10^{-4})	10
2) At small LOCA			
• Primary feed and bleed	30 min	1.6×10^{-3} (2.7×10^{-4})	5
• Secondary cooling through MSRVs	30 min	6.8×10^{-4} (2.7×10^{-4})	10
3) At SGTR			
• Isolation of ruptured SG (1 action)	30 min	6.8×10^{-4} (2.7×10^{-4})	10
• Primary feed and bleed	30 min	1.6×10^{-3} (2.7×10^{-4})	5
4) Secondary side break			
• Isolation of APW from broken side SG	30 min	6.8×10^{-4} (2.7×10^{-4})	10
• Primary feed and bleed	30 min	1.6×10^{-3} (2.7×10^{-4})	5
5) At ATWS			
• Boration	10 min	2.8×10^{-2} (2.7×10^{-2})	5
• Primary feed and bleed	30 min	1.8×10^{-3} (2.7×10^{-4})	5
6) APW water source transfer	60 min	4.4×10^{-4} (2.8×10^{-5})	10

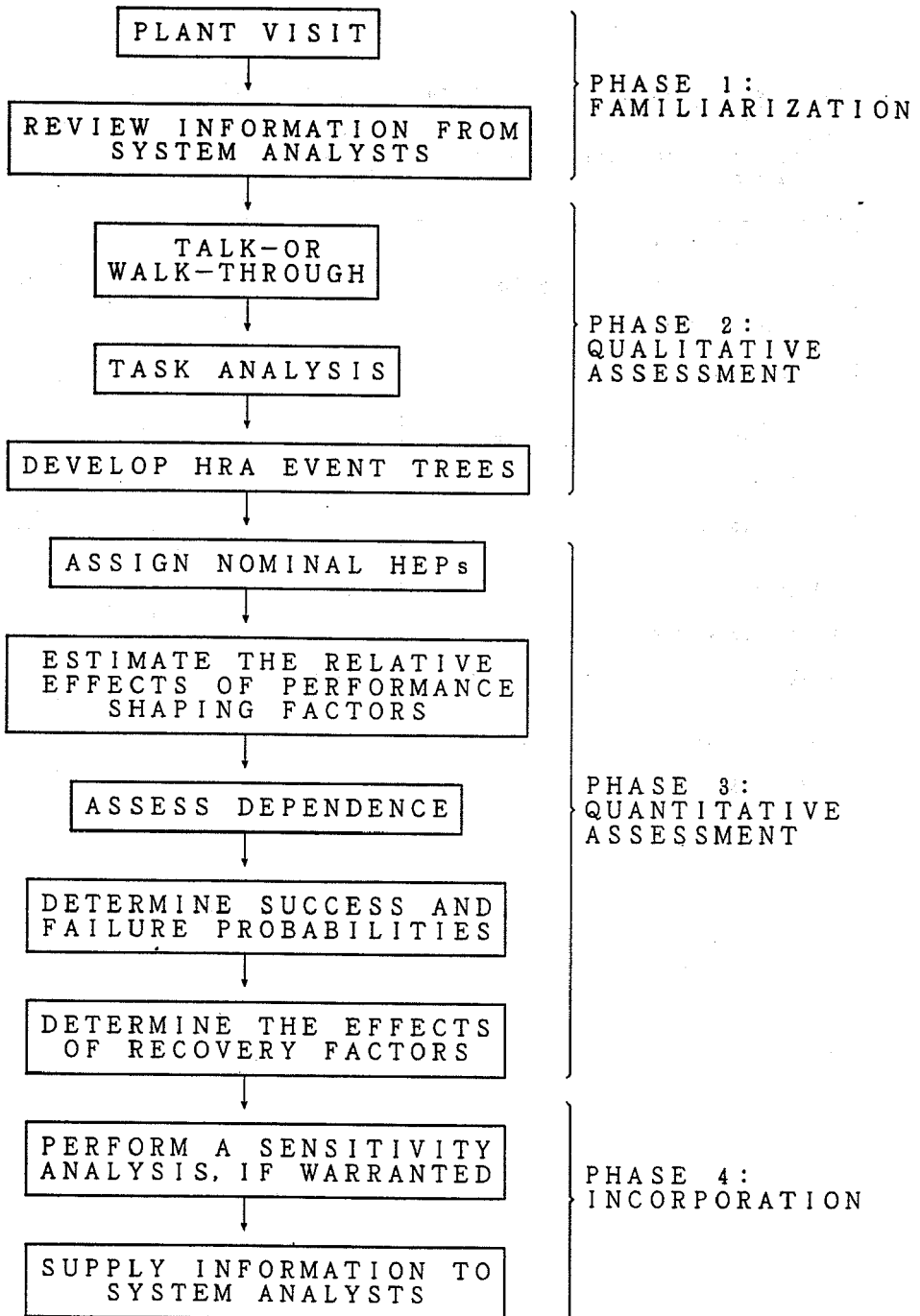


Fig.1 Outline of a THERP procedure

NOMINAL DIAGNOSIS MODEL

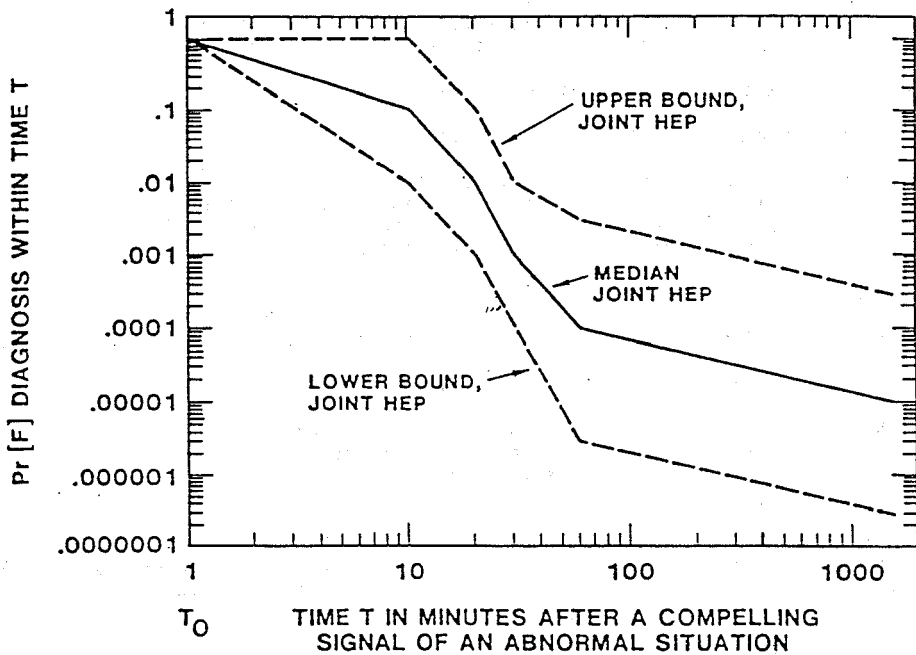


Fig.2 Model of Estimated HEPs and UCBs for Diagnosis Within Time T of One Abnormal Event by Control Room Personnel (From THERP)

(Note) We use "LOWER BOUND, JOINT HEP" as a standard value.

CALCULATION SHEET

The detailed calculational procedures of the following HEPs are presented.

- Instrument calibration error (BWR)
- Failure to initiate reactor depressurization at transient events (BWR)
- Failure to initiate primary feed and bleed operation (PWR)

S1. Instrument Calibration Error (BWR)

(1) Human Error Probability (HEP) Considered

We consider the miscalibration of process instruments automatically to activate ECCS, etc. At first, the HEP of single instrument is considered. Then, the HEP to disable the automatic activation of ECCS, etc. is considered taking activation logic (1 out of 2 twice) into account.

(2) Assumptions

- Task is performed in accordance with the procedure written in calibration manual.
- The calibration manual consists of no more than 10 items and checkoff space is provided.
- The calibration manual is assumed to have no mistake.
- Task is step-by-step and corresponding stress level is optimum.
- PSFs for the instrument are as follows.
 - Analogue type
 - Failure of selection is neglected because the instrument is used for only one purpose.
- The calibration is performed by a maintainer. The task is checked by a checker with check list. Additionally, the task is checked by an operator at the end of the task.

(3) Task Table

STEP	Equipment	Action	Seri/Para
A Rec	Instrument	Calibration Recovery	Parallel

(4) Potential Error List

STEP : A
Equipment :
Action : Calibration
ERROR Branch : A1
ERROR Type : EOM (Error of omission)
Check list is used. But one item is carelessly omitted.

ERROR Branch : A2
ERROR Type : ECOM (Error of commission)
Misread the display indication.

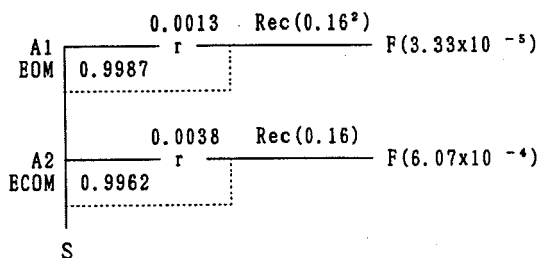
(5) Recovery Factor

The recovery factor by a checker is 0.16 from THERP table No.20.
Combined recovery factor by a checker and an operator is $(0.16)^2$.

(6) HEP Calculation for Single Instrument

HEP TABLE

ERROR Branch	THERP T-NO. (Item No.)	NHEP	EF	STRESS /TASK LEV	BHEP	MHEP	RECOV FACT
A1	20.7(1)	0.001	3	1	0.001	0.0013	0.16^2
A2	20.10(1)	0.003	3	1	0.003	0.0038	0.16
Rec	20.22(1)	0.1	5	1	0.1	0.16	



Total $Fr = 6.4 \times 10^{-4}$

(7) HEP to Disable the Automatic Activation of ECCS, etc.

Activation logic is 1 out of 2 twice. This means that the actuation circuit is composed of the series combination of two parallel circuits. Moderate Dependence is considered for the parallel circuit and factor 2 is multiplied for the series combination. Thus, the HEP for 1 out of 2 twice logic circuit is as follows.

$$F = Fr \times (1 + 6xFr) / 7 \times 2 = 1.8 \times 10^{-4}$$

$$EF = 10 \text{ (From THERP TABLE 20.20 Item 1)}$$

S2. Failure Manually to Initiatr Reactor Depressurization (BWR)

Manual reactor depressurization is necessary to activate low pressure ECCS when all the high pressure ECCS are unavailable at transients.

(1) Diagnosis

Crew should diagnose the occurrence of transients, subsequent failure automatically to activate high pressure ECCS and the necessity of core depressurization in order to activate low pressure ECCS. They should determine the core depressurization by either manual start of ADS (Automatic Depressurization System) or manual opening at least 5 out of 18 safety relief valves (SRVs).

The allowable diagnosis time is 20 minutes. The diagnosis error is obtained from THERP table or time dependent diagnosis error curve (Swain curve). Namely,

HEP = 0.001 (Lower bound, joint HEP)

EF = 10

Mean HEP = 0.0027

(2) Assumptions at Operation

- The operator action is rule-based one that is written in operational procedure.
- The shift supervisor gives the operator appropriate order.
- The ADS activating switches are push button type. So, it is not necessary to consider the operation error of switches. The SRV opening switches are dual direction type. So, operation error should be considered.
- The arrangement of switches on control panel is functionally grouped to prevent operational confusion.
- The layout of switches is mimic.
- The type of switch is commonplace and familiar to operators.
- The task is step-by-step under moderately high stress.
- The recovery actions of both an assistant shift supervisor and a shift supervisor are considered.

(3) Task Table

STEP	Equipment	Action	Seri/Para
A B Rec	Cont. SW	Diagnosis Operation Recovery	Series

(4) Potential Error List

STEP : A

Equipment :

Action : Diagnosis

ERROR Branch : A1

ERROR Type : EOM (Error of omission)

Failure to diagnose the plant status and what to do.

STEP : B

Equipment : Switches

Action : Operation

ERROR Branch : B1

ERROR Type : EOM

Operator fails to recall the oral instruction to initiate depressurization.

ERROR Branch : B2

ERROR Type : ECOM (Error of commission)

Operator fails to correctly select ADS controll switches.

ERROR Branch : B3

ERROR Type : ECOM (Error of commission)

Operator fails to correctly operate ADS controll switches.

ERROR Branch : B4

ERROR Type : ECOM (Error of commission)

Operator fails to correctly select SRV controll switches.
 ERROR Branch : B5
 ERROR Type : ECOM (Error of comission)
 Operator fails to correctly operate SRV controll switches.

(5) Recovery Factor

HD is assumed between an operator and an assistant shift supervisor. MD is assumed between an operator and a shift supervisor. Total recovery factor is as follows.

$$\text{Rec} = (1 + \text{HEP})/2 \times (1 + 6 \times \text{HEP})/7 \quad (= 0.07, \text{ if } \text{HEP} \leq 1.0)$$

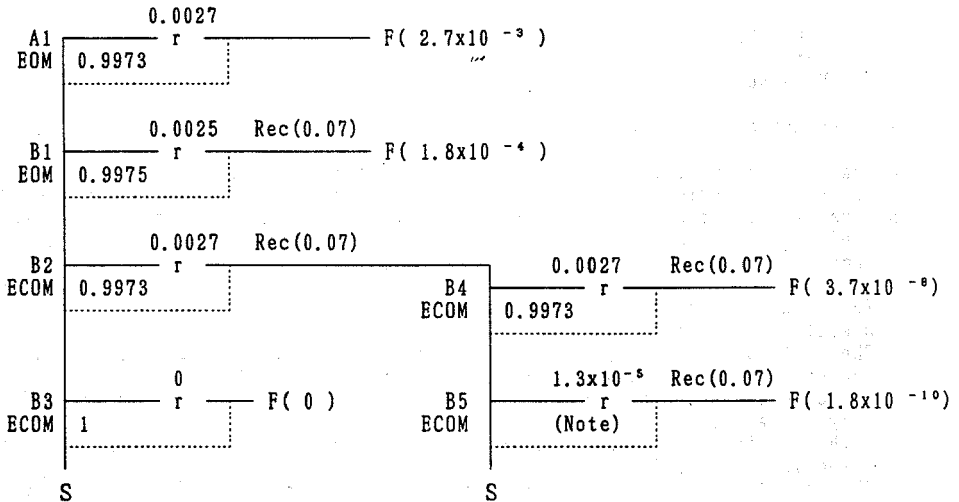
(6) HEP Calculation

HEP TABLE

ERROR Branch	THERP T-NO. (Item No.)	NHEP	BF	STRESS /TASK LEV	BHEP	MHEP	RECOV FACT
A1	20.3(20min)*	0.001	10		0.001	0.0027	
B1	20.8(1)(c)	0.001	3	2	0.002	0.0025	0.07
B2	20.12(4)	0.0005	10	2	0.001	0.0027	0.07
B3		0			0	0	
B4	20.12(4)	0.0005	10	2	0.001	0.0027	0.07
B5	20.12(8)(5)	0.0001	10	2	0.0002	0.00053	0.07

(Values for B4 is applicable to one SRV operation)

* Or time dependent diagnosis error curve (Swain curve) is referred.



(Note) The value represents the failure probability of more than 5 out of 18 SRVs manually to open. HD is assumed for each SRV opening operation failure.

Total F = 2.8×10^{-3}
EF = 5 (From THERP TABLE 20.20 Item 5)

S3. Failure to Initiate Primary Feed and Bleed Operation (PWR)

This operation is necessary to cool the core when both main feedwater system and auxiliary feedwater system are unavailable at small LOCA, SGTR and secondary side break.

After confirming that high pressure injection system (HPI) pump is operating, a operator opens the pressurizer relief valves to depressurize the primary system in order to inject the coolant into the core by HPI.

(1) Diagnosis

Crew should diagnose the occurrence of initiating events and subsequent annunciators to notify the failure of main feedwater system and auxiliary feedwater system. They should decide to depressurize the primary system by opening the pressurizer relief valves (2 out of 2 valves).

Allowable diagnosis time is 30 minutes after the announcement of feedwater and auxiliary feedwater system pump trip or 10 minutes after the announcement of low SG water level status.

The allowable diagnosis time is assumed to be 30 minutes only. The latter announcement is conservatively neglected as a backup information. The diagnosis error is obtained from THERP table or time dependent diagnosis error curve (Swain curve).

HEP = 0.0001 (Lower bound , joint HEP)

Ef = 10

Mean HEP = 0.00027

(2) Assumptions at Operation

Operator is assumed to operate under the directions of shift supervisor. In this case, HPI is assumed to be successfully operating. So, the confirmation of HPI status is not the critical action. Operator action to open the pressurizer relief valves (2 out of 2 valves) is considered to be one set of action. Assumptions related to this action are as follows.

- The task is step-by-step under high stress.
- Operator is enough experienced and skillful.
- The shift supervisor appropriately order the operator to open relief valves.
- The PSFs of relief valve controll switches are as follows.
 - The switches are dual direction type. So, the operation is easily performed by one action.
 - There exists no operational inconvenience caused by stereotypical defects.
 - The layout of switches is mimic.
- The recovery actions of both assistant shift supervisor and shift supervisor are considered.

(3) Task Table

STEP	Equipment	Action	Seri/Para
A	_____	Diagnosis	_____
B	Cont. SW	Operation	Series
Rec		Recovery	

(4) Potential Error List

STEP : A
 Equipment :
 Action : Diagnosis
 ERROR Branch : A1
 ERROR Type : EOM (Error of omission)
 Failure to diagnose the plant status and what to do.

STEP : B
 Equipment : Controll switch
 Action : Operation
 ERROR Branch : B1
 ERROR Type : EOM (Error of comission)
 Operator fails to recall the oral instruction on primary system depressurization.
 ERROR Branch : B2
 ERROR Type : ECOM (Error of comission)
 Operator fails to correctly select RV controll switches.
 ERROR Branch : B3
 ERROR Type : ECOM (Error of comission)
 Operator fails to cofrectly operate RV controll switches.

(5) Recovery Factor

HD is assumed between an operator and an assistant shift supervisor. MD is assumed between an operator and a shift supervisor. Total recovery factor is as follows.

$$\text{Rec} = \frac{(1 + \text{HEP})}{2} \times \frac{(1 + 6 \times \text{HEP})}{7} \quad (= 0.07, \text{ if } \text{HEP} \leq 1.0)$$

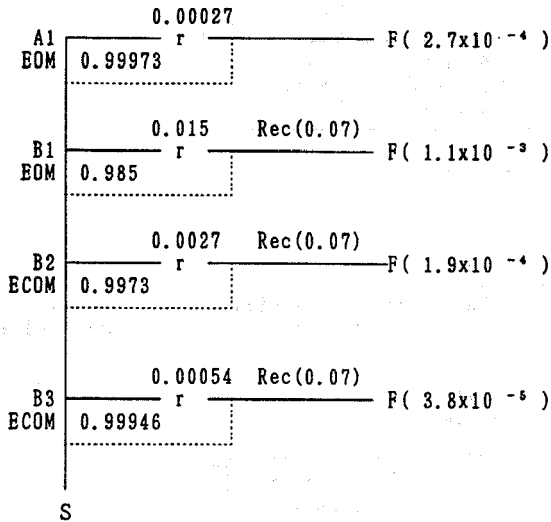
(HD) (MD)

(6) HEP Calculation

HEP TABLE

ERROR Branch	THERP T-NO. (Item NO.)	NHEP	EF	STRESS /TASK LEV	BHEP	MHEP	RECOV FACT
A1	20.3 (30min) *	0.0001	10		0.0001	0.00027	
B1	20.8(2)(c)	0.006	3	2	0.012	0.015	0.07
B2	20.12(4)	0.0005	10	2	0.001	0.0027	0.07
B3	20.12(8)	0.0001	10	2	0.0002	0.00054	0.07

* Or time dependent diagnosis error curve (Swain curve) is referred.



Total F = 1.6×10^{-3}

EF = 5 (From THERP TABLE 20.20 Item 5)

IMPROVED MAIN CONTROL BOARD WITH A BETTER MAN-MACHINE INTERFACE

TOSHIHIRO OSHIBE

NUCLEAR POWER PROJECTS DEPARTMENT

THE KANSAI ELECTRIC POWER CO., INC.

Abstract

Conventional MCB is composed of reactor control board and T/G (turbine/generator) control board. This division is made in accordance with the location of plant facilities.

As compared with this, the improved MCB is partitioned by its function, in other words, by the operational mode for which each board is used. This functional partition gives the configuration that is divided into main control board, reactor auxiliary control board and T/G auxiliary control board.

At the same time, we also adopted extensive use of CRT and the operator can monitor mainly by CRTs.

These two improvements achieved the reduction of the operator's workload and human errors, because the operator can monitor the whole related parameters and can manipulate from the same place almost everytime.

Main control board is used for monitoring and control during the plant condition between HSD (Hot Shut Down) and HFP (Hot Full Power). This board is also used to get the trigger to move to the operational mode of transient or accident.

The other two boards are used during the plant condition between HSD and CSD (Cold Shut Down), and for the peculiar

operation in post-transient/accident.

It has confirmed quantitatively using THERP (Techniques for Human Error Rate Prediction) that this partition and extensive use of CRT realizes the reduction of operator's workload and human errors by comparison with that of the conventional MCB.

The primary function of alarm system misgiving a trigger to decide the next action, so an presentation form with which the operator can grasp the condition at a glance is very useful.

For this reason, we adopted the dynamic priorities alarm system, which can indicate the time-variant importance of each alarm by the color of alarm window. This system uses three colors, red, yellow, and green, for the alarm windows, Red alarm is used as "alarm information", yellow as "caution information" and green as "normal status information". The operator can select the suitable operation only with the "red" and "yellow" alarms, and the total number of the red and yellow alarms taken place is reduced to about one-fifth of that of the conventional system. It is confirmed that this alarm system can greatly reduce the human errors at an abnormal plant condition.

1. INTRODUCTION

In Japan, 18 PWRs are now in operation and 5 others are under construction. The operating plants are keeping relatively high availability factor and low unplanned outage rate. This is attributable to high operation and maintenance quality in addition to high equipment reliability. On the other hand, those under construction have been developed for achieving the optimum functional allocation, which enables the man and the machine to play their maximum roles, and to enhance plant reliability and safety. And such plants incorporate a broad consideration of human factors into plant operation and maintenance as well as upgrading the reliability of equipment.

In this paper, the designs adopted to OHI unit 3 and 4 (1180MWe) which are under construction are summarized. In addition, Advanced PWR (1350MWe) plant under planning is presented.

2. MAIN DESIGN FEATURES

2.1 Improvement of Main Control Room [1]

It is necessary to provide a comfortable working space to the operators in order to reduce their stress, thereby allowing them to constantly exhibit their maximum ability. From this point of view, the shape, color coordination and illumination of the main control room were optimized, in addition to the improvement of the main control board which play the main role of man-machine interface. First, the favorite images of experienced operators were extracted. Then, several alternative designs were evaluated by a quantitative evaluation method using the SD method which is used to evaluate subjective feelings. The final design was determined as follows.

- * Shape : Convex type The ceiling is higher on the center portion than on the peripheral portion
- * Color Coordination : Warm natural (use beige as a basic color)
- * Illumination : The combination of the louver illumination and the spotlights illumination

2.2 Reduction in the Operator's Workload

2.2.1 Functional Partition of Control Board

The conventional control board was composed of reactor and turbine/generator boards. The control switches and monitoring indicators on each board were laid out by the system to which the relevant pieces of equipment belong. While the new type control board is divided into main control board and auxiliary control board. The main control board is used for monitoring and operation during normal operation mode, while auxiliary control board is used for start-up, shutdown and post transient/accident operations. With this control board layout, the operator need not to move around control boards in order to verify the plant status before and after the control actions. Therefore, the workload of operators has been largely reduced. The shape and function of each control board are shown in Fig.1.

Switches and indicators are arranged by the system to which they belong, and are coded by shape and color in addition to labels. They are furthermore designed from the viewpoint of ergonomics (e.g., height, viewing angle).

2.2.2 Automation

(1) Extent of The Limits of Automation

One of the aims of automation is to enhance the plant reliability and safety by reducing operator's workload and human errors, in which the machine (computers) works what it is good at. Automation system is designed for facilitating frequent monitoring and control actions, urgent control actions and diversified control actions. The operation during the period from 15% power up to full power have already been automated.

The following items related to the start-up and shutdown operations in which frequent monitoring and control tasks are required, have been newly automated in recent design by introducing digital control system extensively.

- (1) RCS heat up and cool down
- (2) Main turbine/generator start-up (rolling-up, on-grid and load-up)

- (3) Main turbine turning
- (4) Feedwater pump turbine start-up
- (5) HP turbine steam extraction for cutting in HP heaters

It has already been confirmed that the frequency of monitoring and control actions has been largely reduced by the automation systems mentioned above.

(2) Consideration in Designing Automation System

In designing the automation system, it is important to minimize any effect on the plant caused by the single system failure,, and to be able to be rectified easily. Therefore the control system should be constructed to be dispersed, hierarchal and redundant. Another important point is to give every consideration to the operators. Breakpoint and sequence monitoring systems are incorporated so that the operators may not excessively rely on the automation system, such systems allow the operators to verify the plant status and make their own judgments before proceeding to the next step, and thereby keep maintaining the operator's competence as well as preventing the alienation of man from the machine (automation system). In addition, a countermeasure against the so-called blackbox problem inherent to the automation system is adopted. It is a system, in which the operators can be informed of the on-going automation process being displayed on CRTs, plus voice announcement. The operators can always monitor the on-going status of automation process with these systems (Fig.2).

2.3 Improved System for Information Presentation to Operators

2.3.1 Utilization of CRT

CRTs are designed to improve the information display format, which helps the operators to easily recognize the on-going plant status as well as to form an adequate judgment on plant control. The operators can easily select a display format commensurate to his work from this CRT system. For example, the relevant parameters can be integrated and presented as a function of time in addition to discrete values. This function is particularly useful when an alarm occurs.

During the post trip operation period, the operator has to survey much information for grasping the plant status, the computer surveys the plant status and abnormal components are displayed with red color on CRT. For example, the status of components designed to be automatically activated in the case of plant trip is displayed on one CRT, and failed components which should be started are indicated with flashing for the purpose of calling for the operator attention.

Such improved information display method will be significantly reduced human error rate.

2.3.2 Improved Alarm System [2]

The primary function of the alarm system is to inform the operators of abnormal conditions quickly and exactly. The maximum of about 100 alarms may occur at a time of accident. In order to easily grasp the plant status in such an occasion, a system adopted is capable of changing the color of alarm windows to one of three colors (i.e., red, yellow and green) in accordance with the importance of alarms. This dynamic categorization is carried out by prioritization logic which is based upon a simple physical and/or logical rules. The operators can easily identify the important alarms even in unexpected transients.

Three categories and required operational actions are as follows.

(1) RED : "Alarm Information"

The most important information at a given time, indicating the occurrence of process anomalies or component/system failures. When the "Alarm information" is given, the operator is required to certain operational decision that normally lead to operator's interventions.

(2) YELLOW : "Caution Information"

Information indicating that an automatic component/system action is demanded. When the "Caution Information" is given, the operators have to check the relevant component/system.

(3) GRREN : "Normal Status Information"

The least important information at a given time to which the system does not need to attract operator's attention but which operators may monitor voluntarily.

It appeared from a dynamic verification test using a real-time plant simulator that a total number of red and yellow alarms was reduced to about one-fifth of the conventional alarms (Fig.3).

Operators can respond to transient and accident conditions, focusing their attention on the red and yellow alarms. Human errors will then be reduced.

2.4 Improvement of Maintainability

2.4.1 Redundancy and the Self-diagnostic Function of Reactor Control System

A large number of micro computers are adopted to control the system. Each control system is redundant and switched over from a normal system to a back-up system by the self-diagnostic function of micro computers. And, the plant is designed such that when both normal and back-up systems are failed, the operation is automatically transferred from automatic control mode to manual control one. The introduction of these systems has achieved highly reliable control system. When a print card is failed, the failure mode and the card address are displayed on a plasma display in the control cabinet. The trouble shooting and repair can be done easily within a short period of time.

