Gesellschaft für
Reaktorsicherheit (GRS) mbH

Computer Code Package RALLY For the Probabilistic Safety Assessment of Large Technical Systems

W. Güldner, H. Polke,
H. Spindler und G. Zipf

GRS - 57

Gesellschaft für
Reaktorsicherheit (GRS) mbH

Computer Code Package RALLY For the Probabilistic Safety Assessment of Large Technical Systems

Wolfgang Güldner, Heinz Polke,
Heinz Spindler und Gerhard Zipf

GRS - 57 (April 1984)
ISBN 3-923875-05 -3

NOTE

This report has been prepared by GRS on behalf of the Federal Minister of the Interior. Its content is identical to that of the report GRS-44 (März 1982). The results contained in this report must not be in accordance with the opinion of the orderer.

PREFACE

In the scope of the project SR 122, A.1.1, the GRS has developed the computer code package RALLY (GE 81, GE 80) to compute reliability parameters of large and intermeshed engineering systems.

Since the most important of the individual codes belonging to this package are already documented in detail within GRS, in this report a summarized representation of the tasks and possibilities of the whole computer code package system is presented. In particular, the application of the individual codes to the probabilistic safety analysis of nuclear power plants is shown.

The report is divided into three parts. Following a survey of the individual programs of the RALLY-system, the applicability of RALLY will be discussed in the framework of

- scientific investigations;
- licensing procedures of nuclear installations;
- supervising nuclear installations and
- general administrative check-ups.

After a description of the possibilities given by RALLY, a final chapter will include the analyses, already performed with the aid of RALLY in the licensing procedure and risks studies.

ABSTRACT

This report describes the computer code package RALLY to compute the reliability parameters of large and intermeshed engineering systems. In addition to a short explanation of the different programs, the possible applications of the program package RALLY are demonstrated. Finally, the most important studies carried out so far on RALLY are discussed.

CONTENT

Page

FIGURES

1. INTRODUCTION

For the safety assessment of nuclear power plants and, nowadays, also for other large technical plants, reliability analyses are increasingly required, because of the frequently far-reaching consequences of an accident. By means of these analyses, comprehensive informations may be obtained on how a system failure occurs. The quantitative results of these analyses are for systems, which have to function on demand, the mean or average unavailability $M_s(t)$, and for operational systems the failure probability $Q_s(t)$ or the failure frequency $H_s(t)$. In addition to this purely quantitative assessment, the weak-point and sensitivity analysis is another task of reliability studies.

The statistical data from operational experience for different systems are inadequate to determine their reliability directly. But such data are available for components. Therefore, the reliability of the system can be determined using the relevant reliability data for the components, taking into account the logical combination of the components. To this purpose the systems must be subdivided so far, that the system behavior can be calculated from the failure mode data of subsystems or components, obtained by operational experience. This subdivision, however, leads to large and intermeshed system presentations, which may be described by fault-trees. A fault-tree is a graphical representation of the logic connections between the different components and subsystems related to a given, mostly undesired, initial condition, e. g. a failed system (see chapter 3.1).

The quantitative evaluation of fault-trees, a weak-point analysis and the calculation of the different reliability parameters for large systems are only possible by means of electronic data processing systems. For this purpose, the computer code package RALLY has been developed by the GRS.

2. DESCRIPTION OF THE INDIVIDUAL PROGRAMS BELONGING TO THE RALLY COMPUTER CODE PACKAGE

In addition to a short description of the whole RALLY-package, the different codes belonging to the package are discussed in the present chapter. The possible applications and algorithms are demonstrated. Figure 1 gives a perspective on RALLY and illustrates the data flow between the different programs.

The entire system requires only one data set that can be prepared easily. The informations for the different programs will be selected automatically and processed, i. e., the user need not interfere in the further run of the program.

The system is based on the data and fault-tree processing program TREBIL. In addition to the control of input data, the conversion of the fault-tree logic into a "Boolean equation system" as well as the preparation of data sets for the subsequent programs is the most essential task of TREBIL.

According to the methodological treatment of the reliability analysis, these subsequent programs may be classified in two groups.