2.4.2 Introduction of Visual Maintenance Tool

Visual maintenance tool is prepared for the maintenance of digital control system (Fig.4). For example, the confirmation of data and program processing or the correction of the program can be performed by using this tool. The logic of program displayed on CRT is formatted exactly the same as the I&C block-diagram. Therefore, the contents of processing of analog and sequence operation can be confirmed with the same feeling as the conventional I&C engineering. And maintenance staff need not to read and translate the program with the programming language and symbol.

2.4.3 Improvement of Reactor Protection System

In order to avoid unnecessary plant trip during the in-service surveillance test, complete 4-channel and 4-train system and

automatic bypass control logic are adopted. The reactor trip logic is based on 2 out of 4 logics during normal operation. When one channel is in bypass mode for repair or test, the reactor trip logic consists of 2 out of 3. Unnecessary reactor trip during the test can be protected by this improvement and the trip rate is greatly reduced.

The introduction of automatic test equipment largely saves a time for testing I&C equipment during the annual inspection outage, in addition to monthly surveillance test, with resultant in the well improvement of maintainability.

3. STEPS TAKEN FOR INTRODUCING IMPROVED CONTROL SYSTEM

In order to ensure the operating experiences feedback into the design engineering of such automatic control systems, many well-experienced operating and maintenance staffs contributed at each stage of development, design and verification/validation (Fig.5).

These improvements have been made by the following steps.

- (1) In development stage, needs were identified by interviewing with well-experienced operating and maintenance staffs and the evaluation of effects on plant operation and maintenance after the design change was performed for the purpose of reflecting the operation experiences.
- (2) In design stage, the evaluation of equipment reliability, failure effects and the effects after the design change was performed.
- (3) In verification/validation stage, new control system and main control board were connected to a real-time plant simulator at a factory and the function and performance were confirmed by well-experienced operating and maintenance staffs.

4. THE FUTURE TRENDS OF DEVELOPMENT

Human factors considerations for the plants under construction are summarized above. Much more improvements of man-machine interface for advanced PWR are under way.

The advanced and fully computerized main control board is one of many improvements being made. Almost all the conventional instruments (e.g. switches, lamps) are planned to be replaced by a soft control system by utilizing CRTs and other computer-driven

interface devices. This will allow more compact control board and closer interaction between monitoring and control tasks and resultant reduction in human errors.

In addition, knowledge-based operator guidance system [3] is being developed. This operator guidance system supports the operators in monitoring, judging and making decisions during abnormal transient and accident. In this system, a dedicated computer stores the knowledges about operation and machine, diagnoses the cause of abnormal symptoms with these knowledges and displays the guide for operation.

The automation of the control rod control at lower power is being studied for field application.

To keep enhancing the plant reliability and safety, we will make best efforts to improve the man-machine interface continuously.

REFERENCES

- [1] MATSUSITA, K., et al. , "Improvement of PWR Control Room Design", International Conference on Man-Machine Interface in the Nuclear Industry Tokyo, Japan, February 1988.
- [2] FUJITA, Y., et al. , "Improved Annunciator System for Japanese PWRs : Its Function and Evaluation", International Conference on Man-Machine Interface in the Nuclear Industry, Tokyo Japan, February 1988.
- [3] MIZUMOTO, T., et al. , "Development of Knowledge-Based Operator Support System for Japanese PWRs", International Conference on Man-Machine Interface in the Nuclear Industry, Tokyo Japan, February 1988.
- [4] NITTA, T., et al. , "Design Concept for Human Factor in Recent Japanese PWRs", IAEA International symposium on Balancing Automation and Human Action in Nuclear Power Plants, Munich, Germany, July 1990.

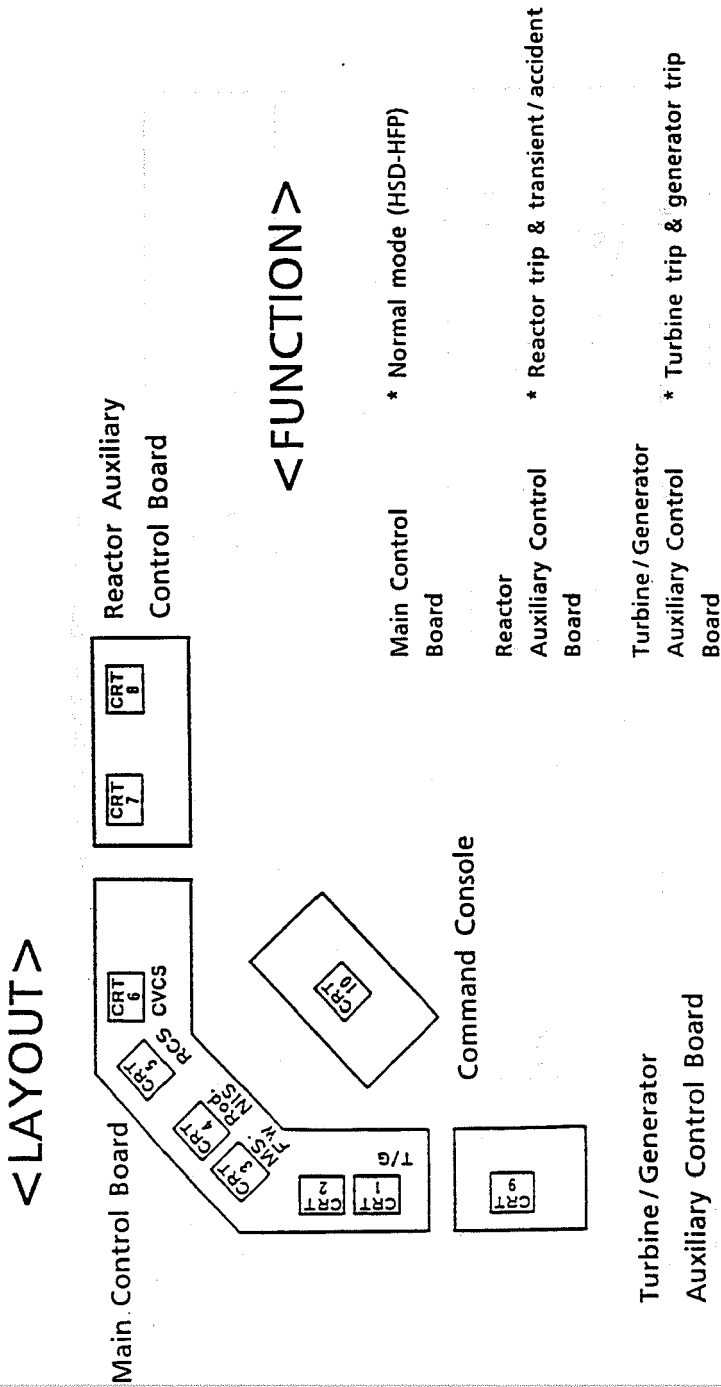


Fig.1 Functional Partition of Control Board

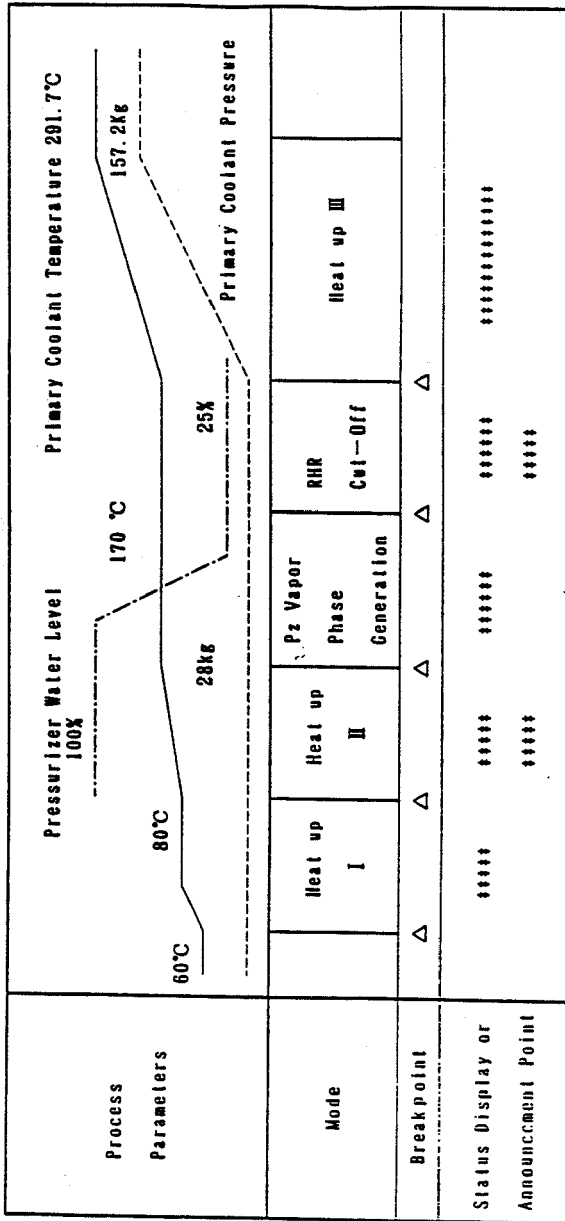


Fig.2 Automatic Heat Up Operation

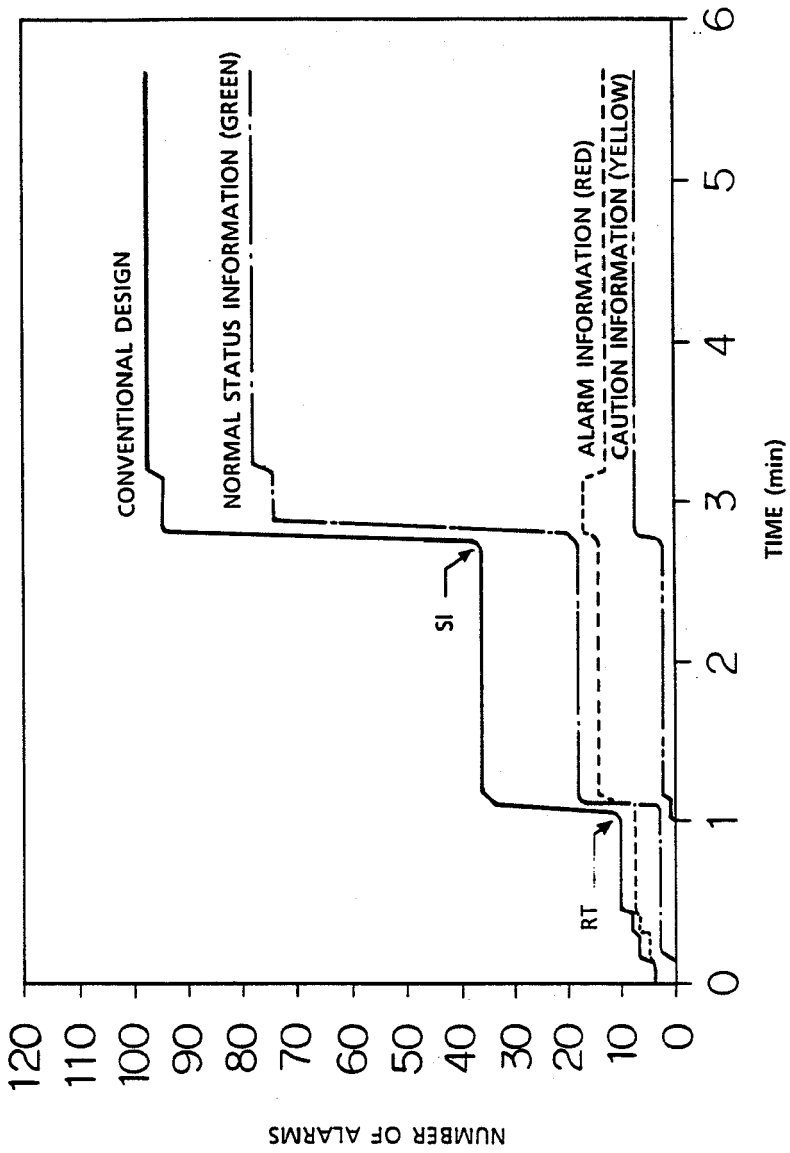


Fig.3 A Number of Alarms Activated During LOCA

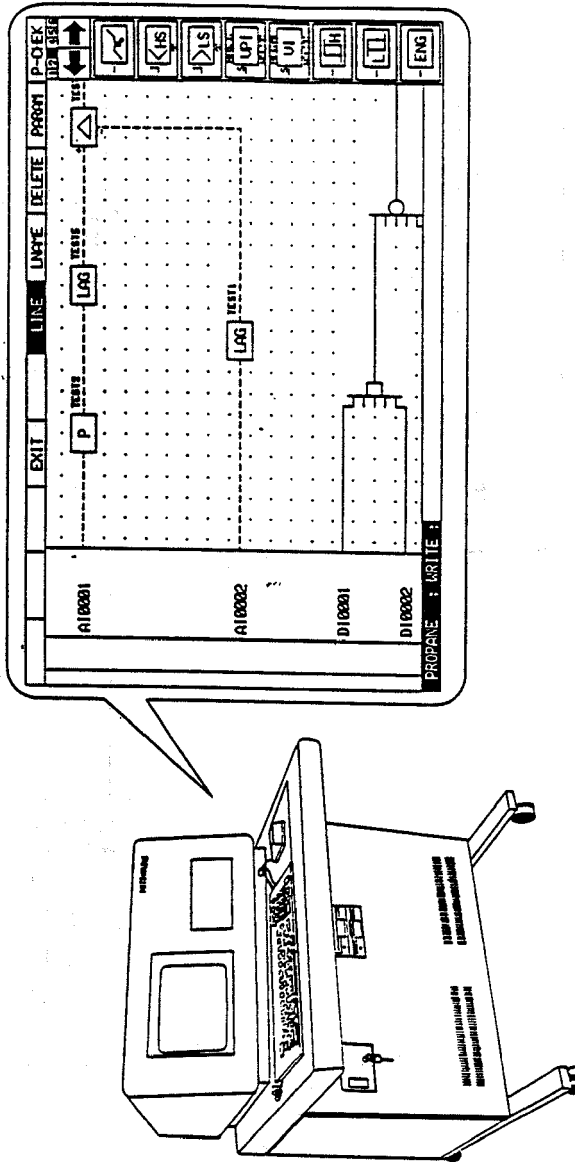


Fig.4 Visual Maintenance Tool

Calendar Year	1982	1985	1986	1987	1988	1989	1990	1991
Plant Construction	<div> <div>▽</div> <div> <div>Power Development</div> <div>Coordination Council</div> </div> <div> <div>Construction Start</div> <div>Reactor Construction Permit</div> </div> <div>▽</div> <div> <div>Turbine Island</div> <div>Basement</div> </div> <div> <div>Commercial Operation</div> <div>▽</div> <div>Fuel Loading</div> <div>Power Receiving</div> </div> </div>							
Digital Control System Development	<div> <div>System Development</div> <div>Basic Design</div> <div>Application Program Verification</div> <div>H/W, S/W Design and Manufacturing</div> <div>System Verification</div> <div>Total Verification and Validation</div> </div>							
Automation System Development	<div> <div>Needs Survey</div> <div>Automatization Boundary Decision</div> <div>Reliability Evaluation</div> <div>System Verification</div> <div>Operability Verification</div> </div>							

Fig.5 Plant Construction and Development Schedules (OHI unit #3)

External Events

Chairman: C. Zaffiro

CSNI WORKSHOP ON "SPECIAL ISSUES OF LEVEL 1 PSA METHODOLOGY"
Cologne, FRG, May 27th - 29th 1991

Issue paper on "External Events"
(CSNI/PWG5 subtask 9.4)

prepared by
Carlo Zaffiro, ENEA/DISP, Rome, Italy

1. Problem description.

In PRA studies for nuclear power plants, external events are those potential accident initiators that are produced on site by natural phenomena or by hazardous activities in the nearness. These events have the common characteristic to threaten in the same time both the plant structural integrity and system operability. Therefore, because of their common cause effect, they might significantly contribute to the estimated risk, being the contribution strictly dependent on the nature and strength of the involved phenomena and also on the plant response to possible consequent accidents.

Methods for assessing accident sequences initiated by external events have been attempted since the WASH-1400 Reactor Safety Study. In practical applications, however, they have resulted of difficult interpretation in the outcomes, due to the uncertainties of the analysis. Uncertainties exist for both the not exhaustive understanding of the physical phenomena associated with the events and the lack of experience on the plant behavior during the accidents.

The past experience on PRAs has shown that, whatever accident initiators have been considered (internal or external events), core melt frequencies are less sensitive to uncertainties than other probabilistic indicators (such as those referred to containment failure, large releases, external sanitary consequences and damage to property). However uncertainties are generally larger for external events than for internal events. That requires much attention be paid when considering the importance of the external events contribution to the assessed core melt frequencies.

Estimates of the external events contribution to the frequency of core melt accidents are currently made in Level 1 PSAs. The methods of analysis, in principle, are similar for all events. They require investigations to determine the on site hazard to the plant, as well as several specific analyses to develop data bases and success criteria for assessing the plant vulnerability and quantifying the probabilities of core melt accidents provoked by the events.

Indeed, because of the uncertainties in the analysis, the treatment of external events in Level 1 PSA is not as complete nor as definitive as in the treatment of internal events. In addition the current studies and research programmes on the physical phenomena to be examined for the

various events have not reached the same development status, and are still in progress. Therefore differences exist in data banks and methods of analysis depending on both the severity and recurrence period of the concerned event. In order to exploit at best the available knowledge in this field, recent applications have used a structured and formalized elicitation process of expert opinion, like in the analysis for the less known severe accidents phenomena. Uncertainty analyses using stochastic techniques (like the Monte Carlo methods and the Latin Hypercube Sampling algorithm) were also made for assessing the degree of the core melt frequency variability generated by the uncertainties of both the used data and assumptions adopted in the models.

At present an attempt to review the status of the art on the treatment of external events in Level 1 PSAs is being carried out in the ambit of the CSNI/PWG5 activities. As result of the work performed so far, a preliminary report has been drafted. The report examines the methods currently used for the seismic, the flooding and the fire events, that in past PRAs were treated more extensively than other events (internal fires are usually considered in PRAs as external events because of their similar characteristic to provoke common cause effects).

The present "issues paper" briefly summarizes the main conclusions of the CSNI/PWG5 report. It also addresses the areas that need of more investigations.

2. Documents stating the status of the art.

In the CSNI/PWG5 draft report on the "Status of the Art of Level 1 PSA" concerning "External Events" references are made to documents that are available in the literature. The references are subdivided according to the following three topics:

- the seismic analysis;
- the analysis of accidents resulting from external floods;
- the fire risk analysis.

The long list of documents indicated in the above mentioned report, shows that the external events have been matter of interest for many studies and PRA applications. However, the most complete and updated analysis, including an extended uncertainty analysis, is the one contained in the NUREG 1150 final report. The reference document of this report is:

- NUREG 1150 "Severe Accidents Risk: An Assessment For Five U.S. Nuclear Power Plants". Vol.1, Final Summary Report, and Vol.2 Appendices A, B and C; U.S. Nuclear Regulatory Commission, December 1990.

A detailed description of the procedures used in this report for the external events analysis is contained in the following document:

- NUREG/CR 4840 - SAND88 3102 "Procedures for the External Event Core Damage Frequency for NUREG 1150" by M.P.Bohn and J.A. Lambricht; Sandia National Laboratories, November 1990.

The final version of the NUREG 1150 report follows the publication of

two previous drafts and incorporates comments of two peer review groups, sponsored by the U.S. Nuclear Regulatory Commission and the American Nuclear Society respectively. Some comments, in particular, are dedicated to seismic events and are reported in the following document:

- NUREG 1420 "Special Review Committee of the Nuclear Regulatory Commission on the Severe Accident Report (NUREG 1150)" U.S. Nuclear Regulatory Commission, August 1990.

A complete risk analysis from fires, always limited to the above plants, is also included in the NUREG 1150 report, whereas the analysis of accidents induced by external floods has been considered only on a qualitative basis through bounding evaluations. However, the best status of the art on this topic may probably be found in the following document:

- NUREG/CR 5042 - UICD 21233 "Evaluation of External Hazards to Nuclear Power Plants in United States" by C.Y. Kimura and R. J. Budnitz; Lawrence Livermore National Laboratory, December 1987.

In that report a review is made on methods to assess the reference design basis and to estimate the frequencies of the major accidents induced by external events, as performed in some existing PRAs.

3. Issues on the seismic analysis.

3.1 Status of the art.

Chapter 1 of the CSNI/PGW5 draft report on external events contains a short review of the basic approach to determine the core melt frequency of accidents provoked by earthquakes. Here following are summarized some considerations made in that report on the status of the art of the analysis.

i) Hazard evaluation.

The seismic hazard is a curve correlating the intensity of the earthquakes, expressed in terms of on site peak accelerations, with their frequency of occurrence. Usually the hazard is determined through a statistical treatment of the available data supported by geo-seismotectonic investigations and theoretical studies. The analysis is affected by considerable uncertainties since the available data and information are not sufficient for fully understanding the physical phenomena involved during earthquakes and thus for developing reliable models. In this regard expert judgments are often used, if necessary, to postulate hypotheses and assign probabilities. Large uncertainties could make the results of difficult interpretation and possible misuse. Less uncertainties, however, exist and more valid results are obtained for sites located in regions with more seismic data, especially if data are referred to longer periods of the seismic history.

Accounting for the uncertainties, various values of the on site peak accelerations are obtained, especially in the field of large earthquakes. Thus families of hazard curves may be produced. That is the case of the

NUREG 1150 report which considers two families of curves, provided by the LLNL and EPRI respectively (see ref.11 and 12 in chapt.1 of the CSNI/PGW5 draft report). The large spreading of the probability values in the lower part of these curves underlines the difficulties to assess the hazard from very strong earthquakes.

The review of methods to assess the on site seismic hazard points out that low probability numbers associated with large earthquakes might not be significant. The meaningfulness level, however, should not be the same in various regions of the world with different seismicity, since the available seismic data and information could have a different consistency. For instance, because of the brevity of historical records, the probability of large earthquakes in U.S. could be judged to be not significant below values of the order of 10^{-3} to 10^{-4} per year, whereas in some European countries (e.g. Italy) the meaningfulness level of the estimated probabilities could be extended down to values of about 10^{-4} to 10^{-5} per year. In general the events associated to the lowest but still significant probability values are considered in the regulations for defining the Safe Shutdown Earthquake (SSE).

ii) Fragility analysis.

The seismic fragility analysis provides the failure probability functions for the plant structures, systems and components under various seismic loads. In such analysis the seismic loads are usually expressed as peak ground acceleration, and fragility data represent the medium values of the acceleration capacity to withstand the loads. Fragility functions, therefore, account for the variability of the seismic response in a given structure, system or component, due to the uncertainties on how the ground motion appears at the plant basement and propagates from the subsoil to the various part of the plant.

Fragility functions are usually developed through the treatment of data and information obtained from:

- observations during earthquakes;
- seismic qualification tests according to usual standards;
- tests on shaking tables simulating actual or theoretical earthquakes;
- calculations with theoretical models.

The treatment is in general a statistical combination of the above data and information supported, if necessary, by expert opinions.

Fragility data have been developed and collected in the past by several scientific organizations, as documented in the available literature (see the ref.13, 14, 16 and 17 in chapt.1 of the CSNI/PGW5 draft report). Generic data, used in some past PRAs, are in particular provided in the NRC document "PRA Procedure Guides" (see ref.2 in chapt.1 of the CSNI/PGW5 draft report). An updated list is contained in the NUREG/CR 4840 report mentioned in par.2.

iii) System analysis.

The seismic system analysis calculates the frequencies of accident sequences, plant damage states and core melt at various ground motion levels selected from the site seismic hazard. The method is conceptually identical to the traditional and well established method of the fault

trees and event trees analysis used for internal events. There are, however, some differences due to the features of the seismic events that act as common causes of failure of the various part of the plant, to be combined sometime with other non seismic failures.

In the system analysis the failure modes and probabilistic failure criteria for important safety systems, structures and components, are mostly determined using the current fault tree techniques and fragility data. The plant response to the site ground motion is also assessed in order to determine the seismic loads in the various part of the plant where the above systems, structures and components are located. The used models should represent the seismic structural behavior of the plant, including the soil structural interactions. Iterative calculations at various levels of the ground motion intensity are usually made, implying increasing and high variable results for the highest less probable values. The variability of results mainly comes from the uncertainties in the hazard analysis and in the failure (seismic and non seismic) rate data, including human errors. Sensitivity studies and uncertainties analyses are made at last to identify dominant contributors to the estimated core melt frequencies and assess the variability range of the final results.

Results from some past PRAs have shown that the seismic core melt frequencies might represent a significant contribution to the global core melt frequency (see table 1 and fig. 5 in chapt.1 of the CSNI/PGW5 draft report). In addition the uncertainties in the estimated values are considerably large and overlap the uncertainty range of results from the internal events analysis.

3.2 Areas where improvements are necessary.

The review of the status of the art confirmed that much work is still needed for decreasing the uncertainties of the seismic analysis, especially in the field of the hazard evaluation. Here following are mentioned the main areas to be investigated for improving the confidence level of the final results.

i) Hazard evaluation.

Current methods for determining the site seismic hazard should be improved in the following areas:

- identification of the seismic sources and determination of the recurrence frequencies for strong earthquakes;
- assessment of the propagation phenomena from the seismic sources to the site for developing realistic and update relationships between site ground motion and relevant earthquake parameters (e.g. peak accelerations vs hypocentral distance, magnitude, etc.);
- evaluation of the site ground motion features that are relevant to the plant response analysis (time histories, response spectra etc.).

Instrumental data and observations should be extensively collected during actual earthquakes in order to improve and convalidate theoretical models and empirical correlations.

i) Determination of the flooding frequencies.

Methods for determining frequencies of various on site flooding levels rely on the development of the Probable Maximum Precipitation (PMP), given that, in general, a severe local precipitation is the controlling event on all the concerned sites (see ref.1 in chapt.2 of the CSNI/PGW5 draft report). For the rarity of the events, however, PMP can be realistically evaluated within the range of the available historical records. A period of about 100 years, corresponding to a frequency value of about 0.01%, is the return period generally used if data are consistent. For larger return periods calculations become difficult and uncertain, especially when, during the flooding, a number of rare phenomena are expected to affect the site and must be correlated together. Statistical methods may be used to treat the available data and information, and expert judgements are often needed to support the analysis. Currently, bounding calculations based on conservative models and hypotheses that are judged to be acceptable by the experts, are used for quantifying defensible frequency values. Moreover, some methodology is available to perform calculations in a formal sense (see ref. 13 in chapt.2 of the CSNI/PGW5 draft report). All analyses, however, do not avoid the uncertainties due to the lack of data and correlations among the involved phenomena.

Site flooding might also occur because of upstream dam failures. Although realistic dam failure probabilities in extreme conditions cannot be easily determined (for the difficulty of accounting of all the involved factors, such as dam location, construction, design capability, etc.), data on dam failures that are available in the literature could only justify values not greater than 10⁻³ per year (see ref. 12 in chapt.2 of the CSNI/PGW5 draft report). Little credit, however, is in general given to failures of modern and well-engineered dams.

From the above considerations it results that at present methods to assess the frequency of on site high flooding levels are valuable only in the range of historical data. These methods are also used in the regulations to determine the Design Basis Flooding Level (DBFL).

ii) Plant system analysis.

The plant system analysis intends to estimate the probability that, given a flooding event large enough to cause a damage on the plant, core damage accidents will occur. To this purpose the analysis requires the development of plant event trees with the use of probabilistic failure data for relevant plant safety functions at various flooding levels. In practical applications these data, also referred as to flooding fragility data, cannot be easily obtained, since at present a realistic world data base does not exist, nor theoretical models are available for assessing the system and component behavior during exceptional inundations. In place of theoretical calculations, expert judgements may be used for making conservative assumptions in bounding analyses, and for estimating probabilities as well.

In the PRA literature there are a few cases in which core melt accidents produced by external floods have been extensively treated, mostly in a

Particular care should be taken when estimating probabilities for large earthquakes, willing to ascertain to what extent these unlikely events may be considered still conceivable, without impairing the meaningfulness of the analysis.

ii) Fragility analysis.

The effort to collect further and updated fragility data should continue especially in the field of the high accelerations, taking also into account relevant ground motion parameters (soil features, frequency spectra, etc.) The aim is to make available an enlarged and exhaustive list of generic data to be used in PRAs. Current methods, in particular, should provide improved failure data on :

- electric components (including relay chatter and circuit breaker trip);
- piping at various plant locations;
- interbuilding piping (caused in particular by soil failures and liquefaction).

Methods should provide the uncertainty range within which data have been actually developed.

iii) System analysis.

System analysis should be improved in the determination of the seismic failures modes of structures and components for various ground motion levels. At the present status of the art the following areas need of more investigation:

- soil structures interactions;
- damping levels beyond design basis;
- models for specific seismic events (different time histories and response spectra etc.);
- combination of failure modes (cascading failures of piping supports, simultaneous failures due to correlated responses, induced fires etc.);
- human behavior during earthquakes.

Research should provide updated methods for generating realistic and best estimate values of the seismic loads in various parts of the plant where relevant systems, structures and components are located. The loads should represent all aspects of interest for the failure modes of such systems and components or supporting structures, accounting for the uncertainties.

4. Issues on the flooding analysis.

4.1 Status of the art.

In chapter 2 of the CSNI/PGW5 draft report on external events a short review is made on the probabilistic methods to assess the core melt frequency of accidents caused by external flooding. Here following are some considerations on the status of the art regarding this analysis.

bounding way. The results have shown that the assessed core melt frequencies are in general very low and sometimes insignificant (see table 1 in chapt.2 of the CSNI/PGW5 draft report). These applications, however, do not contain uncertainty analysis. Uncertainties, mostly coming from the on site flooding hazard, could be consistently high and could cause doubtful results, especially if used for comparison purposes on different sites.

4.2 Areas where improvements are necessary.

Although past PRAs have shown that the contribution to core melt frequency from flooding events is very low, some additional investigations could be still needed, especially in the field of the more complex and rare natural phenomena. Here following are reported some considerations regarding the areas of concern.

i) Determination of the flooding frequencies.

In general all exceptional natural phenomena that may provoke high site flooding levels (severe precipitations accompanied by water run-off from rivers and lakes, storms, strong winds tides, etc.), are surveyed by national and worldwide meteorological organizations. Expert panels usually review the status of knowledge on the above phenomena, and suggest studies for previsional models. For PRA applications, therefore, expert judgements are continuously updated by these ongoing activities. Additional investigations could be requested only in some specific case because of the features of the concerned site.

ii) Plant system analysis.

The limited applications of the approach to calculate the core melt probability in case of exceptional site flooding (beyond DBFL) do not allow to identify particular areas of investigation. On the other hand bounding calculations have demonstrated that enough capacity to achieve safe shutdown conditions could be still available also in case of the total loss of equipment and structures threatened by a severe inundation. With the exception, perhaps, of some particular case, at the moment no additional investigations seem to be necessary.

5 Issues on the fire risk analysis.

5.1 Status of the art.

Chapter 3 of the CSNI/PGW5 draft report on external events, contains a review of methods currently used to assess the contribution of fire events to both the core melt frequency and the containment failure probability. Here following are summarized some considerations on the status of the art of the analysis.

i) Identification of relevant fire zones and determination of fire frequencies.

Relevant plant areas that are sensitive to fire, and existing barriers separating various plant rooms and compartments, are usually identified on the basis of a comprehensive examination of plant layout drawings validated by specific plant visits. Fire areas of concern are those which have either safety related equipment or power and cables for that equipment.

In past PRAs fire frequencies were determined from data that are available from the operating experience on nuclear plants. The few available data were reviewed and treated with current statistical techniques. Fire frequencies in specific areas and small rooms contained in large compartments were obtained through partitioning methods of the available fire frequencies of the compartments. Theoretical models on fire propagations and Bayesian estimations were used to support the analysis and assess the uncertainties (see ref.5 and 6 in chapt. 3 of the CSNI/PGW5 draft report).

Generic fire frequencies in important rooms and compartments of LWRs plants were provided by Kazarian and Apostolakis (see ref.7 in chapt.3 of the CSNI/PGW5 draft report). Some past PRAs produced different fire frequency values because of the special features of each plant (see ref.9,11 and 12, and tables 2, 3 and 4 in chapt.3 of the CSNI/PGW5 draft report). An extensive fire analysis was also performed in the ambit of the risk studies for the NUREG 1150 report. The event data table reported in the NUREG 4840 report (mentioned in par.2) is an exhaustive list of fire events used in that report.

ii) Fire accident analysis.

In general, current regulations on fire protection have made available suitable techniques and equipment for extinguishing fires in nuclear power plants.

In PRAs studies specific analyses are performed for plant rooms and zones where relevant safety systems and electrical supporting equipment are located. The aim is to clarify which kind of fire can develop and propagate in a dangerous way so to provoke accident sequences potentially leading to core damage. The analysis is very plant specific, depending on various circumstances including fire place, duration, propagation and extinguishing modalities. Current fault tree and event tree techniques are used to assess relevant failures and identify various fire propagation paths. In this regard data on the in plant fire barriers failure rate are also needed for determining the failure rate for specific equipment or components. Probabilities of accident sequences are calculated with the available PRA methods (for instance the one of the SET computer program) in which fires are regarded as common cause of failure. Alternative methods include dependencies between fire and components, room interconnections, location of cables and other plant features that are relevant to the analysis (see ref. 3, 4 and 12 in chapt.2 of the CSNI/PGW5 draft report).

Fire induced core damage frequencies were calculated in the fire risk

analysis of the NUREG 1150 report. In this report the results are presented with the uncertainty range and compared with results estimated for other events (see fig.3 and 4 in chapt. 1 of the CSNI/PGW5 draft report). The comparison confirmed that uncertainties may be significant, as also pointed out by some previous PRAs (see ref. 20 and fig 5 in chapt.1 of the CSNI/PGW5 draft report).

iii) Fire development analysis.

In the fire development analysis best estimate methods are used to assess the fire growth, the damage on relevant structures and equipment, and the effects of fire extinguishing actions (see ref.13 in chapt.3 of the CSNI/PGW5 draft report). The aim is to estimate the flashover time that is important to most fire prevention and mitigation measures (flashover time is the time when all flammable surfaces catch fire in the whole area that has been considered and temperatures reach nearly steady state values determined by the oxygen flow into the area). These measures have a high probability of success before flashover conditions are reached, and after flashover must be addressed to limit the fire spreading since all the content of the concerned area is lost.

Various simulating methods have been developed to perform the analysis. This requires that a barrier failure analysis be also performed to determine fire vulnerability data and damage times of plant fire barriers (such as fire doors, security doors, water tight doors, penetration seals and so on). Vulnerability data should include the effects of fire propagation and of heat and smokes transport on the barriers. In addition a recovery analysis is also required to estimate times to detect and suppress fires through the available in plant fire fighting measures. In this regard, data on fire suppression as function of the time are available in the literature for estimating, in conjunction with calculations, the probability that fires are suppressed before flashover. Numerical computer codes using deterministic, stochastic or empirical techniques are available to make calculations (see the list of table 5 in chapt.3 of the CSNI/PGW5 draft report).

5.2 Areas where more investigations are needed.

The frequency uncertainty range that has been assessed for the fire induced core melt accidents, underlines the need of more investigations to reduce the uncertainties. Uncertainties are mainly generated from the fire development analysis because of the unknowns in the understanding the fire growth phenomena and the plant response to fire occurrences and recovery actions.

Here following are mentioned some areas of major concern.

i) Determination of the fire frequencies.

The process to assess the fire frequencies is strictly dependent on the available data on in plant fire events, and must also rely on the capability of the used partitioning methods to account for all factors (such as the amount of electrical components and cables, fire loading,

fire zones occupation, and so on) that are relevant to the fire ignition and propagation in small rooms or buildings from large compartments. Computer codes used to partition fire frequency within a particular fire zone should therefore be improved in order to increase such capability.

ii) Fire development analysis.

Computer codes used to simulate the processes of the fire development and propagation from an enclosure to relevant areas of the plant (such as the various versions of the COMPBURN code) should be improved so to reduce errors and conservative assumptions usually made in the analysis. In this regard typical areas to be more investigated are:

- models to predict hot gases layer temperature;
- radiative heat transfer to targets above the flame;
- convective heat transfer for objects engulfed in the flame;
- heat conduction of objects in the flame and thermal response of barriers;
- mass burning rate of burning objects;
- ignition of insulation cables and damage failure criteria;
- manual fire fighting effectiveness (including smokes control);
- equipment survival in fire environment;
- control systems interactions.

The improvements in the above areas should increase the code capability to predict the time to ignition or damage for critical cables and components, as well as of times to fire suppression through available fire fighting means (including the intervention of fire brigades).

EXTERNAL EVENTS ASSESSMENT FOR AN LMFBR PLANT

K. Aizawa, R. Nakai and A. Yamaguchi

Power Reactor and Nuclear Fuel Development Corporation
Sankaido Bldg., 9-13, 1-Chome, Akasaka, Minato-ku, Tokyo, Japan

ABSTRACT

External events assessment was conducted for a typical loop-type liquid metal cooled fast breeder reactor (LMFBR).

The quantitative screening analyses which identify dominant sequences on the following location-dependent failures were conducted: leak of water/steam/freon, leak of sodium, inadvertent actuation of water sprinkler system, high energy line break causing pipe whip, HVAC fan missile, and fire. The result, which is obtained from conservative evaluation under the assumption that the susceptible components fail, indicates the effect of fire is the largest among those external events.

The quantitative seismic event analysis has also been conducted. Seismic hazard curves and spectral shape have been evaluated using the seismic activity data around the LMFBR site. The design analysis and the testing data for design basis seismic events were used to quantify seismic fragilities of the structures and components. Generic fragility curves were also evaluated based on the fragilities which were used in the precedent seismic probabilistic safety assessments (PSAs). Parametric studies for the probability of seismic failure on the plant level were conducted using site-specific seismic hazard and fragility curves. Several seismic event trees were developed by systems analysis for seismic event. The component failures due to a seismic event were modeled using a Boolean transformation equation technique. Then the seismic induced core damage probability from representative sequences was quantified and the critical components for earthquakes were identified.

1. INTRODUCTION

The Power Reactor and Nuclear Fuel Development Corporation (PNC) is constructing a prototype LMFBR, Monju. In support of its development effort, a probabilistic safety study has been performed since November 1982. The objective of this study is to construct a probabilistic model to be used in evaluating the overall safety of the LMFBR plant. The result of this PSA study will provide an optimum allocation of limited resources to various safety research programs and basic information useful for the development of a basic policy for safety design and evaluation of future commercial LMFBRs.

The level-3 PSA with respect to internal events was completed in 1990. The level-1 PSA with respect to external events is being conducted for Monju^{(1),(2)}. A quantitative location-dependent failures analysis and a preliminary seismic risk analysis were conducted. In order to evaluate efficiently the effect of the external events for an LMFBR plant, PNC has been developing an systems analysis code network. As for the location-dependent failure analysis, the SETS code⁽³⁾ is utilized as a main code. Analysis codes have also been developed for the evaluation of seismic fragility and common cause failure of the redundant system considering the partial correlation.

The plant studied is a loop-type LMFBR plant. Cooling of the nuclear reactor core during normal operation is accomplished by three heat transport system loops. Each heat transport loop consists of a primary heat transport system (PHTS) loop, an intermediate heat transport system loop, and a water and steam system loop. Maintenance of the reactor sodium level is necessary to ensure coolant circulation paths, which transport decay heat away from the core. This function is accomplished by the overflow/makeup system and the PHTS guard vessels. Decay heat removal in this plant is accomplished by either the intermediate reactor auxiliary cooling system (IRACS) or the direct reactor auxiliary cooling system (DRACS). The IRACS can remove decay heat successfully through one-loop operation immediately by either forced or natural circulation following a reactor shutdown. The DRACS can successfully remove decay heat following a reactor shutdown. Reactor power reduction is required to make the reactor subcritical and reduce the power generated in the core to decay heat levels. This function is accomplished by the reactor protection system.

2. LOCATION-DEPENDENT FAILURE ANALYSIS

2.1 QUANTITATIVE SCREENING ANALYSIS

A location-dependent failure is defined as an event in which two or more components fail either as a result of some harsh environments or because one component failure results in a harsh environment which causes other components to fail. The types of dependent failures of interest in an LMFBR are those which affect system redundancies or diversities. A comprehensive list of potential harsh environments was first prepared considering the characteristics of LMFBR. In order to limit the location-dependent failure task to a manageable and yet significant level, it was decided to concentrate on the harsh environments deemed potentially most significant. Available sources on historical dependent failures and events which were identified as having had the potential for dependent failures were reviewed. Over 4000 events^{(4),(5)} were screened; 235 events were selected as actual or potential dependent failure events. The types of location-dependent failure events applicable to an LMFBR are summarized as follows:

- (1) Leak of water/steam/freon
- (2) Leak of sodium
- (3) Inadvertent actuation of water sprinkler fire suppression system
- (4) High energy line break causing pipe whip
- (5) HVAC fan missile
- (6) Fire

The SETS⁽³⁾ location transformation analysis technique is used to solve accident sequence cutsets in terms of combinations of random failures and zones. The resultant accident sequence cutsets are analyzed further to identify exactly which components within the zones must fail. The first part of the SETS analysis, solving for accident sequence cutsets in terms of random failures and zones, is termed the critical zone analysis. The second part of the SETS analysis, determining the basic event cutsets within the critical zones, is termed the underlying cutset analysis.

In the SETS critical zone analysis, each basic event in a fault tree is transformed into both a random failure and a zone representing the location of the component. If A represents the basic event, then the transformation equation is the following:

$$A = AX + /Z1, \quad (1)$$

where

AX = transformed representation for the random failure

/Z1 = zone in which the event A is located

The "X" is used to avoid circular definitions, which the "/" is used so that random failures (AX in the example) and zones (Z1) may be distinguished. Such distinction is required in order to be able to truncate cutsets both by the number of random events and by the number of zones. Transforming all applicable basic events into random and zone contributions and resolving the accident sequences with SETS, cutsets involving random failures and rooms may be obtained. A cutset involving a single zone indicates that there are components within the zones which, if failed, would result in core damage. Similarly, a cutset involving a single random and a single zone indicates that there are components within the zone which, if failed and combined with the single random failure, would result in core damage.

Once the critical zone cutsets have been identified with the SETS code, the analysis of underlying cutsets can be performed. For each critical zone identified, the basic events within a location only were transformed in the following fashion:

$$A = /AX \quad (2)$$

The events are complemented to identify that they are within the location of interest.

The methodology for evaluation of potential location-dependent failures resulting from each initiator involves four steps:

- (1) Identification and quantification of harsh environment sources
- (2) Screening analysis for initiator as an initiating event
- (3) Screening analysis assuming initiator during the mission time
- (4) Refined underlying cutset analysis as required

The quantitative screening analysis is performed under the assumption that all the susceptible components in the location fail. The screening process attempts to rule out certain sequences and certain critical zone cutsets without detailed analyses of harsh environment effects on components. The result indicates that the effect of fire is the largest among the above external events and the further fire analysis is required.

2.2 FIRE ANALYSIS

The methodology used in an LMFBR probabilistic fire event analysis consists of three separate tasks:

- (1) Identification of all potential fire-initiated sequences (both sodium and nonsodium) inducing failure of the decay heat removal system
 - plant systems analysis
- (2) Identification of critical areas containing the decay heat removal system components
 - fire-hazard analysis
- (3) Determination of core damage frequency as a result of fire-initiated failure of the decay heat removal system
 - fire-propagation analysis

Compared with light water reactor (LWR), fire-induced loss of coolant accidents are extremely unlikely in an LMFBR design and are not analyzed. A fire can potentially induce any of the random transients. The most likely transient would be a manual scram initiated because of presence of the fire. Such a fire-induced transient is important to risk only if it also fails mitigating system equipment. Therefore, for an LMFBR fire study, a fire involving the decay heat removal systems or their support systems is assumed to result in at least a manual reactor shutdown.

The identification of critical plant areas is accomplished using the SETS location transformation analysis described before. The resultant critical area to fire event is a room which includes electrical equipment and related cables for actuation and/or control of the decay heat removal system.

Potential fire scenarios in the LMFBR are modeled using fire event trees. The event trees consists of the following headings: ignition, detection, suppression,

propagation, and recovery. The branches of the tree and their associated probabilities represent a possible outcomes of the fire scenario.

The frequencies of fires are obtained by the analysis of historical data. Because of the lack of information on fire occurrences in LMFBRs and Japanese LWRs, the U.S. LWRs data⁽⁶⁾ is used in this study. The failure probabilities of the fire detection are prepared for smoke / heat detector and detection by the plant personnel depending on the location. The propagation of the fire is dependent on the characteristics of the fire area. Fire growth and propagation analysis are performed using the COMPBRN-III code⁽⁷⁾. The thermal response of various targets in the fire scenario is modeled to predict the threshold of the propagation in the fire size and the amount of time required for the fire to damage or ignite critical equipment. The probability of propagation is estimated based on the results of COMPBRN-III code. Recovery is treated in a similar fashion as in the internal event analysis. The human reliability analysis provides the probability of recovery based on the type of recovery and grace time.

Dominant contributors to loss of the decay heat removal system are combinations of the electrical component failures within the electrical panels due to hot gas layer.

3. SEISMIC EVENT ANALYSIS

3.1 SEISMIC HAZARD ANALYSIS

Seismic hazard curves and spectral shape have been evaluated using the seismic activity data around the plant site. Two different methods are adopted for estimating the seismic hazard curves. One is based on Gutenberg-Richter's (G-R) relation obtained from historical earthquake data and the other on the earthquake fault activity from active fault data.

To utilize the historical earthquake data, six seismotectonic zones are identified around the plant site. One can obtain the probability density function of hypocentral distance, $f_{Xk}(x)$ for each zone k . Annual frequency of earthquake occurrence (ν_k) with the magnitude M_l or above is calculated with the G-R relation as follows:

$$\log v_k = a - bM_l \quad (3)$$

where a and b are empirical parameters in the G-R relation and are determined based on the historical record of earthquakes. Upper magnitude M_u and lower magnitude M_l are defined to evaluate of the parameters a and b . M_l is based on the minimum earthquake recorded in the history which caused any damage. Potentially maximum magnitude can be predicted from either the historical earthquake or the characteristics of active fault. The greater value of them is assumed to be M_u for each seismic zone. The probability density function of magnitude $f_{Mk}(m)$ is also calculated using the G-R relation.

Attenuation of the peak ground acceleration (PGA) a is evaluated based on the observation of the historical earthquakes in Japan. Six empirical equations out of eighteen are selected to be appropriate for the rock site and the average value is used in this study. However, in the phenomenological process of propagation and attenuation of the seismic wave, PGA observed at the site is subject to uncertainty. Thus a is regarded as a random variable having lognormal distribution, $f_A(a)$ with the logarithmic standard deviation β .

Combining these quantities, one obtains expected annual number of earthquakes which PGA is equal to or greater than a , as follows:

$$v(a) = \sum_k \int_x \int_m v_k f_A(a|m, x) f_{Mk}(m) f_{Xk}(x) dm dx \quad (4)$$

where k relates to the summation with regard to the seismic zones.

Next, a method to establish the hazard curves based on the active fault data is described. More than 300 active faults are investigated which are located within 150 km distance from the site. The relations between the magnitude and active fault length L and magnitude and slippage d caused by each earthquake are given by:

$$\log L = 0.6m - 2.9 \quad (5)$$

$$\log d = 0.6m - 4.0 \quad (6)$$

respectively. v_k is evaluated using the annual mean slippage S , i.e. $v_k = S/d$. Therefore, $v(a)$ is calculated by:

$$v(a) = \sum_k \int_0^{L_k} v_k f_A(a|m, x) \frac{dl}{l} \quad (7)$$

where L_k is the length of the k -th active fault and the summation is performed in terms of the number of active fault.

Now, assuming Poisson's process, one evaluates the annual probability of exceedance (the probability that the PGA of an earthquake is greater than a specific value a), as follows:

$$P(a) = 1 - \exp\{-v(a)\} \quad (8)$$

where $P(a)$ is the annual probability that PGA of an earthquake exceeds a .

Important points in the discussion are the maximum PGA (that is upper cut-off value) and the uncertainty of the PGA attenuation in terms of logarithmic standard deviation β . Since the research regarding this topics is under way and it is difficult to make a judgement for point estimation presently, sensitivity analysis is to be employed. In other words, two values for β ($=0.5$ and 0.7) and A_{max} ($=1,000$ gal and infinite) each are assumed. The value of A_{max} is determined based on both phenomenological and empirical investigation. β is based on the results of the past statistical analyses of PGA data observed in Japan. The sensitivity of the parameters to the final results (such as annual frequency of core damage or systems failure) is to be investigated by the systems analysis as described in section 3.3.

It is a matter of course that neither data sets reflect the complete seismic sources. However, what is important in the viewpoint of seismic PSA is to derive the best estimate hazard curves and to employ the sensitivity calculation in the area where the physical models and the parameters are subject to uncertainties. In the present study, it has been found that both hazard curves are in agreement with each other. As long as both approaches give similar results, one may consider the hazard curves analyzed are the best estimate on the basis of the current state-of-the-art.

The spectral shape $S_a(T)$ as a function of period T is defined as the acceleration response spectrum normalized by the PGA value. Assuming that the probability density function of $S_a(T)$ is lognormal, the median and logarithmic standard

deviation are to be evaluated. Since $S_a(T)$ is dependent on m and x , the following equation was proposed:

$$\ln S_a(T) = a(T)m - b(T)x + c(T) \quad (9)$$

where $a(T)$, $b(T)$ and $c(T)$ are obtained by regression analysis of earthquake motions observed in Japan. Joint probability density function of x and m , $f(m, x/a)$, when PGA is given, can be obtained using $f_{Mk}(m)$ and $f_{Xk}(x)$. Therefore, the median and the logarithmic standard deviation of the spectral shape are obtained by:

$$\overline{\ln S(T|a)} = \int_x \int_m \ln S(T|m, x) f(m, x|a) dm dx \quad (10)$$

$$B^2(T|a) = \int_x \int_m \{ \ln S(T|m, x) - \overline{\ln S(T|a)} \}^2 f(m, x|a) dm dx \quad (11)$$

3.2 FRAGILITY EVALUATION

The entire fragility curves, which represent seismically-induced failure probabilities at each ground acceleration level, are developed for the major buildings and equipment of the plant based on the safety factor method.⁽⁸⁾ The ground acceleration capacity A is given by:

$$A = A_m \epsilon_R \epsilon_U \quad (12)$$

where A_m is the best estimate of the median ground acceleration capacity. ϵ_R and ϵ_U are random variables with unit medians representing the inherent randomness about the median and the uncertainty in the median value, respectively. The safety factor F on PGA capacity above the reference level earthquake specified for the design (S_2 earthquake) is expressed as:

$$A = F A_{S2} \quad (13)$$

where A_{S2} is the PGA level for the S_2 earthquake.

For structures, the safety factor can be modeled as the product of three random variables:

$$F = F_S F_\mu F_{RS} \quad (14)$$

where F_S is strength factor, F_μ is inelastic energy absorption factor, and F_{RS} is structural response factor. For equipment and other components, the safety factor is composed of capacity factor F_C , structural response factor F_{RS} and equipment response factor F_{RE} . Thus,

$$F = F_C F_{RE} F_{RS} \quad (15)$$

The seismic fragility of structure or equipment is defined as failure probability on condition that an earthquake occurs. The fragility is a function of the intensity of the earthquake and our degree of belief, Q , regarding median capacity, A_m . The double logarithmic normal distribution model is widely used to describe the seismic fragility curves. Using the PGA a as the intensity parameter, the seismic fragility is expressed as the following equation:

$$Pr(a > A | Q) = \Phi \left[\frac{1}{\beta_R} \ln \left(\frac{a}{A_m \exp \{-\beta_U \Phi^{-1}(Q)\}} \right) \right] \quad (16)$$

where β_R and β_U are variabilities of the fragility associated with randomness (ϵ_R) and uncertainty (ϵ_U), respectively. $\Phi(\cdot)$ is the cumulative normal distribution function and $\Phi^{-1}(\cdot)$ is its inverse function. Q lies between 0 and 1.

Selected buildings for the structural fragility evaluation are the reactor building where most of the heat transport system components are involved, the auxiliary building where decay heat removal system and support systems are installed, the diesel generator building, the containment vessel and the screen pump room which provides the support cooling systems with the sea water as the ultimate heat sink. The standard deviations of the floor response spectra are also calculated using Monte Carlo simulation. The results are used in the seismic fragility (structural response factor) analysis of the equipment.

Since the systems in the LMFBR plant differ significantly from those in LWRs, the dominant contributors to seismic risk may not be typical of those most common for LWRs. So the design analysis and the testing data for design basis earthquake were used to quantify plant-specific seismic fragilities of the structures and equipment.

The numerous components are relating to the safety functions and are included in the systems analysis model. Hence it is not practical to evaluate the plant-specific

fragility for every component. Generic fragility curves are evaluated based on the fragility parameters which were used in the precedent seismic PSAs. For the equipment with less importance and/or common to that in LWRs, the generic fragilities are used in principle. For some dominant contributors to the results, however, fragility parameters were modified using a Bayesian methodology⁽⁹⁾. This approach is based on seismic experiences in non-nuclear industry or engineering judgement derived from the comparison of the same equipment class of the LMFBR and LWRs sited in high seismic zone.

In the LMFBR plant under seismic circumstances, it is noted that decay heat can be removed by natural circulation if no boundary failure takes place. In the natural circulation mode for decay heat removal, support systems such as AC power supply and HVAC systems are not necessary except DC battery which supplies power to open sodium valve and vane and damper of dumped heat exchanger when they are on demand. Therefore, the fragility of the coolant boundaries which compose decay heat removal systems were focused on.

From this viewpoint, a methodology to consider the importance of multiple coolant loop failures was developed by assessing the partial failure correlation between three heat transport loops.⁽¹⁰⁾ The resultant failure probability and the fraction of the common mode failure at various acceleration levels which have been evaluated are used as input for systems analysis to quantify the seismic risk.

Sensitivity studies for the annual frequency of seismically induced failures on the plant or system level were conducted using the site-specific seismic hazard curves and generic and plant-specific fragilities. From this simplified sensitivity study, the important equipment is identified for which the fragility estimation is to be updated. Based on the sensitivity study, equipment that needs further refinement of structural response analysis and fragility evaluation has been identified. It has been found that some structural components consisting the coolant boundaries and decay heat removal system and electrical equipment such as batteries and electrical panel are relatively sensitive. In accordance with the recommendations, current efforts are centered on the stochastic structural response analysis and fragility evaluation of the functional failure of such equipment.

3.3 SYSTEMS ANALYSIS

Seismic event trees are constructed taking into consideration for plant responses given large earthquakes which exceed design-basis earthquake. In addition an event which does not require the event tree is considered because it leads to core damage directly. Such an event includes reactor vessel failure or core support structure failure. The resultant event trees are reactor trips assuming loss of off-site power, PHTS leakage within guard vessel, PHTS leakage outside of guard vessel, and DRACS leakage. The event tree headings consist of essential safety features which achieve the safety functions of the reactor power reduction, decay heat removal and maintenance of sodium level.

The fault trees developed for the internal events analysis are used directly with seismic transformation equation. If A represents the basic event, the transformation equation is the following:

$$A = AX + AS, \quad (17)$$

where

AX = transformed representation for the random failure

AS = seismic induced failure

For an electrical component within electrical panel, the seismically induced failures are modeled by the panel failure as well as the component failure. In addition a structure or building failure event may be added as a seismic specific event, if needed.

The probability of AS varies with the PGA. Sequence minimal cutsets are solved for each acceleration level based on the system combinations identified event trees. The quantification of accident sequences for each acceleration level is performed using component fragility data. These accident sequences are the function of the PGA and are de-conditioned by integrating each accident sequence over the hazard curve. Recovery by the plant personnel is only taken into account for non-seismic failure events.

The experiences show that inclusion of system success is essential, since the probability of system success decreases substantially as the PGA increases. In an LMFBR the decay heat can be removed by natural circulation even in the sequence of total blackout. Therefore the integrity of reactor coolant boundary and the safety function for the maintenance of sodium level become more important.

4. CONCLUSION

A comprehensive external events analysis for the LMFBR plant has been conducted in constructing probabilistic models in order to evaluate the overall plant safety. The quantitative screening analyses which identify dominant sequences on the following location-dependent failures were conducted: leak of water/steam/freon, leak of sodium, inadvertent actuation of water sprinkler system, high energy line break causing pipe whip, and fire. The seismic hazard analysis, the floor response spectra analysis, the seismic fragility evaluation for LMFBR-specific structures/equipment as well as the one for various types of structures/equipment important to safety and seismically induced systems analysis were also conducted.

Useful insights are obtained from those analyses and will be utilized to establish rationalized safety design policy for LMFBRs and optimized allocation of limited resources (man power and fund) to various safety research programs.

PNC is continuing to improve modeling for evaluation of the effects of the external events as well as to develop the relating database in order to reduce the uncertainties in the analyses. Those efforts to minimize the uncertainties will enable better utilization of the full scope PSA in the various areas.

REFERENCES

- (1) Aizawa, k., Kani, Y., Nakai, R., Hioki, K., Sakuma, T., Ohshiro, S., Okazaki, S. and Tokunaga, T., "Parameter and Model-Uncertainty in PSA for an LMFBR Plant," Technical Committee Meeting on Advances in Nuclear Power Plant Risk Analysis, Vienna, Austria, September 1986.

- (2) Yamaguchi, A., Nakai, R., Kani, Y. and Aizawa, K., "Current Status of Seismic PSA Study on LMFBR at PNC," International Post-SMiRT 10 Seminar #9, Irvine, USA, August 1989.
- (3) Worrell, R. B., "SETS Reference Manual," NUREG/CR-4213, 1985.
- (4) Murphy, G. A., "Survey and Evaluation of System Interaction Events and Sources," NUREG/CR-3922, 1985.
- (5) Acey, D. L., Chapman, J. R., and Lydell, B. O. Y., "Classification and Analysis of Reactor Operating Experience Involving Dependent Events," EPRI NP-3967, 1985.
- (6) Bohn, M. P., Lambright, J. A., "Procedures for the External Event Core Damage Frequency Analyses for NUREG-1150," NUREG/CR-4840, 1990.
- (7) Ho, V., Siu, N., Apostolakis, G., and Flanagan, G. F., "COMPBRN-III - A Computer Code for Modeling Compartment Fires," NUREG/CR-4566, 1986.
- (8) PRA Procedures Guide: "A Guide to the Performance of Probabilistic Risk Assessment for Nuclear Power Plants," NUREG/CR-2300, January, 1983.
- (9) Yamaguchi, A., et al., "Bayesian Methodology for Generic Seismic Fragility Evaluation of Components in Nuclear Power Plants," to be published in Proc. of SMiRT-11, Paper M4/3, Tokyo, August, 1991.
- (10) Yamaguchi, A., "Seismic Fragility Analysis of the Heat Transport System of LMFBR Considering Partial Correlation of Multiple Failure Modes," to be published in Proc. of SMiRT-11, Paper M4/2, Tokyo, August, 1991.

**POSSIBILITIES AND LIMITATIONS OF PROBABILISTIC FIRE SAFETY
ANALYSES ILLUSTRATED BY ANALYSES IN THE GERMAN RISK
STUDY**

by H. Liemersdorf

Gesellschaft für Reaktorsicherheit (GRS) mbH

Cologne, Federal Republic of Germany

**To be presented at the OECD/BMU Workshop on "Special Issues of
Level 1 PSA", Cologne (FRG) May 27th till 29th, 1991**

Possibilities and Limitations of Probabilistic Fire Safety

Analyses illustrated by Analyses in the German Risk Study

1 Introductions and Background

Actually in Germany and abroad a uniformed and harmonized approach for probabilistic fire safety analyses for nuclear power plants is not available. For that reason the German PSA-Procedure-Guide does not have any description for fire events. Due to this fact German PSA-Studies carried out systematically do not include fire safety analysis up to now.

However, risk studies for nuclear power plants in USA show that the risk contribution due to an internal fire can be of importance. Therefore, probabilistic fire safety analyses are necessary within the scope of PSA-Studies on principle. But there is a need for discussions to come to an agreement for the procedure.

It is the aim of this paper to give a review about the problems in connection with probabilistic fire safety analyses illustrated by analyses carried out in the German risk study /1/. Referring to that possibilities and limitations of probabilistic fire safety analyses should be indicated.

2 Approach of the Risk Analysis

The effects of fires in a nuclear power plant may range from the usual conventional consequences such as loss of production and loss of property to the release of radioactive substances from auxiliary equipment to a core meltdown. Within the scope of Phase B of the German Risk Study, only such fires are investigated as can initiate a core meltdown. As compared with such events, it is possible to neglect the risk contributions resulting from fires involving radioactively contaminated materials at the nuclear power plant.

For that reason it is to be sufficient for PSA-Studies to analyse only fires being relevant for the reactor safety.

Furthermore, only fires with overlapping consequences for systems and redundancies can be regarded significant. That means that a local fire which is bounded to a single component,

e.g. a smouldering fire at an electrical engine, has not to be considered. Such local fires are implicated in the reliability analyses by the components failure rates.

When analyzing the effects of fires, the first step is to determine the compartment areas where major fire loads and safety-related systems are located. Apart from the actual fire compartment, the determination also includes adjacent compartments if the fire may encroach upon these.

For the compartments selected, the course of the fire is investigated by means of a fire specific event tree analysis. For reducing the amount of analyses an additional reduction of the number of compartments is necessary. With respect to this, qualitative or quantitative procedures are possible. In the German risk study both have been done.

For the fire specific event tree analyses, Fig. 1 shows a simplified event tree diagram. Based on the consequential fire damage determined to have been caused to the safety-related systems, and also based on the respective frequencies, the system-specific event tree analysis is performed.

Because of the limited database available for the plant investigated, generic data were used for the determination of the fire occurrence frequencies. In this context, statements concerning the frequency of fires in nuclear power plants are available as mean fire occurrence frequency per plant and year and as compartment and building-specific fire occurrence frequencies.

From a comparison of US literature on the mean fire occurrence frequency per year and plant, a mean of 0.17 fires per year and plant is derived for US light water reactors /2/.

Special data for nuclear power plants in the Federal Republic of Germany are not available to a similar extent because of the smaller number of plant operating years as compared with the United States. However, the evaluation of the data available /3/ permits the conclusion that there is not major difference in fire occurrence frequencies in nuclear power plants in the Federal Republic of Germany and the United States.

The Study used the fire occurrence frequency of 0.17 fires per plant and year which had been determined. Furthermore, it was assumed that it will be possible to use the US compartment-specific data for nuclear power plants in the Federal Republic of Germany, provided there is no major difference between the buildings and/or compartments as far as

their functions and layouts, the types and quantities of combustible materials and the potential ignition sources are concerned.

The fire-specific event tree analysis distinguishes between a pre-flashover phase and a post-flashover phase. The intensity which a fire develops is determined by the quantity, the arrangement and the properties of the combustible materials as well as by the size and ventilation conditions of the fire compartment. The ventilation conditions, in turn, depend on the position of the ventilation and/or fire dampers and on fire doors at the beginning and in the course of a fire and on their fire protection quality (ventilation and compartment isolation).

The decisive factor for the actual development of a fire is the point in time at which the fire is detected by the operating personnel and/or by fire detection equipment in the fire compartment (direct fire alarm) and the point in time at which it is fought by active fire extinguishing measures (direct fire fighting). Even if the fire is already extinguished during the pre-flashover phase, systems accommodated in the fire compartment may fail. This will always be the case if parts of a system are involved in the fire, or if the temperature limits to be adhered to by the system are exceeded.

A fire alarm may also be effected by fire detection systems in adjacent compartments or by the detection of system failures (indirect fire alarm). However, this can only be anticipated during the post-flashover phase. The active fire fighting measure during the post-flashover phase mainly aims the prevention of a further propagation of the fire and at the protection of vulnerable systems in adjacent compartments (indirect fire fighting). Whether or not systems in adjacent compartments will also fail mainly depends on the fire protection quality of the compartments during a fire and on whether they will function properly (fire zone limitation). If compartment and/or ventilation isolations such as a fire door are open, or if the fire resistance rating of these structures is insufficient, the fire may encroach upon adjacent compartments if fire fighting does not start in time.

The failure probabilities to be inserted at the various fire-specific branches of the event tree diagram may depend on the time and on the course of the fire itself. The main aspects in this context are the development of the temperatures in the respective compartment areas where the safety-related systems are located and the temperatures which have to be expected there.

In this context, Fig. 2 is a schematic representation of the compartment temperature time history and the fire-specific event sequence.

Depending on the successfully isolation of the ventiation (closing of dampers in the ventilation system or of fire doors) at the time t_2 , two fire sequences I and II are possible. Fire fighting may start at different times. T_k means the critical temperature of the safety related equipment.

The schematic representation of the fire sequences in Fig. 2 may be more complex in reality. For this representation, the temperature increase and the expected temperature level in the respective compartment areas have to be determined.

For that reason expensive codes with a more complicated fire modeling are necessary in general. Depending on the variation of the possible boundary conditions (e.g. type, amount and location of the fire load and the ventilation) the results of the calculations are different temperature-time-histories with different consequences for safety related equipments. In general, a correlation between the occurrence frequency for a particular temperature-time-history and the occurrence frequency of a fire determined statistically can not be found. Therefore the probabilities for the different temperature-time-histories have to be estimated. The uncertainties of these determinations can vary.

With respect to the fire effects calculated, it should be examined, whether an influence on the failure behavior of the respective safety-related systems has to be anticipated and, thus, whether failure probabilities which depend on the fire sequence have to be taken into consideration. Finally, the result of the fire-specific event tree analysis is the frequencies of consequential fire damage involving a failure of safety-related systems. In Fig. 1, the consequential fire damage is marked 1, 2 and 3.

The following event tree analysis in terms of systems engineering analyzes the influence of the fire-related system failures on the overall behavior of the existing safety systems. In this context, system failures which are independent of the fire are taken into consideration provided the contribution to be anticipated cannot be neglected. This is the case, for example, if due to fire-related failures there is only a single redundancy available of a system which is important in terms of safety.

In general, failures of components due to a fire lead to transients which will be usually investigated in PSA-Studies. Therefore, the same event tree or fault tree diagrams can often be used. However, has to be considered, that, due to the fire sequence a lot of components of different systems and redundancies can fail and that these failures are correlated with the fire sequence.

For components and systems outside the fire areas, no fire-related influence, e.g. by corrosion or temperature is postulated in the analyses of the German risk study. In particular cases such influences could be important.

3 Results of the fire risk analysis for the NPP Biblis B

The results are:

- Frequency for plant condition not coped with by design safety systems (accident management measures not considered) due to an internal fire:
1,7 E-7/a

The figure 1,7 E-7/a represents a contribution of less than 1% to the total frequency of such plant conditions analyses in the study (2,9 E-5/a over all events)

- Under consideration of accident management measure the core melt frequency due to an internal fire is estimate to:
 - high pressure conditions: 1 E-8/a
(represents a contribution of less than 2% of the total core melt frequency under this conditions)
 - low pressure conditions: 1 E-7/a
(represents a contribution of 4 % of the total core melt frequency under this conditions)

4 Findings for possibilities and limitations of probabilistic fire safety analyses

- Delimitation of fire areas have to be investigated in detail

It is necessary and convenient to reduce the amount of investigations in detail. Therefore, an approach has to be made reducing the number of fire areas or fire compartments which have to be analysed as far as possible.

In a first step qualitative criteria can be used:

- amount of fire load
- importance of the safety of the equipment
- number of redundant systems and their physical separation for fire
- quality of fire protection

Findings from deterministic safety analyses are also helpful in this context.

The number of fire areas or compartments selected in that way can be reduced once more in a second step by using representative areas for a lot of areas with similar fire sequences and similar consequences on safety related equipments. However, in this cases the number of the similar areas must be considered in the total evaluation.

In third step (or in case with start of the analysis) of reducing the numbers of fire areas quantitative procedures are available (e.g. in /4/). Usually, that means simplified, rough probabilistic analyses for the determination of fire spreading with simple estimations for the fire effects and the reliability of fire protections measures.

- Determination of the fire occurrence frequency

For the analyses in detail, compartment-related data will be needed in general. In some cases there is a need for plant specific data to evaluate a particular fire scenario inside a compartment. In practice, plant specific data are not available (due to the low number of fire incidents). Compartment-related data are available on the basis of generic data. These data can be used in general, sometimes however a modification is necessary.

If there is a need for a fire occurrence frequency for a particular fire scenario inside a compartment, e.g. an oil fire depending on the volume of a oil leakage, generic data can be problematic. In this case an estimation by modeling the situation in the plant is better for getting realistic data. But it is difficult to evaluate the uncertainty of such an estimation.

- Determination of fire effects

On principle time-dependent values of

- temperature
- pressure

- concentration of corrosive or toxic fire products

are necessary for the fire compartment or in case for adjacent compartments. But in general, thermal effects cause the equipment failure. For that reason, the knowledge about the possible temperature-time-histories has to be mostly sufficient. For the probabilistic evaluation it is important to evaluate the probability of the different possible temperature-time-histories.

The expense being necessary for the theoretical determination of fire effects depends on the kind of consequences. For a lot of fire events only the possibility for a fire spreading to the next compartment is important. Therefore in general a calculation with a relatively simple "single-room postflashover fire model" is sufficient. If the fire spreading or the local distribution of temperature inside a compartment (e.g. cable spreading room below the control room) or between rooms which are not separated (e.g. containment) are important a more complex "multiple-zone or multiple-room fire model" is necessary. Such models have to describe the preflashover phase of a fire, too. To some extent codes are still under development.

- Reliability data for fire protection measures
It is to differentiate between
 - structural fire precaution measures, e.g. walls, fire doors, dampers in ventilation systems and cable or pipe penetrations through fire barriers,
 - Technical fire protection measures, e.g. fire detection systems, stationary fire fighting systems and systems for water supply and
 - operational fire protection measures, e.g. manual fire fighting by plant personnel or a fire brigade.

For the structural fire precaution measures statistical data for the fire resistance are available resulting from standard fire experiments. With these data, the failure probability for reaching the nominal fire resistance can be determined. In the PSA the calculated temperature-time-curves have to be transferred to the results from standard fire experiments. Therefore one possibility is the transfer of the "time-integral", of the real temperature-curve to the standard-fire-curve for the determination of an "equivalent fire resistance".

For fire doors and fire dampers is to be considered that the reliability is also influenced by other criteria (technical failures or human factors).

The reliability of technical fire protection measures can be determined by a special fault-tree-analysis. An example is shown in Fig. 3. If no data from nuclear power plants are available (e.g. only from conventional industry) the reliability will be estimated too low in general. To some extent plant specific data determined by the evaluation of results of systematical checks of fire protection measures are available.

If stationary fire fighting systems will be actuated manually the reliability of the actuation and the time delay from the fire detection time until the time of actuation mainly influence the total reliability.

For the effectivity and the reliability of the manual fire fighting in nuclear power plant no certain databasis is given up to now. However, operational experiences show that a lot of fires have been fought successfully in the ignition phase by the plant personnel or in a later phase by the fire brigade. On the basis of US data /3/ the non-availability of manual fire fighting have been estimated with a value not better than 3×10^{-1} per demand depending on the time delay between fire detection and fire fighting by the fire brigade.

- Failure criteria of safety-related equipments

It is to differentiate between

- electrical equipments (e.g. cables, switchgears, instrumentations, electrical engines and electronics) and
- mechanical equipments (e.g. tanks, pipes, pumps, valves)

and for the mechanical equipments also between integrity and function. In German studies /1,3/ the component temperatures have been used as a failure criterion. (Fig. 4). The failure temperatures as shown in Fig. 4 are only rough values with many uncertainties. But the experiences of the studies have shown that in most cases the component temperatures determined differ from the failure temperature (above or below) of a large difference. In these cases the uncertainty of the failure temperature does not have any influence on the results. In other cases, where the distance between the component temperature and the failure temperature is very small, the uncertainty can be reduced by a specific investigation of the component.

REFERENCES

- /1/ Gesellschaft für Reaktorsicherheit (GRS) mbH,
Deutsche Risikostudie Kernkraftwerke Phase B,
ISBN: 3-88585-809-6, Verlag TÜV-Rheinland,
Köln, 1990

- /2/ G- Apostolakis, M. Kazarians,
Fire Risk Analysis for Nuclear Power Plants,
NUREG/CR-2258, Sept. 1981

- /3/ Gesellschaft für Reaktorsicherheit (GRS) mbH,
Optimierung von Brandschutzmaßnahmen und Qualitätskontrollen
in Kernkraftwerken,
ISBN 3-92387-10-X, GRS-62, Sept. 1985

- /4/ Nuclear Power Plant Fire Protection
Fire Hazard Analysis -
NUREG/CR-0654, Spet. 1979

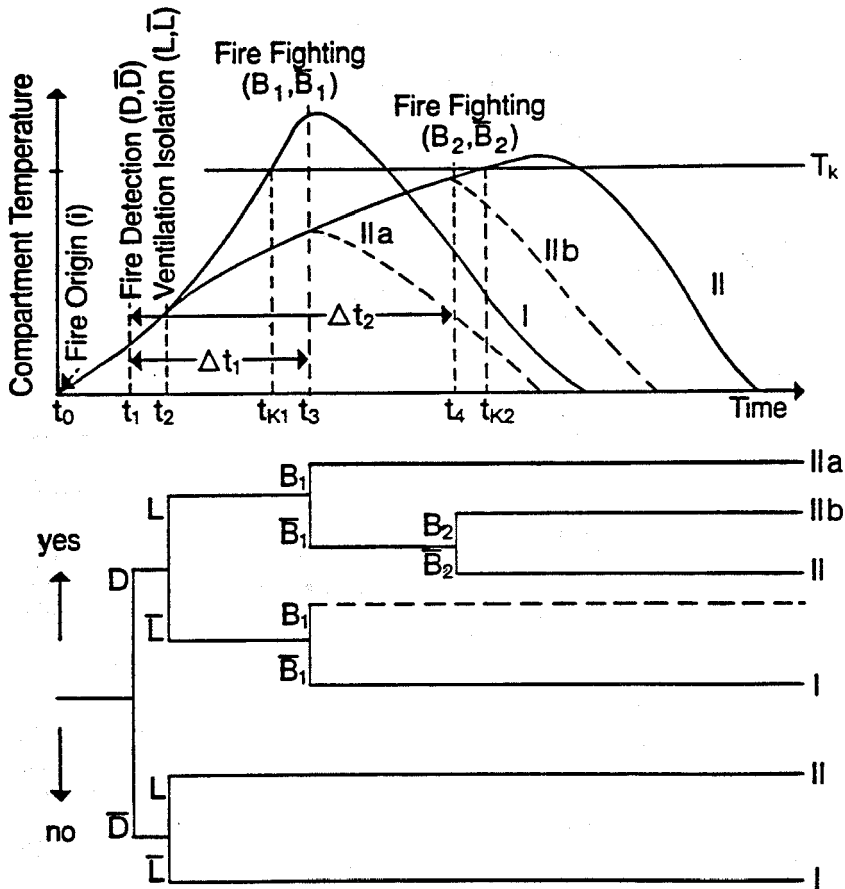


Fig.2: Interrelation between the Compartment Temperature Time History and the Fire-Specific Event Sequence (Model)

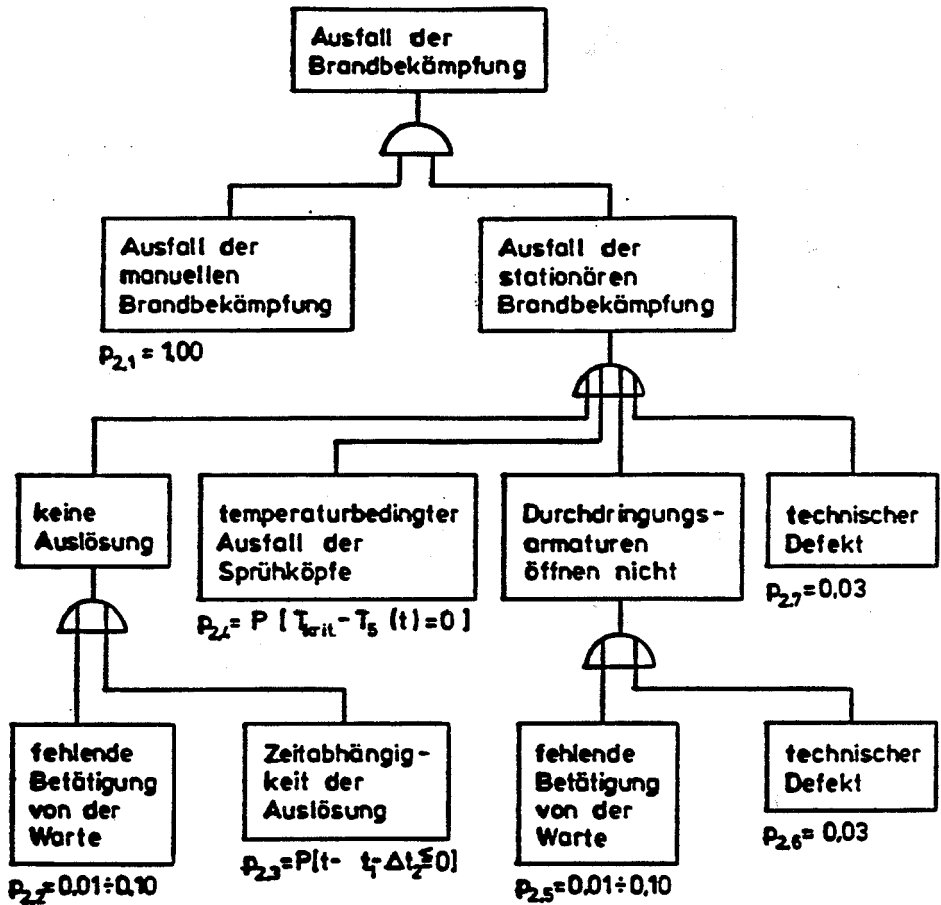


Fig.3 : Example for a Fault-tree "Failure of fire fighting inside a BWR-Containment"

Failure Criteria for Equipment Failure Temperatures

Electrical equipment

Failure of cable insulation	< for burning cables temperature ≥ 200 C
Failure of electronic equipment and switchgear	< temperature ≥ 70 C temperature ≥ 200 C (for safety-related equipment inside the containment)*

Mechanical equipment

Loss of function, i.e. of drive units, valves	Temperature ≥ 400 C
Leakages in seal membranes	Temperature ≥ 400 C
Loss of integrity	not relevant

)* designed for "Loss of coolant accident" conditions

Fig. 4:

SEISMIC ASSESSMENT FOR N.P.P. ACCORDING TO ITALIAN PRACTICE

S. D'Offizi¹, L. Magri², F. Muzzi²

¹ ENEL, Roma

² ISMES S.p.a., Roma

The definition of design seismic ground motions for antiseismic design can be schematically subdivided into naturalistic aspects and engineering aspects.

At the base of the naturalistic aspects, which are essentially geological and seismological, there are the following postulates, generally accepted by the scientific community and present in all standards, technical guides and recommendations:

- earthquakes are the mainly due to the tectonic activity;
- the tectonic regime acting in a specific area does not change during the life time of a nuclear power plant;
- the probability of the creation of a new seismogenetic structure or of seismic reactivation of a dead structure in an area with no seismicity, without neotectonic effects and not in agreement with the general kinematic model is so low that such events are not taken into consideration.

A good characterization of the geological/seismological aspects can enable us to make decisions of great importance, such as the exclusion of a particular area or the identification of seismogenetic zones, even if it is not able yet to supply by itself numerical parameters which can be used immediately by the engineer for design purpose.

As far as it concerns the engineering aspects, either the process of antiseismic design or analysis or check out of a structure, natural and artificial slopes, foundation materials, is fairly consolidated in its praxis, or to be more exact, the meanings of the various hypotheses of schematization or of the levels of conservatism innate in each of them and in the design process as a whole are quite well known.

Thus the most critical point in the process is the translation of the design earthquakes defined in geological and seismological terms into engineering parameters.

One of the main difficulties lies in the fact that when the design seismic ground motion is transformed into engineering terms, as it must be, the design process, which proceeds

through analytical or numerical models of the structures in order to foresee their behaviour, comes into account.

Therefore the transformation of the design seismic ground motion into engineering terms cannot be made without considering on one hand the geological/seismological hypotheses which defined it, and on the other hand its adequacy to the schemes and the engineering methods.

The conservatism of the antiseismic design of a nuclear power plant must be therefore achieved by harmonizing the safety margins of the whole process, which proceeds from the definition of the seismogenetic structures to the determination of the main stresses in the structural elements, passing through the definition of the parameters of the design seismic ground motions.

The process for the definition of the ground motion parameters may be either deterministic or probabilistic. For safety purposes the methodology usually adopted is a deterministic one, and till now few probabilistic approaches have been proposed.

The approach practiced in Italy is a deterministic methodology specifically intended to face above all the problems related to complex orogenetic collisional and/or post-collisional areas, as for instance the Mediterranean regions. In fact, in the orogenic areas, the surface structures could only represent an indirect sign of the dislocations and strains which involve the crustal structures significant from the seismogenetic point of view. As a consequence, the movements, which can be reconstructed on the surface by the analysis of the strain field, are generally the sign of deep dislocations which are not directly connected to the surface tectonic evidences.

This approach has been applied for the study of nuclear power plant sites in Italy, Belgium, Pakistan, USSR.

The methodology practiced in Italy for evaluating the seismic ground motions for safety purposes in N.P.P. sites can be summarized as follows (Fig. 1):

- a) Definition in three dimensions of the geological structures potentially active and capable of generating earthquakes.

A reliable good structural model, connected with the most recent geological evolution by the neotectonic model, can be the basis for a first correlation with the seismic frame. This correlation allows us to determine the structures that can release energy as seismic waves.

The location and delimitation of the structural units are carried out on the basis of the

study of: satellite imageries as far as it concerns the surface trend of the different structures; geophysical studies (gravimetry, reflection and refraction methods, heat flow, magnetometry, etc.) for the definition of the deep trends of the structures; geological studies to reconstruct the tectonic evolution of the area and to define the rheological features of the involved rocks.

The neotectonics permits to relate the elements of the defined structural model with the recent tectonic activity and to characterize its stress field.

Moreover, the definition of the kinematic model allows to define and delineate the single elements of the system and to describe the trend of the movement during a significant span of time, in order to foresee where the earthquakes may occur (even with incomplete seismic catalogues), which are the spatial limits of the sources and which is the seismic potential, and to give information about the stress field that causes the earthquakes and about the source rupture mechanism.

- b) Definition of the seismological setting, carried out by the historical research on past seismic events, by the assessment of the macroseismic parameters, and by the evaluation of the instrumental data, including those from local microseismic networks, in order to compile a complete and reliable seismic catalogue, that is the basis for the characterization of the seismicity in space and time.
- c) Definition of the seismogenetic zones, on the basis of the structural and kinematic geological models and of the seismological setting, that is of the zones whose seismogenetic activity can cause significant vibratory ground motions at the N.P.P. site.

Each zone is characterized by:

- name and reference to kinematic model;
- geometry, kind of kinematism and, if possible, velocity of the present movements and nature or rheology of the rocks involved;
- maximum historical epicentral intensity and/or maximum magnitude described in the seismic catalogue;
- maximum potential seismicity consistent with the kinematic model and, if available, with nature or rheology of the rocks;
- average and minimum distance from the site;
- maximum historical intensity felt at the site;

- maximum macroseismic intensity computed at the site by the attenuation laws and the maximum epicentral intensity;
 - potential intensity computed at the site by using the attenuation laws and the maximum potential seismicity.
- d) Computation of the free-field surface peak ground motion parameters, on the basis of the seismogenetic zonation, and applying the correlations available in literature among magnitude, distance and acceleration and those between intensity and acceleration, for each of the above outlined seismogenetic situations.
- e) Definition of the design geotechnical profile, by detailed local geological survey and geotechnical investigation, necessary for the study of the seismic response at the site. This profile takes into account the soil characteristics and the geomorphological conditions at the ground surface or near the ground surface.
Cross-hole and laboratory tests allow to obtain the variability of the shear modulus and of the damping as a function of the shear strain.
- f) Definition of the site specific response spectra for each seismogenetic zone, on the basis of the seismogenetic zonation and of the design soil profile, considering the maximum historical effects and the maximum potential ones, respectively used to establish the operating earthquake and the design earthquake at free-field surface conditions and at foundations level.
The representative strong motion accelerograms recorded worldwide in conditions as much as possible similar to those considered to define operating and design earthquakes are selected, the corresponding response spectra are computed and at last smoothed site specific response spectra are evaluated by statistical analysis of the spectral ordinates.
Our experience indicates that this step considerably improves the evaluation of the vibratory ground motion at the site with respect to the use of the general purpose correlations among seismological parameters and engineering vibratory ground motion parameters available in the literature.

Of course, the more accurately the characteristics of the significant seismogenetic zones and the attenuation conditions between these and the site, and the N.P.P. site response are defined, the less will be the conservative assumptions required by the process.

In Fig. 2, a schematic flow chart of a probabilistic seismic assessment is shown. The whole process may be briefly described as follows:

- geological and seismological studies lead to the definition of a seismotectonic zonation, generally expressed in terms of seismic regions or provinces; the seismotectonic zonation so obtained is usually performed at a larger scale compared with the one necessary for a deterministic approach, that is seismic regions so defined extend to very wide areas;
- for each defined seismic region the fundamental seismic parameters (occurrence rate, probability density function of magnitude or epicentral intensity, and maximum potential magnitude or intensity) are evaluated;
- an attenuation model is assessed, using seismic data like intensity maps, isoseismals, accelerograms;
- the seismicity at the site is at last computed, by combining at the site the probabilities of occurrence of seismic events from every seismic region, attenuated by the attenuation laws. The seismicity at the site is usually computed in terms of recurrence mean times of intensity or acceleration at the site, or as hazard curves, that is curves representing maximum horizontal acceleration at the site vs probability of exceeding.

It is worthwhile noting that for a safety assessment the required probability levels are very low, often of the order of 10^{-6} . One of the most important consequences, is that the seismic regions defined for a probabilistic assessment must be large enough to include a sufficient number of earthquakes to perform reliable statistical analyses. Therefore all the detailed information provided by an accurate geologic study could not be properly taken into account.

The main reason is related above all to the difficulty in evaluating reliable parameters for the seismicity of small areas. In fact, for instance, the nearly exponential shape of the probability density function for magnitude or epicentral intensity imposes a very precise determination, in order to avoid glaring errors in the high magnitude range, to which the required low level probabilities correspond. A good definition of an exponential density function needs a large sampling, namely provided by the earthquakes occurred in a large areas during a long span of time. Similar considerations may be proposed for the evaluation of the other seismic parameters. Moreover, as far as the occurrence rate is concerned, non-stationary processes in time should be taken into account for very long period statistical analysis.

An other crucial point in the probabilistic process is related to the definition of the attenuation model. In particular, for the evaluation of low probability values, the distribution

of the statistical errors around a mean attenuation law, usually obtained by least-square fitting method, is of fundamental importance. In fact, low probabilities of exceeding specific accelerations or intensities just correspond to the outliers in the attenuation model. In the standard practice the statistical errors are assumed to be lognormally distributed, basically due simply to an evident asymmetry of the recorded data around the fitting line. This assumption may be considered enough reliable at most up to one or perhaps two standard deviations, but can lead to unpredictable results for more unlikely events.

Due mainly to these problems, even if the computational theory for the evaluation of the probabilities at the site is a well established matter, in our opinion the present state of the art of the probabilistic seismic assessment cannot be considered sufficient for safety purposes, and particularly for N.P.P. sites, and further studies are necessary.

The deterministic approach based upon the above described methodology is to be considered more reliable due to the fact that the seismotectonic model is the result of the agreement among a considerable amount of data namely geology, geophysics, seismology, geotechnics.

The present level of knowledge, on the contrary, recommends the use of the probabilistic studies for assessing the seismicity expected during the operational life of a structure, and anyway for periods of time comparable with the duration of the complete part of the seismic catalogues.

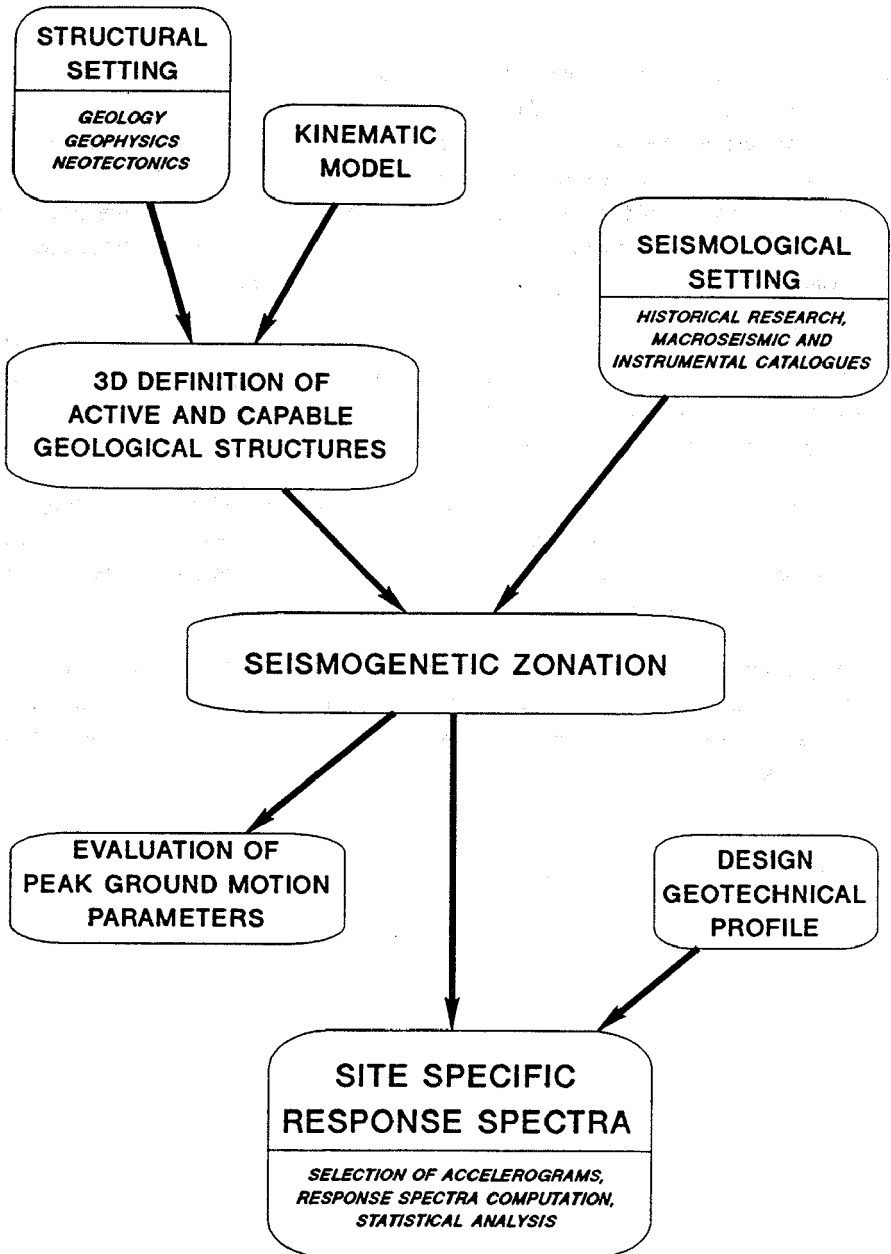


Fig. 1: flow chart of the methodology for the seismic assessment of N.P.P. sites

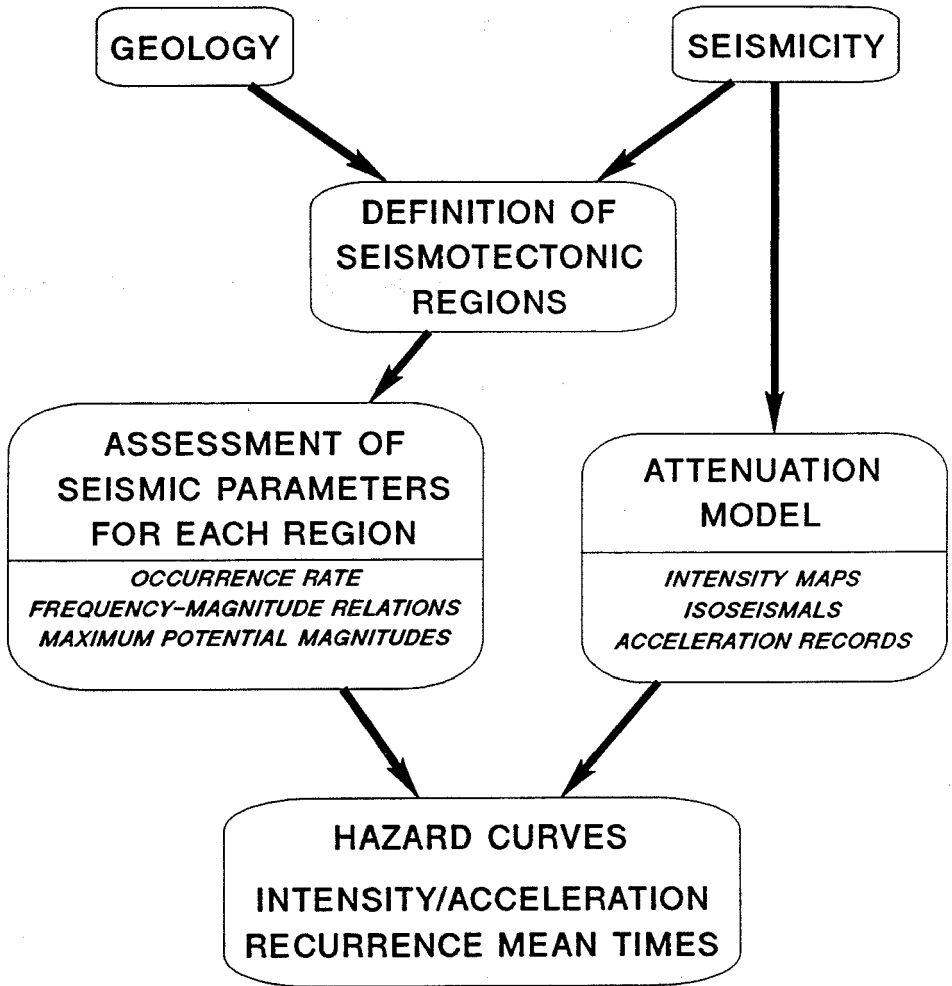


Fig. 2: flow chart of a probabilistic seismic assessment of N.P.P. sites

**CSNI WORKSHOP ON SPECIAL ISSUES OF LEVEL-1 PSA
27/29 MAY, 1981 - COLOGNE GERMANY**

**EXPERIENCE GAINED IN ITALY ON THE PROBABILISTIC ANALYSIS
OF
ACCIDENTS INITIATED BY SEISMIC EVENTS**

**A. PUGLIESE A. VALERI C. ZAFFIRO
ENEA DISP - ITALY**

a: \ haz2.wrt

INTRODUCTION

In the licensing of the past generation NPPs ENEA requested for all operating and under construction NPPs the performance of Probabilistic Safety Studies finalized to show the compliance with established Safety Goals. The current ENEA goals were:

- a) Core Damage Frequency (CDF) in the range $1\text{E-}6$ - $1\text{E-}5$ ev/y
 - b) High Releases Frequency (HRF) in the range $5\text{E-}8$ - $5\text{E-}7$ ev/y
- High Releases means ex-plant release of I-Cs $> 0.1\%$ of the core inventory.

For two of the NPPs (Caorso and Alto Lazio BWRs) the PSS [1,2] included also the evaluation of seismic contribution of the LOOSP, which in current PRAs usually represents a dominant event for Core Damage occurrence and external fission product releases likelihoods. This paper describes the experience gained for the Carso Plant, being the application to Alto Lazio conceptually similar.

THE PRA FRAME

The results of the first Caorso PSS review showed both CDF and HRF were dominated by the LOOSP event, but while the CDF met the probabilistic goal ($6.42\text{E-}6$), the HRF resulted higher than the reference goal for the ex-plant releases ($1.1\text{E-}6$). The interpretation of the results allowed the individuation of specific items where design and procedure modifications could allow the reduction of the HRF. Specifically the contribution of the LOOSP was important for both the CDF value and HRF; the LOOSP, in turn, resulted dominated by the seismically induced loss of external grid for 24 h: the importance of the seismic LOOSP was 27% on CDF and 34% on HRF.

It is known the fragility of i) electrical insulators located at ground level in the plant switchyard and ii) ceramic insulators of power transmission lines, expressed in terms of the median acceleration capacity to withstand seismic loads, is rather low, let say the median value of such capacity is about 0.2 g. Consequently it was assumed in the PSS that an earthquake with a PGA (Peak Ground Acceleration) greater than 0.2 g as capable to induce a generalized failure on the external grid, i.e. LOOSP, in the Caorso site.

The cumulative frequency of the earthquakes capable to damage the external grid ($\text{PGA} > 0.2 \text{ g}$) was roughly estimated as $2\text{E-}3$ ev/y from the available seismic data of the whole Pianura Padana. The recovery time of 24 hr was realistically assumed on the base the experience gained during past Italian destructive earthquakes, like the Friuli 1976 earthquake.

As far as the Caorso site is concerned, it has been recognized by experts that the site, even if placed inside the Pianura Padana, has a specific tectonic behaviour and the frequency of $\text{PGA} > 0.2 \text{ g}$ could potentially result substantially lower than

the mean value applicable to whole area (the value used was $2E-3$). So the a realistic seismic hazard analysis on the site - not available at that time - was considered necessary in order to support lower figures. This work has been done by ENEA in the frame of its activity on PRA review, using the in house available expertise on seismic analysis.

The situation for Alto Lazio plant is similar to the Caorso situation, i.e. a too high value of frequency for $PGA > 0.2 g$ was assumed while the local seismicity could promise a substantially lower frequency estimates.

In the next paragraph it is explained the approach used to assess the seismic hazard for the two above mentioned Italian sites, which allowed the use of four times lower values, i.e. $5E-4$ for the Caorso Plant. Some conservative assumptions made in the analysis provided a high level of confidence to results, useful to protect the decisional actions against the uncertainties associated with the basic data and the methodology. The values can be compared with those derived from the hazard curves used in NUREG 1150. The median frequencies for the same event ($PGA > 0.2 g$) are: i) about $4E-5$ in LLNL Surry Hazard curve ii) about $2E-5$ in EPRI Surry Hazard curve (see respectively Fig. 3.3 and Fig. 3.4 of [3]). The effects of the reassessed value on the PSS results were: i) a 20% reduction on CDF ($5.14E-6$) ii) a 25% reduction on HRF ($8.20E-7$).

The new seismic LOOSP value was not sufficient to meet the Safety Goal: other hardware and procedure modifications were necessary to further reduce the CDF and to push the HRF value within the $5E-8$ - $5E-7$ range. But the figures reduction coming from the seismic LOOSP reassessment was of great relative importance.

HAZARD ANALYSIS

The Seismic Hazard Analysis (SHA) provides estimates of the probability of future levels of the ground motion, using earthquake hazard models which express assumptions regarding the timing and size of events on the base of the physical understanding of all earthquake processes and with the support of a statistical treatment of the available data. SHA general procedures involve the following steps:

- delineation of the source of earthquakes and estimates of their activity rates
- description of the activity by a recurrence relationship
- description of the attenuation of ground motion with distance from the earthquake source
- evaluation of probability of exceedence for various levels of ground motion at a site.

Following the above approach the seismic hazard for the two Italian NPPS sites (Caorso and Alto Lazio) was determined. As first analysis step the seismic source zones were identified. The Italian earthquake catalog is lengthy; the CNR-PFG catalog [4], that spans over almost 1000 years, reports about 27000 events, and historical manuscripts report even on

B.C. destructive earthquakes. On the other hand the complex tectonic setting of the Italian region does not allow to establish a clear relationship between geologic structures and earthquakes. The seismic sources zones used in the PSHAs are then areas that share common tectonic and geologic attributes. Areas boundaries were evaluated not only by epicentral locations of historical seismicity but on geologic evidence as well.

In figures 1 is reported the map of Italy with the indication of historical epicenters taken from the catalogue; the location of the Caorso and Alto Lazio sites are also shown in the map. Figure 2 shows a map that indicates the boundaries of the selected seismic areas for the Caorso site, and the historical epicenters contained therein. As far as the Caorso site is concerned, for each seismic area it was assumed that the spatial occurrence of earthquakes is uniform and the yearly number of the expected earthquakes decreases exponentially with increasing magnitudes. The assessment of source seismicity mainly depended on the events taken from the CNR-PFG catalogue for the areas under investigation. This database was analyzed in order to identify the time intervals where it can be considered complete. Statistical analyses were performed on the selected events to estimate variables of earthquake magnitude recurrence model; available empirical relationships were used to estimate the magnitude of historical events. The probability distribution of earthquake size was represented with a so called double-truncated exponential distribution. The upper bound magnitude (m_l) of each source was defined when possible relying on geologic information. Otherwise m_l was defined as the magnitude that, in a linear Gutenberg & Richter occurrence relationship, has a probability of exceedence lower than 10^{-3} . Earthquakes with magnitude below 4.0 were excluded from SHA, since small earthquakes have little effects on engineered structures.

The selection of a suitable attenuation relationship is one of the most critical elements in any assessment of ground motion hazard. Attenuation model translates the hypothesis about boundaries and seismicity of a seismic source into estimates of probability of exceeding a given intensity of ground motion. Generally speaking, appropriate attenuation model should be developed by strong motion records obtained in the area under investigation or in comparable geologic, seismological and local site conditions. Since 1976 many earthquakes have triggered the Italian national strong-motion network but very few accelerograms have been recorded in the investigated region. Then the attenuation of ground motion had to be estimated using relationships based on either national or worldwide strong motion data.

Although response spectral values may be the most useful of the parameters describing ground motion, most of the available attenuation relationships deal with peak horizontal acceleration. This parameter was the most important one in carrying out PRA, as its goal was to assess the seismic probability failure of electrical insulators located at ground

level in the plant switchyard, and so the probability failure of the external grid inducing LOOSP in plant accident.

At that time available attenuation relationships were mainly developed using strong motion data recorded in western United States, most of which in California, along the S. Andreas fault. The most important relationships were developed assembling with care a suitable database in order to avoid unintentional biases such those arising from recording instruments, record processing and multiple recordings from one event.

Many problems arise in selecting the attenuation relationship to be used in the SHA, mainly because of different parameters used by authors in defining earthquake size, propagation and site effects.

Referring to the earthquake size parameter the most commonly used is magnitude and particularly the Richter local magnitude M_l , the surface magnitude M_s and the moment magnitude M , this being, more then others, a very measure of the earthquake size.

The parameter commonly used to characterize the attenuation of ground motion, as it travels from source to site, is the distance source to recording station. Among the distance measures adopted in developing attenuation relationship, the epicentral and hypocentral distances are the most readily available for earthquakes. Some authors prefer distance measures such as closest distance to rupture zone and closest distance to surface projection of rupture zone as they claim that site ground motion is mainly affected by the nearest part of the fault rupture. In any case the attenuation relations should be able to account for local geological effects that has been recognized greatly amplify the motion in selected frequency range. At that time the relationship proposed by Joyner and Boor (JB), [5] seemed to be the best choice but the distance measure. Because of methodology used in defining seismic sources these should be better considered as loci of future epicentral location. Using data recorded by the Italian strong motion network, relationships were developed using both epicentral distance (SP_e) and, merely for comparison purpose, the closest distance to the surface projection of rupture zone (SP_f); the complete description of method can be found elsewhere [6].

Fig. 3 shows two attenuation relationships using fault distance. Comparing the above relations it is evident that JB always estimates higher values of acceleration for distances up to 100 km, with higher value at short distances, let say below 15 km. Considering magnitude less than 6.5 there is that the difference is even much higher. Moreover the JB standard deviation is higher than SP_f ones. All these aspects have a great influence on estimated site hazard: at Caorso, using JB we have predicted acceleration values that on the average are up to three times those obtained with SP_f relationship. A so high ratio value can be also explained considering that, in selecting the seismic sources, one of them, let say the less credible one, was located at less than 10 km far away from the

site. Looking at the hazard results it was evident that plotting numbers of expected events versus acceleration, those curves do not show any tendency to saturate even for numbers of event less than 10^{-8} suggesting that likely the sources upper bound magnitude m_l would have been overestimated.

Fig. 4 shows results of the hazard analysis for Caorso using SP_e attenuation relationship, that for the consideration made above seems to be more realistic than others. The same general consideration applies when using SP_e relation, the curve seems not to saturate, even if the estimated peak values are a little bit higher than those estimated using SP_f .

The same approach was followed for estimating the Alto Lazio hazard, except for using only the SP_e attenuation relationship. Care was used in including seismic sources in PSHA and in selecting the m_l magnitude values. Sensitivity analyses were carried out also to estimate the amount of hazard that belongs to earthquakes having size greater than the source historical maximum one. The results show that appropriate selection of m_l values greatly contribute to avoid anomalous hazard estimation characterized by non-saturation trend.

CONCLUDING REMARKS

The seismic hazard curve for the Caorso site shown in Fig.4 indicates that the frequency of $PGA > 0.2$ g is about $5E^{-4}$. This value was obtained using a realistic assessment of the site ground motion, but using conservative assumptions for the strongest earthquakes. This conservatism was judged to be sufficient for encompassing the uncertainties of the analysis. Introducing in the PSS a set of modifications the HRF resulted within the range set in Safety Goal ($1.1E^{-7}$) and the relative contribution coming from the seismic LOOSP reassessment had an important role.

Also the CDF - even already inside the Safety Goal range - benefited from the new analyses.

On the other hand the review of the Caorso PSS was aimed at reducing the probability of the LOOSP sequences (including the seismic initiated ones) that are dominant in the assessment of the global CDF and HRF. No other seismic failures, therefore, were considered to be significant for investigating other accident sequences (as for instance LOCAs due to failures of supporting structures, or transients due to equipment malfunctions generated by seismic events). The uncertainties affecting the whole process of generation and propagation of the earthquakes to the site, and the plant response to the site ground motion at the subsoil level, are so high that no reliable predictions can be made for the seismic loads acting on the various structures and safety systems of the plant. The seismic failure rates for such structures and equipment are determined with large uncertainties that could be also quantified through available stochastic techniques. That leads to conclude that the limited application for the Caorso PSS is valuable for assessing the actual CDF and HRF values for making decisions on the plant safety. Other results from a

more complete seismic risk analysis could be wrongly interpreted and not properly used for making decisions.

REFERENCES

- [1] CAORSO PSS - Report NO. ENEL DCO 401.V040.VR001; rev1-June 1988
- [2] ALTO LAZIO PSS - Report NO. ENEL AZ1.0040.RRXP.3561.01-Sept 1986
- [3] NUREG/CR-4840 - SAND 88-31102 - Procedures for the External Event Core Damage Frequency for NUREG-1150
- [4] CNR-PFG - Catalogo dei Terremoti Italiani dall' anno 1000 al 1980 - 1980
- [5] Joyner, W.B. and D.M. Boore - Peak Horizontal Acceleration and Velocity from Strong Motion Records Including Records from the 1979 Imperial Valley, California, Earthquake - Bull. Seism. Soc. Am. 71,2011-2038 -1981
- [6] Sabetta, F. and A. Pugliese - Attenuation of Peak Horizontal Acceleration and Velocity from Italian Strong-Motion Records - Bull. Seism. Soc. Am. 77, 1491-1513 - 1987

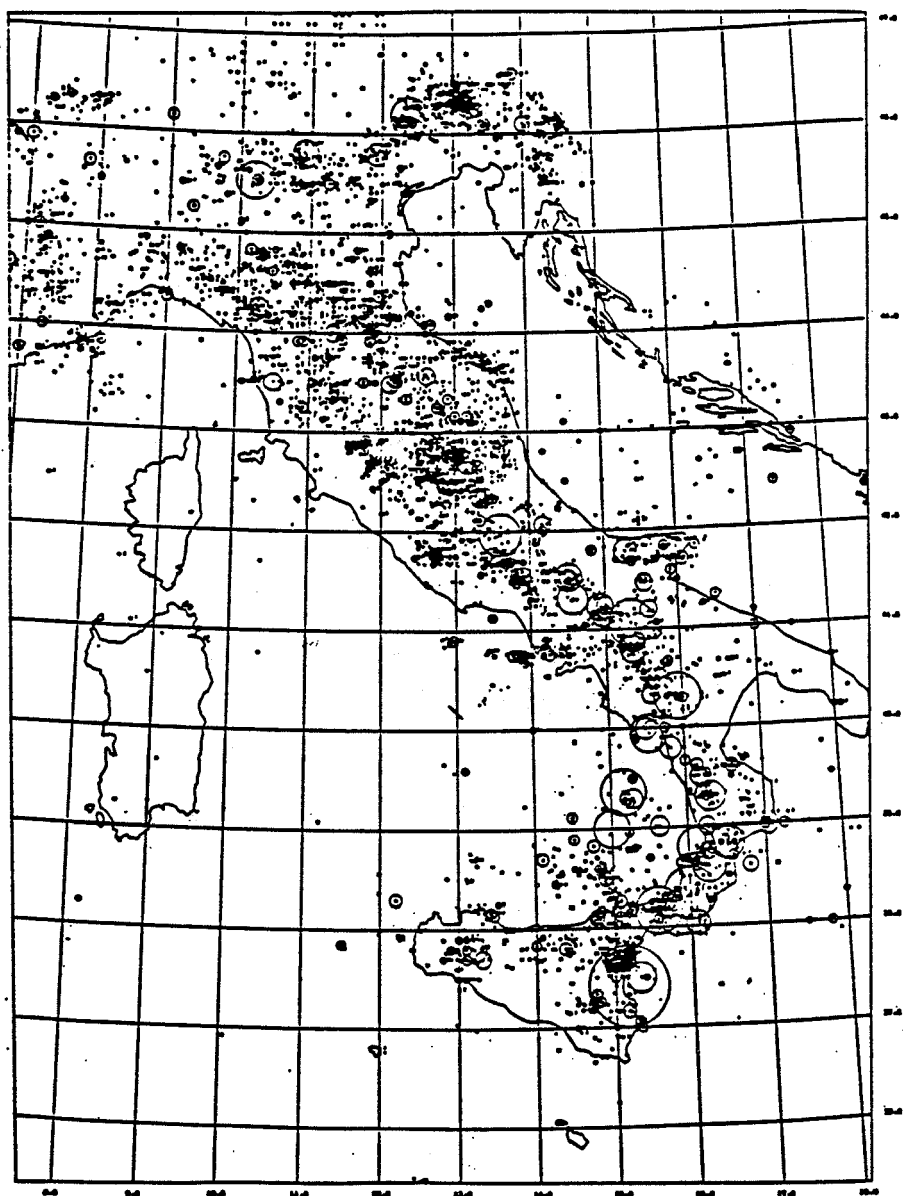


Fig. 1 Map of the Italian historical epicenters
(from the CNR-PFG catalogue)

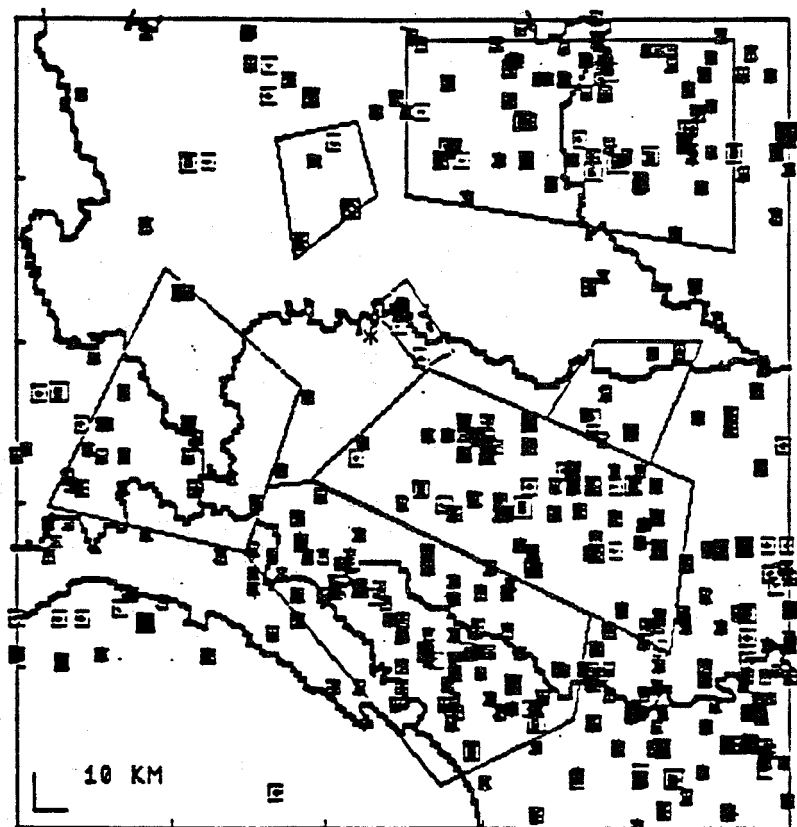


Fig. 2 Map of the Caorso seismic areas

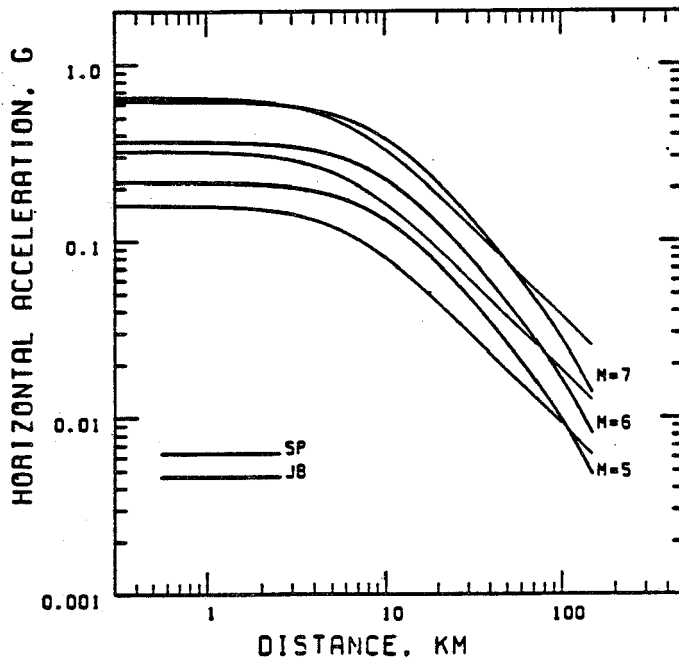


Fig. 3 Earthquake attenuation relationship

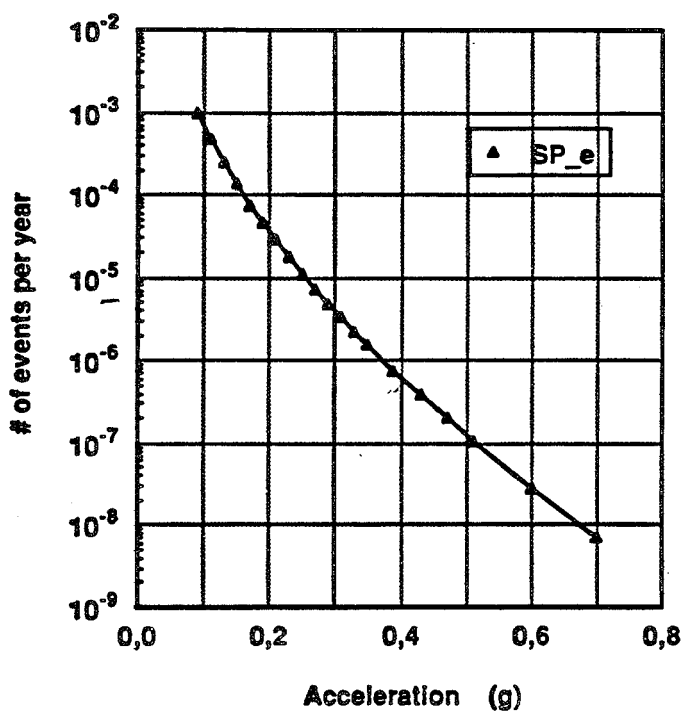


Fig. 4 Seismic Hazard for Caorso

Special Topics

Chairman: R. Stück

H. Pamme, L. Seyffarth, RWE Energie AG, Essen

Experiences with data collection, retrieval and interpretation for PSA purposes

OECD/BMU Workshop on "Special Issues of Level 1 PSA"

Köln 27.-29.5.91

H. Pamme, L. Seyffarth, RWE Energie AG, Essen

Experiences with data collection, retrieval and interpretation for PSA purposes

1. Introduction

One main activity within the PSA framework is the collection of plant specific availability and reliability data. In the past however most nuclear power plants had not focussed their technical data collecting activities directly towards the generation of statistical reliability data. Thus only "alternative" data banks are available which e.g. have stored technical data for logistic, maintenance or management purposes. In order not to loose the historic experience (beside significant events which are welldocumented) these data sources must be analysed to reveal the "hidden" informations for the data generation task in probabilistic assessments.

This paper intends to demonstrate this data retrieval and analysis procedure within RWE nuclear power plants (RWE-NPP). The available technical data sources and the combined use of various data banks will be described. One example will show the retrieval, analysis and interpretation of failure events.

2. Data flow and data bank structures at RWE-NPP

Figure 1 provides an overview of different data sources and data banks with potential relevance for the generation of probabilistic data. The data banks are decentralized and available at each RWE-NPP in the same structure. The vertical axis shows the time points of the (realized or intended) installations.

The most important basic informations concerning failure events is contained in the work orders. These work orders (as form sheets) are required for all technical activities on all components within the plants. Their main purpose however is up to now not the detailed description of failure events but the planning, control and documentation of maintenance and repair activities. The work orders are correlated to components by the use of a plant codification system. Short text informations can generally be added to describe the failure or deficiency.

Most informations of work orders are collected in the ISIS-data bank (ISIS = "Instandhaltungs-Steuerungs- und Informations-System" = maintenance control and information system).

The AES-data bank (AES = "Anlagen-Erfassungs-System" = plant inventory system) contains component data and descriptions with a mainly logistic orientation (e.g. manufacturers, parts lists).

The NOVA-system (NOVA = "Nachweis des ordnungsgemäßen Verhaltens der Anlage" = documentation of regular plant behaviour) was originally installed as an analytic tool to check and document the regular starting procedures and sequences of safety systems after test and demands (e.g. transients). It contains mainly binary signals of specific electronic limit switches, sensors and breakers from the process computer.

The FRAU-data bank (FRAU = "Freischaltungen und Aufträge" = system isolation releases) contains all informations concerning system or component isolation activities (e.g. to allow repair or maintenance activities on safety systems) within the plant. The release form sheets together with references to the corresponding work orders serve as input informations to the FRAU-data bank.

The ASS-3-data bank (ASS = "Anlagen-Schadensstatistik" = plant related failure statistics) contains "improved" informations of failure events for components of important operational and safety systems. The ISIS-data for these components are supplemented by codifications (e.g. concerning failure causes) and further background informations of the failure event. These supplements are prepared within the technical departments of the plant. The ASS-3-data bank was installed as an information source mainly to optimize the availability of the plants.

These described data sources must be combined to derive "task-specific" reliability parameters. The term "task-specific" here refers to a clear definition and description of what has to be quantified (e.g. failure probability for a sudden failure per demand or event rate for a specific external leakage). It is obvious that the ASS-data-structure and the available depth of information provides the easiest approach to start an engineering analysis of failure events.

3. Requirements for the statistical derivation of reliability data

The "task-specific" derivation of statistical reliability parameters requires the definition of event conditions which caused a specific failure. Thus the set of available component and event based informations from the different data sources must be manually "filtered" until a remaining subset of suitable events is revealed. This subset forms the "sample" for the further statistical treatment.

With a combined use of the available data banks at RWE-NPP the "environment" and conditions of a failure event can be reconstructed. The following table gives some examples which informations can be derived from the various banks:

Data bank:	AES	ASS-3	ISIS	NOVA	FRAU
Parameter:					
Event descriptions		X	0		
Time point of event		X	X	0	
Unavailability times		X	0		0
Repair times		X	0		
Repair activities	0	X			
Startup-frequencies		X		0	
Operating times		X		0	
Component life times		X	0		
Reactor status		X		0	
"Sample size"	X				
System unavailabilities					X

The "X" shall indicate that the corresponding information is mostly available in a good quality, the "0" indicates that a detailed analysis of raw data is required to derive the "true" information.

4. Example

The available amount of historic information in the various data banks with relevance for the generation of probabilistic data shall be discussed in the following example.

The "global task" was the analysis of failure events of high pressure transducers (within the reactor protection system) which indicate the reactor pressure. The "specific task" was the analysis of events which led to a (more or less) sudden loss of a pressure signal during operation. The aim should be the estimation of a failure rate for the sudden loss of a pressure signal in the reactor protection system. The component boundary for the transducers was the component housing including the electrical and pipework connections.

4.1 Derivation of the sample size

The analysis of the AES-bank for the RWE-NPP (Biblis with 2 PWRs, Mülheim-Kärlich PWR, Gundremmingen with 2 BWRs) revealed that all plants use trans-

ducers with a Bourdon tube mechanism for the reactor pressure measurement. This type of transducers is also used in other systems (e.g. feed water system) but the sample was restricted to transducers with the described function.

An overview of the operating experience is given in the following table:

<u>Plant:</u>	<u>Gundremmingen</u>	<u>Biblis</u>	<u>Mülh.-Kärlich</u>
Number of transducers	2 x 9	2 x 12	8
Operating experience (in years)	12.5	29	~ 1
Observed events	1	2	1
Observation period (in reactor years)	12.5	10	1

The "operating experience" is based on years with real plant operation (including plant revisions). Here it is assumed that the "life consumption" of transducers mainly takes place during phases with a pressurized reactor vessel. The sample contains 50 transducers, the cumulated observation time (for this example) is approximately 240 years.

4.2 Event analysis

The observed 4 events with a (nearly) sudden loss of function were found within 310 ISIS data bank entries. Most of these entries only document periodic testing activities. This kind of transducers is up to now not included in the ASS-3-data bank. One example of an ISIS-data set is shown in figure 2. It becomes obvious that the detection and analysis of these data sets is a necessary engineering task and effort.

Furthermore the experience has shown that pure data bank inquiries which are only based on the use of codified informations can lead to incomplete or irrelevant events in samples. Only a sufficiently "intelligent" access to a data bank can reveal also those relevant informations which are available but stored at a "partially wrong" place (e.g. produced by codification errors or non-exclusive codification options).

The detected relevant events are shortly described in figure 3. Obviously the failures with a sudden character are very quickly detected by the voting logic of the reactor protection system.

Event number 4 is often cited in the German "nuclear community" as the "classical" common mode failure (CMF) for transducers. It must however be noticed that this event with multiple failures did not influence the function of the mechanical and electronic parts of the transducers under normal operating conditions. Only a coincident LOCA-event might lead to humidity or water ingress into the transducers and thus lead to potential malfunctions. However due to the use of diverse components (2 groups of 2 transducers) within one reactor protection redundancy (here 2 out of 4 voting logic) even these multiple failure events under LOCA-conditions would not lead to an erroneous pressure output signal of the reactor protection system.

Another interesting result of this event analysis was that also incipient failures (within the tolerance of the voting logic) mostly had their origin in the electric/electronic parts of the transducers (e.g. drift of resistors). These incipient failures were all revealed within periodic tests.

4.3 Quantitative assessment

The analysis showed that sudden failures of transducers were not observed up to now coincidentally with reactor trips (e.g. transients). Failures are detected very quickly after their appearance (e.g. wrong calibrations within revisions detected during warm-up phase) or failures are "self-annunciating" due to the voting logic of the reactor protection system.

Due to this experience the failure rate for sudden failures of transducers is estimated to be "around" 10^{-6} /hour (assuming the exponential model). The potential event rate for multiple coincident failures (CMFs) of transducers is estimated to be significantly smaller.

4.4 Data limitations

The above discussed data bank structure and the example showed that the historic experience since ~ 1982 can be revealed with an at least satisfactory information quality.

The quantification however must mostly be correlated to (estimated) cumulated operating times of a whole sample. Individual lifetimes of components or parts of components which are not contained in the ASS-3-data bank are very often not available. Thus potential ageing effects of components can only (if at all) indirectly be detected e.g. due to increased spare parts consumptions.

Additionally the "life cycle" (consisting of subsequent operation and repair phases) of many individual components within the plant cannot be traced back.

These disadvantages will be solved for "PSA-relevant" components by the development of a relational data bank system which is especially designed to reduce the manual effort of data analyses (as still shown in the example above). Furthermore extensions in the ASS-3-bank will improve the data quality and quantity.

5. Conclusions

The available data bank structure which was originally not designed for the derivation of reliability parameters allows the retrieval and analysis of failure event data and operational data. Due to the varying quality and quantity of raw data informations with respect to special reliability or availability questions engineering and combinatorial effort is required to reveal the partially hidden event history.

It also became obvious that not all data bank entries entitled as "failures" (with given failure modes) are relevant with respect to a specific probabilistic question. This fact also emphasises the necessity for individual data analyses which gain more insight in a component failure behaviour than the simple acceptance of "generic" and abstract data from literature.

Thus a global complaint concerning the lack or scarcity of reliability data (i.e. either failure or "success" data in case of no failures) is no longer justified. This statement seems to be valid also for other utilities because comparable data collections are also available at other nuclear power plants.

RWE has started a project to ease the combined access to the various data banks at RWE-NPP. The result will be a relational data bank system which will allow a centralized analysis of the component history. Additionally the statistical treatment of qualitative analysis results will be possible.

Figure 1

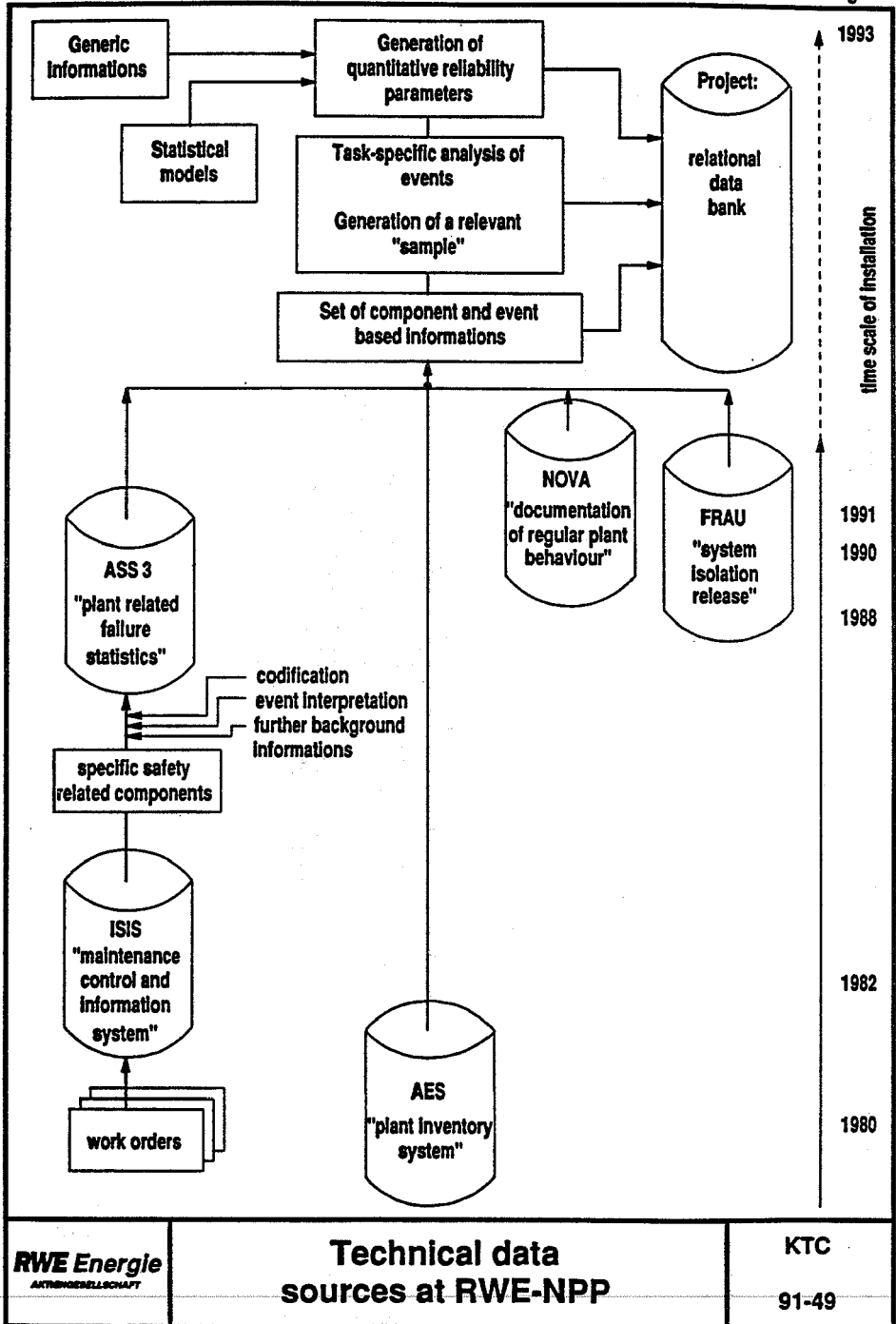


Figure 2

KKS/ARZ1 STAMM SG		T S L K CODE		PLANR		ABKL ZHOEFFN		1.TANA		V		PL/PA-V		V-PLZT		V-PLARO		ABN-ZERT	
AUTNR AA		KKS/ARZ		P W		ABKY		ABSENDE		DATLEANA		PL/PA-E		E-PLZT		E-PLARO		ABN-KOST	
T E X T						ABSCHLUSS		ISTSTD-E		ISTSTD-F		ISTSTD		ISTRK		2 X K X			
21YC04		075859 2		R 5 9		X		IR10		29.11.86		29.11.86		2 28 3		12			
		075859 N		21 YC04 P101				PBB		03.12.86		01.12.86		28 3		12		289750	
										10.12.86		7		6		13		289750 108	

Figure 3

Event Number	Event description	Reactor state	detection	event cause	repair activity
1	wrong pressure indication (deviation of -16 bars)	warm-up phase after revision	2 out of 3 voting logic of reactor protection system	human error, miscalibration during revision	new calibration
2	no electric output signal	revision	in-service test	human behaviour, incorrect treatment during revision	plug changed, output signal transformer changed
3	wrong output signal (deviation of -1 mA = -5 bars)	power operation	2 out of 3 voting logic of reactor protection system	malfunction of capacitor in the power supply unit	exchange of transducer repair at manufacturer
4	potential loss of function in LOCA events due to humidity ingress via a lost or loosened plug, potential common-mode-failure !	"LOCA" required	during periodic inspection	loss of plugs or loosened plugs, wrong tolerances between plug and housing	exchange of transducers, modification of plug
Event summary					KTC 91-51
RWE Energie <small>ANTENNEBESCHULT</small>					

**Frequencies of Leaks and Breaks in Safety Related Piping of
PWR-Plants
as Initiating Events for LOCAs.**

by S. Beliczey
Gesellschaft fuer Reaktorsicherheit (GRS) Cologne, Germany

To be presented at the OECD/BMU Workshop on "Special Issues of Level 1 PSA" Cologne (FRG) May 27-29, 1991.

Introduction

We are looking here at the frequency of leaks and breaks as far as they are initiating events, not as caused by say external events. The LOCA-relevant piping of the plant is that fraction of all the piping that contains primary system coolant. It consists of piping of various nominal widths ranging from 10mm (piping for instrumentation and control) up to 800 mm (main coolant recirculation line).

Piping is involved that retains the reactor coolant against an atmospheric environment, but also piping that separates the primary coolant from the secondary steam system (inside the SG). This indicates a large range of possible leak sizes.

The analysis of the effects of LOCA events shows, that there are various ranges of leak rates that are to be distinguished corresponding to the capabilities of systems that are directed to assure the safe condition of the plant (1. slide). The actuation and subsequent operation of these systems is a further barrier to prevent core damage.

Other ranges apply for the steam generators.

The frequency of some leak rates will be dominated by inadvertent or faulty opening actions of valves.

Some LOCA-relevant leak rates however are mainly caused by wall-penetrating cracks or a break of a pipe. These damages in the walls of the primary coolant retaining system and their frequencies will be discussed here.

Description of the system considered

The systems to be considered are shown schematically in the slides 2.-4. Slide 2. is a view of the primary coolant loop. The nozzles are to be seen, where the surge line and the RHR systems are connected to the recirculation lines.

Slide 3. shows the primary Coolant Volume Control System schematically.

Finally, slide 4 shows the Residual Heat Removal System. This system is operated at pressure levels different from the pressure at normal power operation. In addition, leaks or breaks of the primary coolant retaining system inside the steam generators, i.e. of the SG-tubes, are to be considered.

Distinctions are to be made with respect to the location of the leak for at least two reasons:

- To make a probabilistic statement on a LOCA it is necessary to know whether the leak can be shut off from the reactor circuit. If yes, there is an additional barrier existing before a LOCA.
- The effect of a leak is not necessarily confined to the loss of the coolant. In some compartments it can cause the flooding of equipment that is necessary for the actuation or operation of important machinery.

Methodology

Now the question arises, how operating experience and theoretical considerations can be used to determine frequencies of various leak rates in various sections of the piping to be considered.

First, structures have to be identified that are liable to failures. Experience shows, that cracks occur mainly at the vicinity of discontinuities such as wall thickness changes, branchings, junctions and turns. Usually such structures are manufactured by applying welds. The frequency of failures in straight pipe sections can be neglected in comparison with failures in the structures just mentioned.

Using these ideas, we come to the conclusion, that the frequency of failures is not determined by the length of the piping, but rather by the number of structures liable to failures. We call such structures risk relevant (or leak relevant) structures. Thus, operating experience and the statistics drawn from it is not being related to a plant or a group of plants, but to the amount of risk relevant structures of various sizes that are present in all plants that are considered as data basis.

Now some remarks on the possible sizes of leaks: For piping designed and manufactured to the very stringent standards of the primary system of a PWR and at the stress level given in such a piping, fracture mechanics considerations show, that the maximum leak size to be reasonably taken into account - apart from a total break of the guillotine type - is at about 2 per cent of the pipe total cross section. (slide 5). This slide displays all cross sections to be taken into account in the primary circuit.

Slide 6 shows the amount of leak relevant structures.

To use statistical evidence, not obtained but from operating experience with the plant considered, can lead to an extremely pessimistic estimation of frequencies and even to contradictions. Even additional experience with similar plants does not improve the situation satisfactorily.

For safety related piping in a PWR not only the number of leak and break occurrences is low, but also the amount of operating experience compared with that of other technical systems. The statistics that can be drawn from this situation yields very large uncertainties with respect to the frequencies that should be assigned to leak and break occurrences. Further if no additional mathematical models were used, a zero occurrences statistics for both a leaking crack and a break within the same diameter category would mean the same frequency for both kinds of failure, of course within the uncertainties given by such a statistics.

I am taking an example:

The statistical evidence "In 100 years of operating experience no occurrence of a break of a main coolant recirculation line." would lead to an interval estimation of the frequency:

The 95% quantile of the frequency distribution of a break of such a line is

$$\lambda_{95} = 1.9 \times 10^{-2} / \text{Year}$$

the mean value being $\bar{\lambda} = 5 \times 10^{-3} / \text{Year}$

This uncertainty in knowledge is rather useless!

Another example:

The statistical evidence: "In 100 years no occurrence of even a smallest leak in a line of nominal width in the range DN 100 -150." would yield the same estimate for the frequency of a leak as found in the previous example for a break.

Engineering judgment would suggest that the frequency of such a small leak in a piping of less stringent quality assurance must be much larger than that of a break in a 800 nominal width piping!

The results of the two statistics mentioned, do not contradict to this statement, though they cannot confirm it because of the great uncertainties involved.

So what is to be done in such a situation?

If zero occurrences (faults) statistics apply for an event, a precursor of the event should be identified if possible.

The statistics of this precursor may consist of more occurrences, or may still be based on zero occurrences.

Anyway, the frequency of e.g. a break could then be estimated from the statistics of a precursor e.g. of any leak, multiplied by the conditional probability that a leak is caused by a break given that any leak has occurred.

Though a representative distribution of the number and the size of flaws and a statistics of the activation of crack generating mechanisms is not known, a rough estimation of the ratio of the frequency of a break to that of any leak λ_B / λ_L has been tried.

Considerations made at the estimation of this ratio are displayed on slide 8.

Operating experience with PWR primary circuit piping shows that for DN 25 piping (DN ...nominal diameter in mm), taking $\lambda_B/\lambda_L=0.1$ is of the right order of magnitude.

Probabilistic fracture mechanics calculations for large diameter PWR-piping e.g. /1/ (DN350 -800) show λ_B -values that are by about six orders of magnitude less than the corresponding λ_L -values. For BWR-piping λ_B differs from λ_L by three or more orders of magnitude. However the assumptions of these calculations are not satisfactory, the flaw distributions being taken from weld samples too little.

These considerations and the intention of being conservative with the λ_B/λ_L -values led us to a simple ansatz for the dependency of / on the nominal diameter of the piping considered.

We take the relationship:

$$\lambda_B / \lambda_L = \frac{2.5}{DN}.$$

valid for the diameter range 25 to 200 mm.

In primary circuit piping in the range of DN 80 to DN 150 there had been no occurrences of leaks even of the smallest size. For piping DN 50 three small leaks have been experienced. There have been no breaks.

Now we face the difficulty of having some piping of nominal width that is present only in a very small amount. Applying zero fault statistics to such small amounts would again lead to results contradictory to the values obtained from piping of a similar but not the same nominal width, but of a greater amount.

For piping in the range DN 50 - DN 150 it was desirable therefore to regard them as a common sample, to avoid too small reference samples for zero leak occurrences. Though the diameters are differing, the potential leak causing mechanisms are quite similar due to similar loadings and manufacturing criteria.

Considerations on the conditioning of leak-frequency on piping size /2/ yield relations shown on slide 9. The relation:

$$\lambda_L = C \cdot \frac{L \cdot D}{t^x}$$

is applicable if the stress level is kept konstant.

L can be interpreted as the length of the piping as has been done in some statistics, or as the number of risk relevant spots, as we have done it

t is the wall thickness

C a factor of proportionality that can be determined from the overall statistics.

The exponent x can be determined on the basis of different hypotheses but also from failure statistics of extended piping systems.

In our study the D/t-ratio of the piping in the range of DN 50 - DN 150 has been constant D/t=10. The exponent was chosen 2, based on /2/.

The weighting of the piping of different diameters for the leak frequency from statistics has been performed with formula (2 (slide 9)).

Piping with nominal width equal or greater 250 mm within the primary circuit meets the break exclusion considerations.

The description of the conditions needed for break exclusion would need some more time than available now.

However if statements in terms of probabilities are needed, we cannot set the frequency of a break zero.

Worldwide probabilistic fracture mechanics calculations show results for the frequency of a break of such piping that are much below 10^{-9} /year.

Because of some reservations with respect to the assumptions of those studies we restrict our statements to:

"The frequency of breaks of a piping of nominal width equal or greater 250 mm is less than 10^{-7} /year."

We regard this as a conservative statement.

Now let me outline the considerations that have been made to determine the frequency of leaks in the steam generator:

Different ranges of leak rates are to be distinguished here as compared to the piping considered so far. The reason is, that primary coolant leaking out through the steam generators is getting outside the containment and therefore lost for emergency core cooling.

Experience with SG-tube deteriorations shows that no mechanism is to be expected that causes the break of more than one tube simultaneously, except for the impact of the break of one tube on one of its neighbors. Thus the break of one tube can be regarded as a precursor of a multiple break. The probability of a breaking tube to cause the break of a neighboring one is considered to be little, but of course not zero.

For the frequency estimation of the break of a single SG-tube, a zero faults statistics, derived from the experience with KWU-type PWRs has been used. The statistics is based on an experience of about 90 years of operation.

The frequency of a simultaneous break of two SG-tubes has been calculated by a Monte Carlo simulation of the impact of a breaking tube on its neighbors.

Before showing the results, some general remarks on the method to determine the frequencies should be made.

The results are distributions that say what we currently know about the frequency of the events we are interested in (e.g. a break).

We try to find some generic data, to form a prior probability distribution for the unknown failure frequency. This distribution is to be updated or specialized by specific statistical evidence using Bayes' theorem.

To get generic data turned out to be difficult owing to the very specific operation conditions of the primary system of a PWR.

Let us have a look once again at the large diameter piping of the primary system:

The prior distribution of the frequency of a leak, that must be taken from some reasonable consideration lies at values, that are by some orders of magnitude smaller than the distribution that can be derived from the statistical evidence.

In this situation Bayesian inference shows, that the importance of statistical evidence for the large diameter piping is little. It is confined to the statement:

"The statistics is in no contradiction to the frequency, that has been determined from general considerations".

Slide 10. summarizes the methodologies used with piping of different diameters in the primary system.

The results

The results, except for the steam generators are shown in slide 11.

The table shows the most frequent mechanism, that causes a leak in the given leak range.

Leak areas less than 2 cm² do not require actions of safety directed systems, thus they are not relevant for our pursuit.








The frequency of the leak category 2-12 cm² is by a good order of magnitude higher than that of the next higher category.




The frequencies of leaks greater than 200 cm² may be regarded as the probabilistic expression for the exclusion of such leaks.

Slide 12 shows the results for leaks in a steam generator.

References

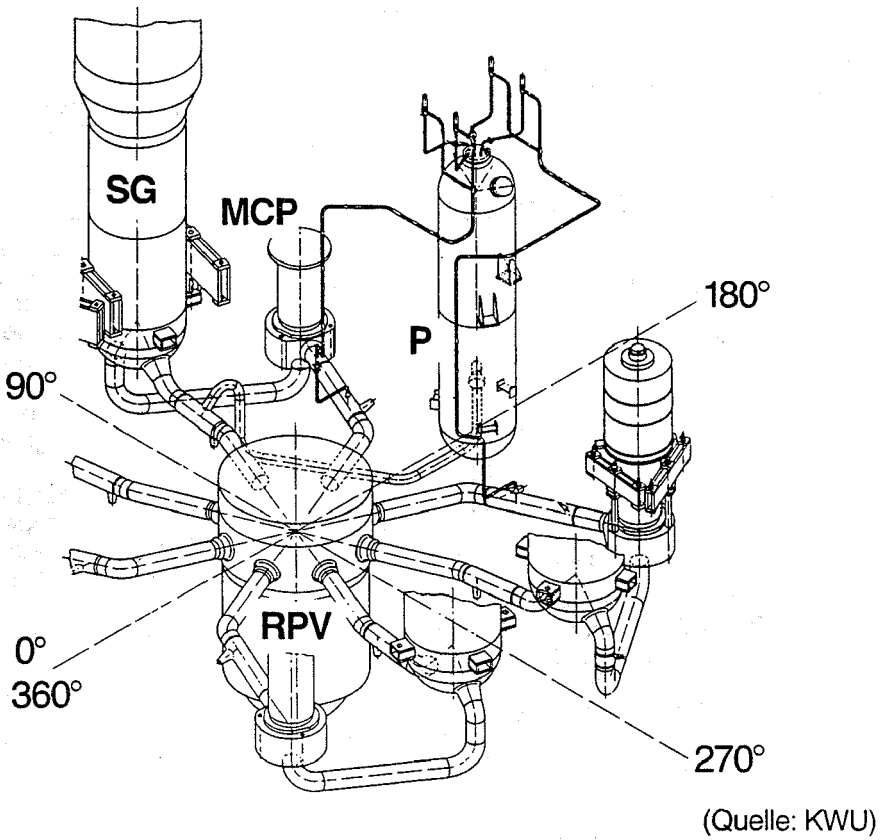
-
- /1/ Hegemann, J. et al.
"Deutsche Risikostudie Kernkraftwerke, Phase B" Ausloesende Ereignisse und Ereignisablaeufe fuer Kuehlmittelverluststoerfalle.
RWTUEV Essen, Jan. 1985.
 - /2/ Thomas, H.M.
Pipe and Vessel Failure Probability
Reliability Engineering 2 (1981) pp 83-124

Leak cross section (cm ²)	System functions required					
	High pressure injections	Accumulator injections	Low pressure injections	Low pressure recirculations	Admissible delay of secondary side cooldown (min)	Feedwater supplies
 > 500	—	—	1	1	∞	—
 200–500	1	—	1	1	∞	—
 300–500	—	2	1	1	∞	—
 80–200	3 or 4	—	2	2	∞	1 main feedwater supply or 2 aux./emergency feedwater supplies
	2	—	1	1	60	
	1	—	1	1	30	
 50–80	2	—	1	1	60	
	1	3	1	1	60	
	1	—	1	1	30	
 25–50	2	—	1	1	90	
	1	—	1	1	60	
 2–25	1	—	1	1	> 120	
	—	—	1	1	30	

-  large leak
 medium leak
 small leak

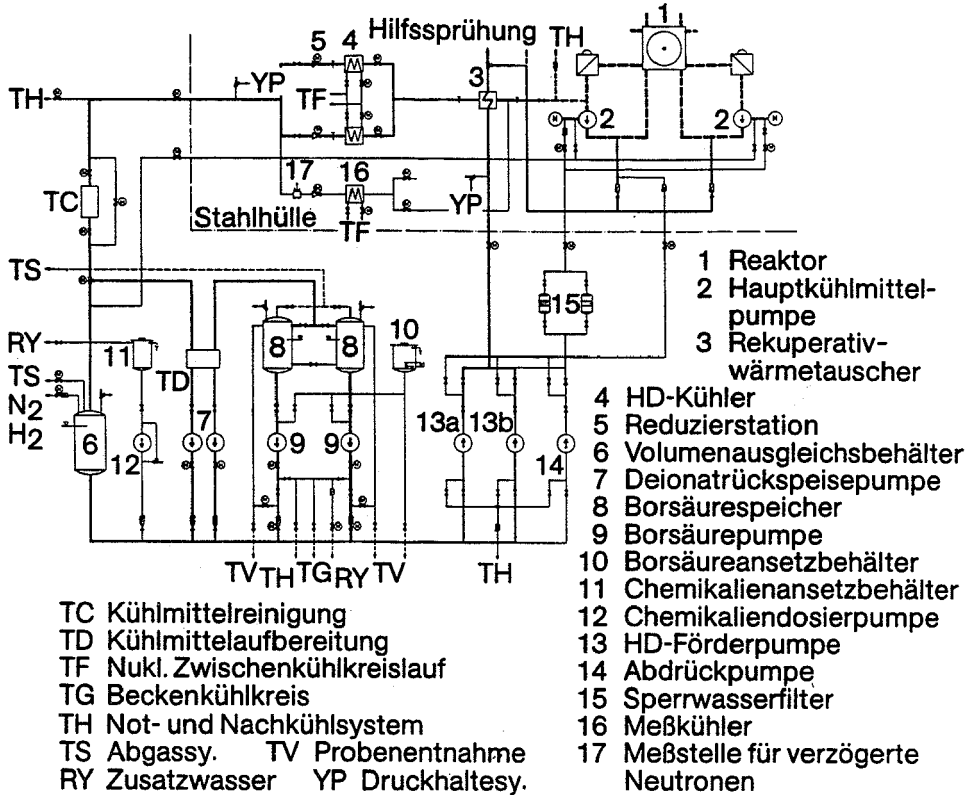
Minimal Requirements for the System Functions
for Emergency Core Cooling and Residual Heat
Removal in Case of Leaks in a Reactor Coolant Loop

Fig. 1



VIEW OF PRIMARY COOLANT LOOP

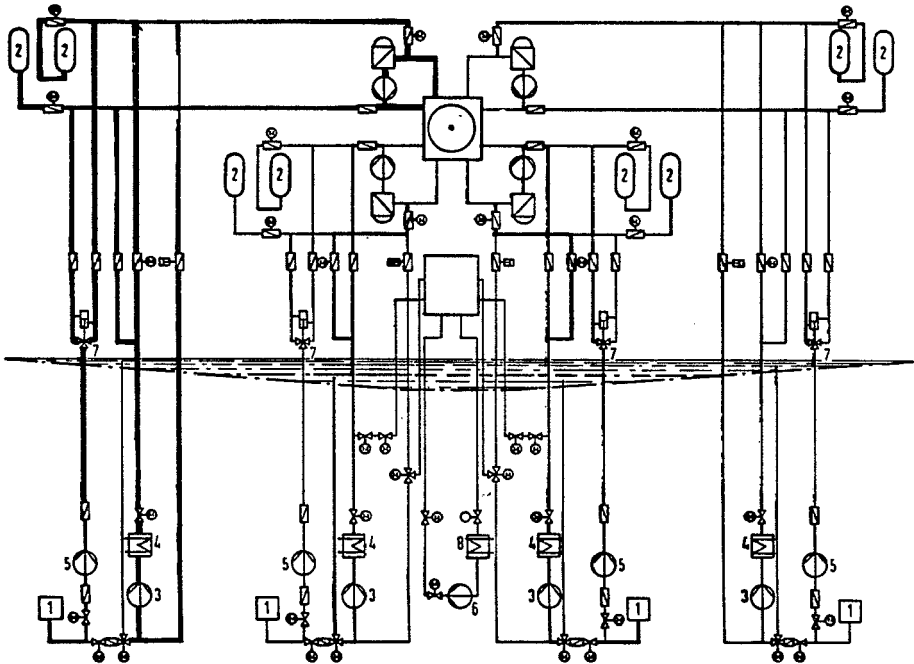
Fig. 2



(Quelle: KWU)

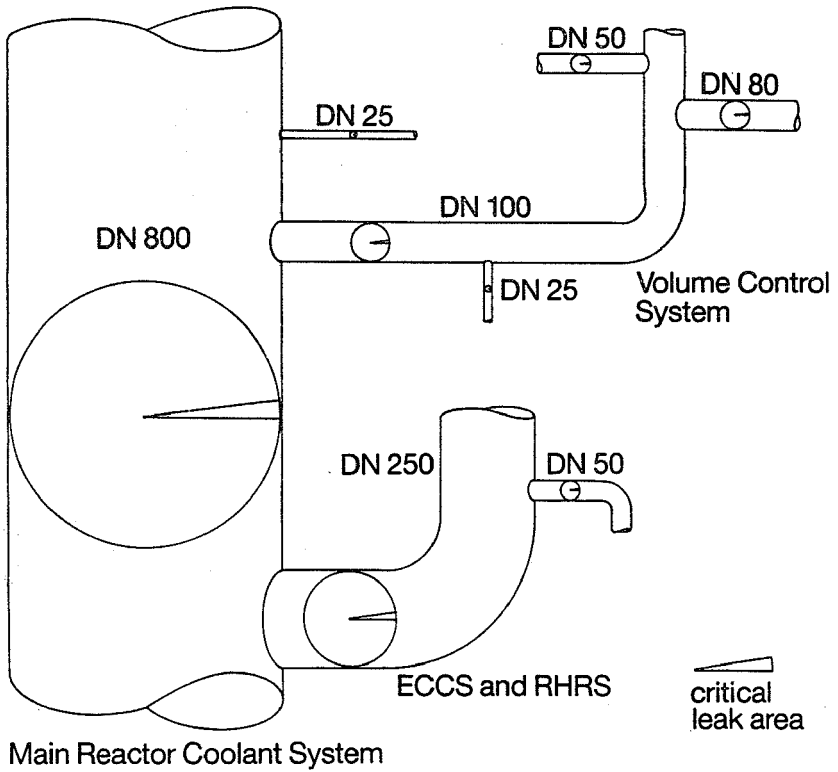
VOLUMENREGELSYSTEM PRIMARY COOLANT VOLUME CONTROL SYSTEM

Fig. 3



ECCS AND RHR SYSTEM

Fig. 4



NOMINAL DIAMETERS OCCURRING IN DIFFERENT PRIMARY COOLANT CONTAINING SYSTEMS

Fig. 5

Risk Relevant Areas

Number of Spots of Potential Leak N (DN)

nom. dia. DN	operation conditions	within containment		out of containm.		
		leak can not be shut off		leak can be shut off		
		1A	2A	once 1A	twice 1A	1A
800	POWER	0	64	-	-	-
400	RHRS	-	-	-	-	48
350	POWER	10	0	-	-	-
300	RHRS	-	-	-	64	115
250	POWER	28	0	-	-	-
250	RHRS	-	-	148	40	40
150	POWER	18	0	-	-	-
125	RHRS	-	-	32	84	20
100	POWER	12	0	38	-	34
100	RHRS	-	-	64	-	28
80	POWER	(16)	(16)	4	24	36
80	RHRS	-	-	-	24	-
50	POWER	32	16	-	-	12
50	RHRS	-	-	-	-	48
25	POWER	435	0	24	-	20
25	RHRS	-	-	-	48	48
15	POWER	74	0	12	8	18
15	RHRS	-	-	92	-	80

DN... In mm

RHRS... residual heat removal system (during refuelling)

()... depending on valve opening condition

1A... leak from one side

2A... leak from both sides

Fig. 6

Tendency of conditions with increasing diameter:

Piping manufactured of the same material and designed for the same pressure duty

- loadings due to vibrations not taken into account at the construction and the design are of decreasing influence
- transient loadings from liquid flow (e.g. closing actions of valves) are taken into account at the design for larger piping
- the number of layers of weld beads is increasing, thus the influence of faults of a single weld-bead are decreasing
- conditions at the manufacturing can be better monitored and prescriptions on supervision are more stringent
- additionally to general plant operation-supervision the number of recurring inspections is increasing
- the reliability of leak detection in an early phase is increasing due to the larger amount of leak

Fig. 8

**Leak frequency vs. piping size
(same stress level, same material)**

$$\lambda_{L_D} = C \cdot \frac{L_D \cdot D}{t_D^x} \quad (1)$$

L_D length of the piping with diameter **D**
or number of "risk relevant" spots

D diameter

t_D wall thickness

x exponent, $2 \leq x \leq 3.5$

$$C = \frac{N}{\sum_D \left(L_D \cdot \frac{D}{t_D^x} \right) \cdot T} \quad (2)$$

T operating time

N number of occurrences

Fig. 9

PRIMARY CIRCUIT PIPING

three different sets of conditions and corresponding approaches to the determination of leak frequencies.

DN < 50

- operating experience used:
 - ▣ statistics of leaks from cracks
 - ▣ statistics of leaks from breaks
- determination of leak frequencies:
 - ▣ statistical inference

$50 \leq \text{DN} \leq 150$

- operating experience used:
 - ▣ statistics of leaks from cracks
- determination of leak frequencies:
 - ▣ overall statistics, specified by
formulas for the dependence of crack and break
frequencies on nominal bore, and
ratios of frequencies of breaks to those of wall-
penetrating cracks in dependence of nominal bore

DN \geq 250

- operating experience does not yield more than the
statement:
“no contradiction to results drawn from fracture
mechanics considerations”
- determination of leak frequencies:
consideration of results of fracture-mechanics-based
probabilistic analyses performed on piping of high
quality standards

Fig. 10

leak area cm ²	major contribution	parameters of confidence interval	frequency/(plant-year)		
			leak that cannot be shut off	leak that can be shut off once	leak that can be shut off double-fold
> 0.05	wall penetrating crack	λ_{50}	1.4 E-1	1.4 E-2	6.3 E-3
		λ_E	1.5 E-1	1.5 E-2	7.4 E-3
		λ_{95}	2.7 E-1	2.8 E-2	1.6 E-2
0.05-2	sev DN	λ_{50}	2.4 E-3	8.7 E-4	6.6 E-4
		λ_E	5.4 E-3	1.1 E-3	8.5 E-4
		λ_{95}	2.1 E-2	2.7 E-3	2.2 E-3
2-12	sev DN	λ_{50}	2.2 E-3	1.4 E-3	3.0 E-5
		λ_E	2.8 E-3	1.8 E-3	8.0 E-5
		λ_{95}	7.3 E-3	4.8 E-3	3.0 E-4
12-25	sev DN 50	λ_{50}	3.1 E-5	-	-
		λ_E	1.4 E-4	-	-
		λ_{95}	6.0 E-4	-	-
25-80	sev DN 50 (2A)	λ_{50}	3.9 E-5	1.7 E-5	2.5 E-5
	sev DN 80 (1A)	λ_E	1.5 E-4	8.2 E-5	1.1 E-4
	sev DN 100 (1A)	λ_{95}	6.7 E-4	3.5 E-4	4.5 E-4
80-200	sev DN 80 (2A)	λ_{50}	2.3 E-5	-	-
	sev DN 150 (1A)	λ_E	8.8 E-5	-	-
		λ_{95}	3.8 E-4	-	-
200-400	sev DN 250	λ_{50}	<1 E-7	<1 E-7	<1 E-7
		λ_E	<1 E-7	<1 E-7	<1 E-7
		λ_{95}	<1 E-6	<1 E-6	<1 E-6
> 400	sev DN \geq 300	λ_{50}	<1 E-7	-	<1 E-7
		λ_E	<1 E-7	-	<1 E-7
		λ_{95}	<1 E-6	-	<1 E-6

sev... severance, DN...nominal value of diameters in mm
1A... leak from one side, 2A... leak from both sides

LEAKAGE FREQUENCIES INSIDE CONTAINM.(PWR)
Fig. 11

Leak Frequencies of Steam Generator Tubes (DRS-B)

Operating Experience

(SG's of KWU-Type, ~ 16.000 Tubes Incoloy 800)

- used for statistics: ~ 90 plant-years until 12/88, FRG only
- degradation phenomena observed:

wastage, mostly one sided	(864),	fretting	(157)
pitting	(2),	denting	(0)
stress corrosion cracking	(0-1)		
- 5 leaks through wastage weakened areas, all $A_L \ll 0.02A$
- wastage corrosion rate nearly stopped with
"All Volatile Treatment" (AVT) ($A \sim 3\text{cm}^2$)

Leakage Areas, Determination Method, Results

(λ = freq. / plant-year, λ_E = mean val., λ_{95} = 95% confidence limit)

leakage area	method	λ_E (λ_{95})
0 $< A_L \leq 0.02 A$	statistics of small leaks and assumption of several small leaks simultaneously through wastage weakened areas due to pressure transient (KWU exper.)	6 E-2 (2 E-1)
0.02 A $< A_L \leq 2 A$	zero failures statistics, no large leak occurred	6.5 E-3 (2.5 E-2)
2 A $< A_L \leq 4 A$	zero failures statistics, no breaks occurred, assumption: one break triggering an additional one	1 E-5 (1 E-4)

For leakage areas $> 4 A$ no meaningful scenario found
Flying plugs not included in working scheme at that time

Fig. 12

**CSNI WORKSHOP ON
SPECIAL ISSUES OF LEVEL-1 PSA**

Cologne, Germany

27th-29th May 1991

Evaluation of Low Power and Shutdown Events in German PWRs

by M.Simon

Gesellschaft fuer Reaktorsicherheit

1. Introduction

The safety of nuclear power plants during shutdown and low power operation is an area of concern in nuclear business today. Regulatory bodies and other responsible organizations all over the world show a high interest in the investigation of the shutdown risk after first preliminary results of U.S. and French studies. Decay heat removal must be ensured during any operation mode, but the requirements on the respective systems are often reduced in the shutdown modes. Some of the safety systems or their components may be inactivated for inspection and maintenance, automatic interlocks will be switched off. However, the time available after an event to perform manual recovery actions is comparatively long. Results from former PSA cannot be fully applied to shutdown mode because of the different status of significant safety systems during power operation and the time available for recovery actions.

The operation of PWRs with reduced inventory in the reactor coolant system (RCS) was perceived as a particularly sensitive condition by operating experience. Another area of concern is the unintentional criticality during shutdown. In PWRs unintentional criticality can occur as a consequence of boron dilution in the RCS.

The results of the French PSA back the need for a careful and detailed evaluation of plant safety during low power operation and shutdown. The core damage frequency during these operation modes contributes substantially to the overall core damage frequency in French PWRs.

Although operating modes like reduced inventory in the RCS or boration and dilution of the RCS are specific for PWRs, there are other areas which can affect both PWRs and BWRs, such as complete loss of AC power or loss of coolant during shutdown.

2. GRS - Study on Shutdown Risk

2.1 Scope of the Study

The results of the French PSA initiated a study for German PWRs (sponsored by BMU) which is performed by GRS. Our study shall investigate the applicability of the French findings on German PWRs. The reference plant for the study was Biblis, Unit

B, because this plant was also the reference plant for the German risk study. The study which is performed in co-operation with the utility is divided into two parts:

- In phase one a qualitative assessment of the applicability of results of the French PSA and of foreign events related to non-power operation should be performed. This phase of the study includes the investigation of existing measures (hardware, design, administrative) to prevent such events and to cope with them, respectively. The possible consequences of those events should be assessed. Finally, relevant sequences should be selected for an indepth analysis in phase two of the study. In addition the assessment should show whether there are event sequences, which require short term corrective actions.
- In phase two of the study, selected event sequences from phase one will be investigated more detailed using both PSA methods to assess the contribution to core damage frequency as well as thermal-hydraulic and neutron-kinetic codes to evaluate the consequences of such events. Phase two shall provide recommendations for possible improvements if necessary.

Phase one of the study was finished in April 1991. The following event sequences were investigated:

- loss of decay heat removal
- loss of coolant
- inadvertent dilution
- loss of vital AC power.

Following the qualitative assessment two of these events were evaluated in more detail: loss of decay heat removal and inadvertent dilution. These events will be discussed in this paper.

To assess the impact of these events on plant safety, the existing countermeasures have to be taken into account. These include the prevention of the initiating event and the ability to cope with the event if it has occurred (recovery actions). The countermeasures contain hardware measures like interlocks, instrumentation and control as well as administrative measures. The administrative measures include e.g. requirements on the availability of RHRS-trains in different plant operation modes and

procedures in the operating manual. Additionally, feasible accident management (AM) measures have been considered.

2.2 Loss of Decay Heat Removal During Mid-Loop Operation

As the coolant inventory in the RCS is rather small in mid-loop operation, a loss of decay heat removal may result in a fast increase in temperature up to boiling in the core depending on the time period since shutdown. Two sequences may result in a loss of shutdown cooling in this mode:

- loss of Residual Heat Removal (RHR) function because of air binding of the RHR pumps (figure 1)
- loss of RHR function because of component unavailability.

For these two scenarios the probability of a loss of decay heat removal during mid-loop operation was estimated for the reference plant. With respect to loss of RHR because of air binding the procedure for lowering the RCS level from full to mid-loop, the existing level monitoring, the automatic measures to prevent pump cavitation and the recovery actions after possible loss of RHR pumps were evaluated. **Figure 2** shows the mid-loop level monitoring of the reference plant. It consists of two level transmitters with different measuring ranges. The mid-loop level monitoring device is permanently installed, but it is not active during power operation. Before lowering the level in the RCS the level monitoring has to be taken into service by manual actions.

The provisions to prevent a loss of RHR at mid-loop operation because of air binding can be summarized as follows:

- redundant loop level instrumentation,
- exact procedure to take the loop level instrumentation into service and to verify its proper operation,
- exact procedure for level reduction in the RCS,
- automatic reduction of RHR pump flow before entering the reduced level operation,
- automatic isolation of letdown flow if loop level decreases below mid-loop,

- possibility for level restoration by one LPSI train if the two operating trains of the RHRS are lost.

Remark: In German PWRs the RHRS is a four train system which it is also used as a Low Pressure Safety Injection System (LPSIS). During mid-loop-operation at least two trains perform the decay heat removal. Additionally, by procedure one train must be in stand by for the injection mode.

A loss of all RHR trains during mid-loop operation because of component failures had also been taken into account. First probabilistic assessments indicate that the contribution of these two event sequences to the core damage frequency may be significant.

Therefore, event sequences in different plant modes during shutdown with the loss of decay heat removal will be investigated in detail in phase two of the study.

2.3 Inadvertant Boron Dilution

Within cold shutdown mode the subcriticality of the reactor core of a PWR cannot be achieved by control rods alone. The RCS must be borated. In the reference plant a boron concentration of $\geq 2\,200$ ppm is required for cold shutdown.

The injection of non-borated water into the RCS can result in an unintentional criticality of the reactor. The French PSA showed event sequences which could lead to a fast deboration in the core.

The worst scenario involves starting a reactor coolant pump (RCP) in a loop which contains an unmixed plug of non-borated water. This non-borated water enters the bottom of the reactor core and a rapid decrease of the boron concentration within the core happens. The event could result in a prompt criticality with high neutron flux and possible fuel element failure. A postulated sequence for such a scenario would be a loss of offsite power (LOP) during plant startup, continued dilution of the loop during LOP (figure 3) and finally restart of a RCP after power return (figure 4).

The consequences of unintentional deboration depend on the amount of demineralized water which had been released into the RCS and the intensity of mixing

of the plug of water on its way from the loop to the reactor core. In phase one of the study a variation of these parameters has been performed to determine the amount of water, which would make the reactor critical. Assuming low intensity of intermixture the investigation showed that the injection of even a quite small amount of water would result in prompt criticality.

The probability of a water slug scenario was estimated for the reference plant. Interlocks in the control system exist, which will stop dilution following a LOP, i.e. if none of the RCPs is running. However, no procedures were found for shift personnel guidance to stop dilution of the RCS in the startup mode after LOP.

For the reference plant it was found that the automatic supervision is of high quality, as it is redundant and each redundancy closes the valves in both trains of the boron and demineralized water make-up system (**Figures 5 and 6**). The failure rate of this supervision, which stops dilution when all RCP are switched off, was estimated and the resulting core damage frequency was assessed essentially lower than in the French PSA. Nevertheless, due to the potential severe consequences the scenarios of fast deboration will be investigated comprehensively during phase two of the study.

3. Conclusions

The preliminary findings of phase one of the study require no immediate corrective actions or immediate improvements for the reference plant, however, a priori the contribution of low power and shutdown operation to the overall risk is not negligible. Therefore, a broader review of initiating events and a systematic evaluation of resulting event sequences are necessary. During shutdown, requirements for the availability of safety systems are reduced and automatic actions to recover from shutdown events are either limited or even disabled. But, in this mode of operation more credit may be taken from manual actions than during power operations due to the time available.

A comprehensive investigation of all relevant sequences will be performed in phase two. This includes a classification of all relevant modes of operation and the investigation of significant initiating events as well as their potential consequences.

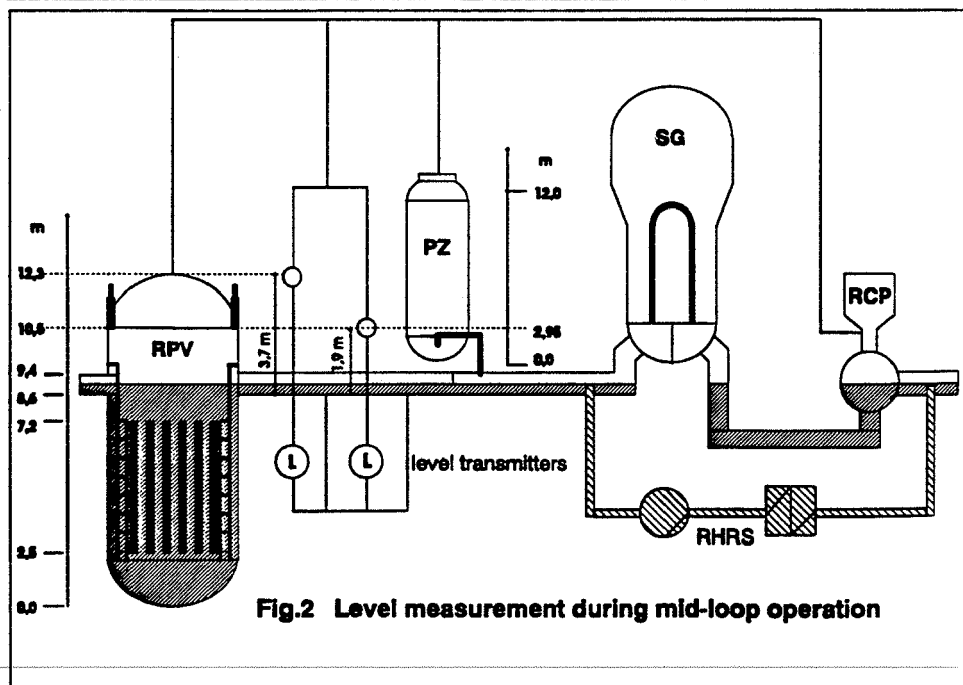
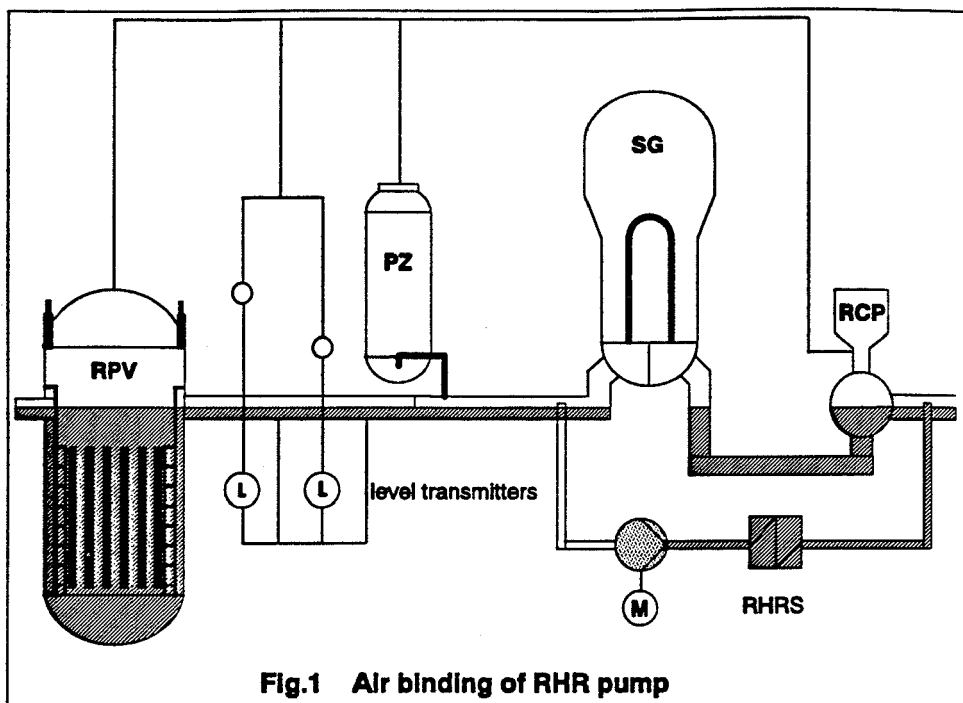
The evaluation of the operating experience is another important area of interest. German and foreign events will be analysed thoroughly.

The PSA methods can be used and should be used for the assessment if existing procedures and system requirements are sufficient or if additional improvements are necessary to assure a high safety level during shutdown operation. The assessment of risk must also include human performance. Its quantification will be a high challenge for PSA studies on this field.

Phase one indicated some possible areas of improvements, which depend on the design of the NPP. These areas include:

- Availability of at least one steam generator during hot shutdown and cold shutdown with the RCS closed, to provide decay heat removal after a loss of the RHRS. Even if the loss of RHRS happens during mid-loop operation with the RCS closed, the SG would allow a reflux-condenser cooling that is sufficient for decay heat removal according to first calculations.
- Additional water injection capacity from further sources to prevent boiling, when the RHRS has been lost and the RCS is already open. This coolant water has to be borated to avoid a dilution event.
- Prevention of boron dilution when the RCPs are not operating. This has to be assured by highly reliable automatic measures, which will not only close valves in the boron and demineralized water make-up system but also stop the make-up pumps to prevent a fast dilution by a water slug after restarting the RCPs.
- Additional guidance for the shift personnel to make sure that no inadvertent dilution has occurred before starting a RCP.

Finally, phase two of the study will qualitatively discuss the applicability of the results from the reference plant to other German NPP's. The risk of shutdown and low power operation of BWRs will be investigated within the PSA for a German reference BWR. This study has been started in 1988.



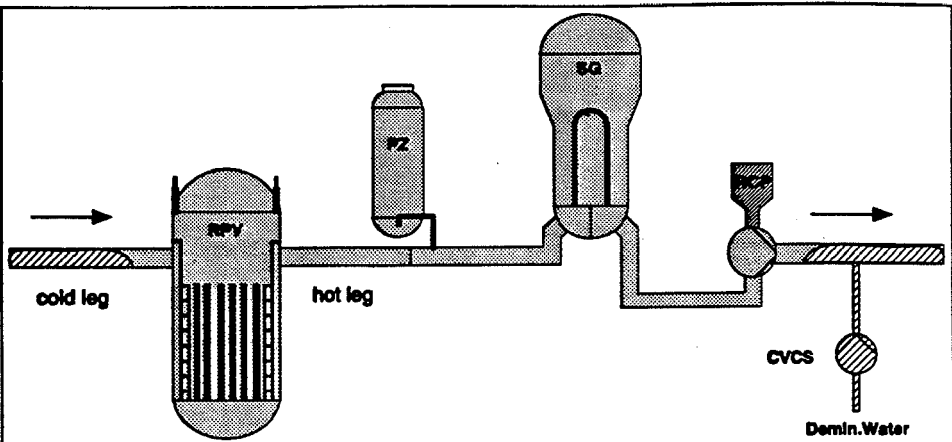


Fig.3 Water slug scenario (1)
All RCP stopped

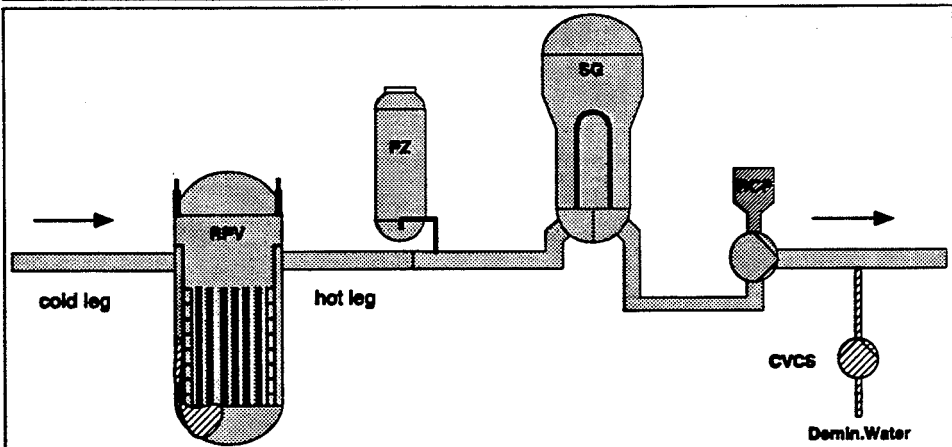
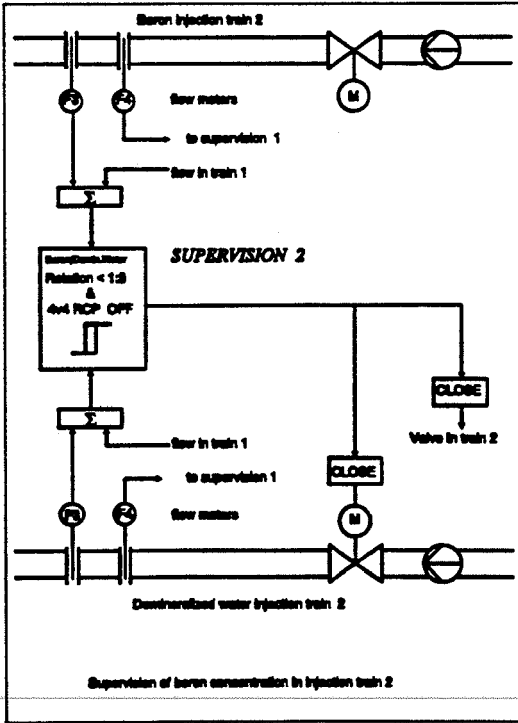
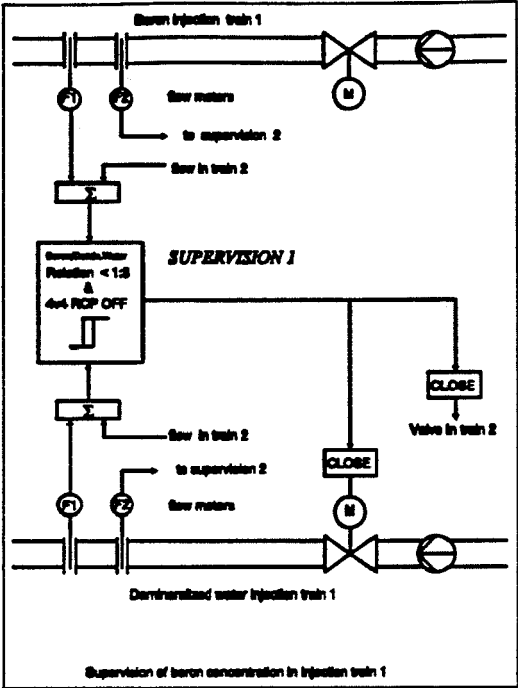


Fig.4 Water slug scenario (2)
Start of a RCP



CSNI WORKSHOP ON SPECIAL ISSUES OF LEVEL-1 PSA
27/29 MAY, 1981 - COLOGNE GERMANY

**LIVING PSS USED TO SUPPORT THE DEVELOPMENT OF A NEW
GENERATION OF BWR**

V. CAVICCHIA - E. TRAINI
ENEL - ITALY

L. MATTEOCCHI - A. VALERI
ENEA DISP - ITALY

INTRODUCTION

In 1988 the Italian Government established to postpone any decision on nuclear power use until 1993; in the meantime National Organizations concerned with Nuclear Power, are committed with the study of the new generation of reactors (whose safety is based on more intrinsic and passive safety features) to be proposed for a future resumption of nuclear power. Investigations are addressed to passive and simplified reactors with enhanced containment capability. Reference Criteria are still in discussion but the trend is toward very stringent requirements, in order to get Plants Licenseable with no need of a Preplanned Evacuation Emergency Plan. Plants presently under study are:

- . Simplified Boiling Water Reactor (SBWR) - General Electric
- . AP600 - Westinghouse
- . PIUS - ASEA Brown Boveri.

This paper describes the experience gained by some Italian Organizations with PSS living use in support of SBWR design development.

General Electric is currently developing the design of a new 600 MWE BWR, based on the use of simplified and passive systems and able to cope with severe accident situations without Operator Actions for 72 h.

The economic effort for the design development is supported by DOE and EPRI and the balance is supplied, in terms of manpower and testing of new equipments, by an international Team of Japanese, Italian and Dutch Organizations. In this frame two Italian contributors are involved in PSS activities: i) ENEL, the Italian Power Generating Board, is committed in the PSS implementation and ii) ENEA DISP, the Italian Regulatory Body, performs the PSS Peer Review. Phase 1 PSS has been completed and reviewed, while a Phase 2 PSS is currently under way. A basic requirement of the PSS methodology must be its ability to interact, in an almost real time, with the design while it progresses. To meet this requirement the model must be easily accessed and modified in order to follow the frequent design updates.

Living PSS approach was used, based on the practical ground on a fast interactive workstation. Software used for implementation and review was installed on PCs [1]. After the PSS Phase 1, done by ENEL [2], ENEA DISP peer-reviewed the study to assess the methodology adequacy [3]; the integration of these activities proved a good interaction with the design.

PROBABILISTIC SAFETY GOALS FOR PASSIVE SAFETY PLANTS

Qualitative Safety goals for a new passive BWR plant are based on the following concepts:

- a safety expressed in a way more understandable to the public
- a safety less dependent upon operator behaviour
- preventive and mitigative design such that a Preplanned Emergency Evacuation Plan is not necessary.

Quantitative Safety Goals definition to support Qualitative requirements are still not frozen; possible Goals could be:

- cumulative frequency of event sequences leading to a population dose exceeding the EPA PAG limit in short term (24 or 36 hr) lower than a small value
- core damage sequences with sudden catastrophic failure of the containment should be avoided by design or their occurrence should be negligible.
- Land contamination frequency must be negligible.

STUDY PHASE 1 IMPLEMENTATION

The Phase 1 PSS was conducted by ENEL at GE USA offices in the second half of 1989.

ENEL has a long standing experience in PRA implementation, see [4,5].

The SBWR PSS case has some peculiarities affecting the methodology:

- a) need to demonstrate low consequences with low frequency of occurrence
- b) presence of specific design features, with a lower dependency upon support systems
- c) data uncertainty for some new technology components
- d) need to demonstrate that the plant safety level is less dependent on Operator Actions than current plants.

This implies greater methodology effort than past generation PSS in the following areas:

- a) completeness of initiating event set, including i) peculiar initiators of the new design, ii) all Plant states, low power conditions included and iii) external events
- b) extensive Common Cause Failure treatment also among identical components in different systems
- c) systematic consideration of errors of Commission in Human Reliability and Risk Sensitivity calculations with no credit for Operator Actions
- d) evaluation of sequences without core melting, potentially leading to doses greater than the PAG limit, as in the cases of LOCA with a failure in the containment isolation.

In general terms the compliance with very low figures for Safety Goals imposes additional effort, because deeper analyses are necessary to discover low probability coupling events, which could be negligible if the CDF goal is $1E-4$ but not in the case of a smaller frequency Goal. As the SBWR

design is under development, the living PSS is articulated in successive phases. The Phase 1 was performed in the early design phase when only the conceptual design was available and without systematic dedicated supporting analyses in many areas (thermal-hydraulic analyses, external releases..).

One of the purposes of phase 1 was the identification of the thermal hydraulic analyses needed to support the final PSS. Success criteria were based on engineering judgement and extrapolation of a few preliminary analyses. The design details needed to perform the analyses but not yet included in the design documents were assumed by the design engineers. The software used for the study was based on a workstation [1] installed on PCs which allowed fast interaction for the current updating of the model.

Main study results showed the perspective to meet the safety goals with some design modifications and supporting analyses in specific areas identified by the PSS.

At the prevention level, the contributions of the internal events to the CDF was assessed very low except for the failure of the overpressure protection in ATWS.

For the mitigative aspects the containment effectiveness to prevent doses greater than EPA PAG limits could be enhanced if improvements were made on:

- i) long term cooling function failure
- ii) pressure suppression function bypass
- iii) ATWS (overpressure protection and failure to manually inject boron).

For the items listed above, the PSS suggested the following modifications able to satisfy the safety goals:

- a) increase the number of Safety Relief Valves (which work also in spring mode)

this makes negligible the contribution from overpressure failure in ATWS to the CDF

- b) dedicated components for short term and long term passive cooling functions - both functions were performed by the Isolation Condenser; this modification enhances the reliability of the long term containment cooling
- c) logic cards diversification; this makes negligible the containment isolation failure
- d) Boron Injection automatic actuation - this makes reactor shutdown function more reliable than past manual actuation
- e) automatic Feed Water Runback to limit reactor power in ATWS

b), c), d) and e) have the potential to make negligible the probability of a containment failure.

The PSS showed - with specific sensitivity calculations - also the potential fulfillment of the established Safety Goal without Operator Actions for 72 hr.

The above suggestions were recognized sound by the designer and were i) directly transferred in the design or ii) assumed as basis for systems modification.

Also a seismic level 1 PSS was performed. The result is that increasing the ability of the Isolation Condenser and of the Reactivity Control System to withstand high Peak Ground Accelerations in a seismic event and the using a realistic site specific Seismic Hazard Curve, the contribution of the Seismic event to CDF will be negligible.

STUDY PHASE 1 REVIEW

The Phase 1 PSS review was performed by ENEA DISP in 1990. ENEA DISP possesses experience in PRA review gained in past licensing activities.

The review objectives were to assess:

- the adequacy of the methodology
- the Study usability in the Regulatory Process (10CFR52) and to suggest design modifications
- give suggestions to the SBWR design.

For this review DISP worked on the original model - magnetic support - using the same workstation software; this can be considered sound because the computer code has been widely validated by DISP in past uses. In positive terms this approach gave the possibility to reach low level PSS items and also allowed many sensitivity requantifications. This fact gave effectiveness to the review because usually requantifications are outside the scopes of a Peer Review. No systematic Fault Tree independent requantifications were made.

Main review findings, comments and suggestions

Overall Comments

SBWR Phase 1 PSS can be considered a good piece of work as far as methodology is concerned.

In some areas the extent and the quality of the analyses can even be considered as an improvement of the present practice, specifically in its interactive and living usability.

As the Phase 1 PSS was conducted on the basis of some assumptions based on engineering judgement due to the lack of supporting analyses, some uncertainties are present in the quantitative results.

The quantitative effectiveness of the suggested design changes should be measured with more accuracy in the successive Phases of the study; nevertheless the proposed modifications can be considered sound on engineering and qualitative bases.

Detailed comments

Low level comments were addressed in the review; more significant ones are listed below:

- 1) The accident prevention is based on i) Power Conversion system, ii) Passive Safety grade systems, iii) Active non Safety grade systems and iv) Operator Actions (OA). To show Plant safety level adequacy without operator, the PSS contains a sensitivity to no reliance on OA for 72 hours. Systematic importance analyses were performed for individual non-safety system/components, such as diesel generators.

A sensitivity to no reliance at all on not safety grade systems should also be done in order to show how much safe is the Plant without the active systems operation.

- 2) Transients and LOOSP contribution to CDF is small if compared with the results of the past PRAs. In the PSS this low contribution is explained with i) the passive Isolation Condenser effectiveness, ii) the design requirement for low Transients Initiating Events Frequencies, iii) the Feed Water pumps equipped with electrical motors and iv) the low dependency on Support systems.

If their low contribution could be justified by the Isolation Condenser design, a very low value needs a more careful attention to discover potential couplings among redundant systems.

- 3) CDF is dominated by LOCAs Contribution (about 90%); this result is different from past PRAs where often Transients and LOOSP events dominate. The frequency of a transient event has less uncertainty than LOCA event because it is derived by more extensive operating experience. A sensitivity or uncertainty analysis could give more confidence on upper bound (95%) values.
- 4) Level 1 PSS part (Core Damage Model) appears more accurate than level 2 & 3 parts (Mitigations & Consequences) as the severe accident and radiological analyses were planned downstream of the phase 1; consequently the suggestions to the design given in PSS can be considered more valid when addressed on items affecting CDF or items regarding containment bypass due to system failure.

CONCLUDING REMARKS

The whole process of PSS implementation and review showed to be effective in producing a well balanced Study.

A more accurate assessment of the benefits coming from the suggested modifications - now incorporated in the design - will also be possible in the in progress Phase 2 of PSS, which is based on more detailed design information and on specific supporting analyses for Success Criteria, Severe Accidents and External Releases.

The authors like to stress the key role played by the living approach, allowing easy and fast model updating which is an important feature in general terms, but becomes essential when applied to a new design development where things are often changed.

The ability of living PSS to give an integrated picture of the plant will help to get more confidence on the Plants safety level.

The communications among PSS world and SBWR systems designers were effective with the help of the living study feature i.e. showing potential risk reductions obtainable upgrading specific design items.

Some software enhancements are possible: workstation are now powerful and accessible in cost terms; RISC based computers are faster in calculations and allows the management of large blocks of memory.

Living PSS based on powerful workstation will play an important role in the development of next generation NPPS with enhanced safety (preventive and mitigative).

REFERENCES

- [1] NUS-5218 NUPRA 1.2 Users Manual - The NUS Probabilistic Risk Assessment Workstation - November 1989 P.J.Fulford
- [2] GE Nuclear Energy NEDC-31790P - ENEL DSR/VDN C03.V106 Preliminary SBWR PSS - December 1989 (Proprietary Document)
- [3] ENEA/DISP SBWR 91-001 - Review of SBWR Phase 1 PSS
- [4] NEDE-30090 - Alto Lazio Station Reliability Analysis - December 1984
- [5] ENEL DCO 401.V040.VR 001 NUS 4954 - PSS Caorso NPP - June 1988

Summary of Discussions

Chairman: R. Virolainen

Summary of discussions

• Analysis of dependencies

There was general agreement that the treatment of functional and secondary dependencies poses no major problems. Common cause failures, however, are a concern. Data are so scarce that plant-specific common cause failure rates can hardly be expected to be obtained. For this reason all possibly available data sources, i.e. chiefly licensee events reports and reliability data acquisition projects must be made use of. A procedural framework for the interpretation of such information should be developed bearing in mind that it has to cater for the specific aspects of the different sources. Single failures considered on technical grounds to be potential common cause candidates should be included in the data base. Engineering judgement was considered an unavoidable element in the preparation of common cause data. Therefore the possibility of establishing a framework which would lead to a more consistent exercise of such judgement should be explored. Both activities aim at ensuring a maximum of clarity about the genesis of common cause data.

A controversial discussion referred to the subject of the use of Markov methods. Some advantages were claimed for its application. On the other hand, the vast number of equations resulting even for relatively small systems was considered a serious drawback.

• Time dependent phenomena/Uncertainties

- Time dependence

More attention should be paid in preparing PSAs to the possibility that there may be components whose failure rates are affected by "aging" or "learning". There is evidence that at least in some cases this effect may be noticeable. However, it must be kept in mind that the possible influence varies with the type of component and its

function inside the plant (e.g. operational or safety system) as well as the maintenance regime. Therefore a plant-specific evaluation is indispensable.

- Uncertainty

Qualitative uncertainty analysis, i.e. the identification of uncertain assumptions and parameters was considered an important task. Concerning the subsequent task, that of quantifying uncertainties, there was general agreement that the uncertainties affecting reliability data could be treated satisfactorily. However, considerable weaknesses in the handling of modelling uncertainties were recognized. An exploration of the potential of possibility theory for treating uncertainties was deemed desirable.

• Human Error

In general, in PSA only errors of omission are assessed and to some extent errors of commission. It is recognized that there is an urgent need for progress with respect to knowledge based actions. This is especially so because the contemplation of non-full power states and accident management measures requires more and more complex human interventions to be quantified. Another important case for the modelling of human interventions is the isolation LOCA. Despite quantification problems already the qualitative assessment of the conditions under which human interventions have to be performed has considerable merits in that it generally shows design and procedural weaknesses which can then be removed.

A very important aspect is the evaluation of operating experience and simulator experiments for obtaining human error probabilities. The problem of transferring simulator experience to real situations was believed to be solved to a large extent by using experience gathered in examination situations.

The lack of data may be compensated to a certain extent by varying the probabilities used for human error and assessing the impact on the PSA results. Expert judgement is believed to also give good results in this context. Human error is still considered one of the areas which requires research in order to arrive at more reliable

PSA results. In the meantime, doubts about the quality of human error assessment should be catered for by using larger error bounds on the data of Swain than those given by him.

• External Events

The presentations addressed the treatment of earthquakes and fires. It was generally felt that the methods for analysing external events are not so mature as those used in other areas of analysis involved in PSA contributions. Contributions from many different disciplines are required. Uncertainties of results are still substantial.

For analysing the plant response to seismic loads a lot of expert judgement is still needed. Conservative assumptions are usually made so that earthquakes larger than those assumed for the analysis are virtually impossible.

The view was held that the analyses should be limited to the loss of power induced by earthquakes as an initiating event; on the other hand, there was some concern that fires caused by earthquakes are generally not addressed.

The treatment of external events should be included in a PSA even if the analysis were to be only qualitative, since it directs attention to possible weaknesses of the plant. Due to the large uncertainties associated with the analysis of external events in Japan different safety goals for plant internal and plant external events are used.

• Special Topics

The session covered a variety of different topics, viz.:

- reliability data acquisition
- determination of the frequency of leaks and breaks in pipes
- low power and shut-down events

- living PSA

It was considered desirable to establish generalized criteria for the acquisition of reliability data including topics like e.g. the component definition. If these criteria were adopted internationally an intercomparison of data might become possible and there would be a better guarantee that generic data, which have to be used in some cases would really apply to the components under consideration. It was recommended to place more emphasis on the acquisition of data on human error.

However, it was generally recognized, that "grey areas" are unavoidable in the field of reliability data, whatever the effort invested in their acquisition.

The difficulties in generating reasonable reliability data for passive components were recognized.

Given the preliminary results of the French PSA on risk contributions from non-full power operation it was believed that this topic will be addressed in most future PSAs. The belief was expressed that the French results are perhaps overly pessimistic, a view which was somewhat supported by the preliminary investigation of the Biblis-B plant. It should be kept in mind, however, that results on non-full power operation are even more plant-specific than those for full power operation. The possibility of problems from an excessive number of alarms complicating operation actions in non-full power conditions was pointed out.

Gesellschaft für Reaktorsicherheit (GRS) mbH

Schwertnergasse 1
5000 Köln 1

Forschungsgelände
8046 Garching

ISBN 3 - 923875 - 36 - 3