- Direct simulation

Programs using the Monte-Carlo-Method simulate the failure mode of components (and consequently of the system) by means of random number generators. This way, very large and intermeshed systems may be analysed with a little mathematical effort. The subsequent failures, common-mode-failures, cold redundancies, functional tests and repairs can be considered relatively easily. The disadvantage of simulation programs is in the enormous increase of computer time for analysing very reliable systems, as the accuracy of results depends on the number of simulated failures. Using variance-reducing methods, in some cases even systems of high reliability can be calculated by simulation. Variance-reducing methods, however, require from the user an exact knowledge of the applied procedure.

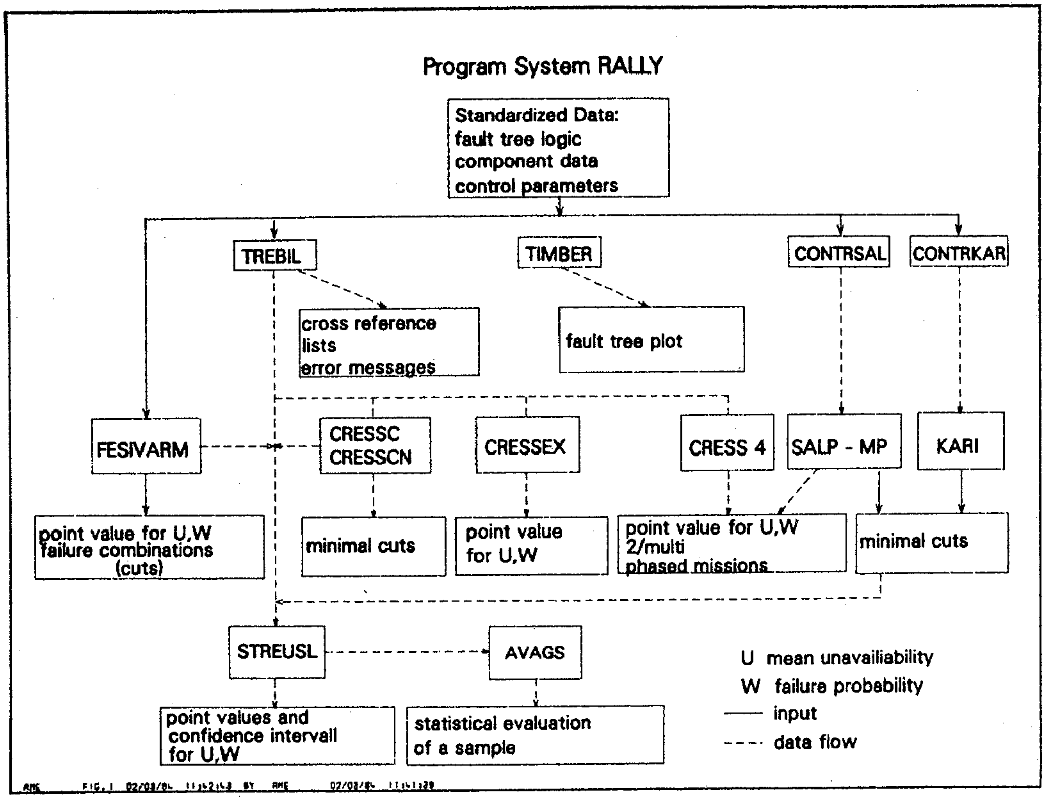

Fig. 1:
Schematic representation of the computer code package RALLY

- "Minimal cut"-approach

In addition to the Monte-Carlo-Simulation, the "minimal cut"-approach has proven to be useful in determining the reliability parameters of large intermeshed systems. In this context, the "minimal cut" is a minimal combination of components, the failure of which leads to the system failure. The "minimal cut" method is divided into 2 steps:

- the determination of minimal cut sets of a given system function (fault tree) and
- the subsequent computation of reliability parameters of the system by means of these cuts.

With $C_1, C_2, \ldots C_n$ being the minimal cut sets of a system function, the mean unavailability $M_s(t)$ of the system is

$$M_s(t) = \frac{1}{t} \int_0^t U_s(t')dt' \leqq \frac{1}{t} \int_0^t \sum_{i=1}^{n} U_{C_i}(t')dt'$$

$$\text{with } U_{C_i}(t) = \prod_{j \in C_i} U_j(t)$$

where $U_s(t)$ (i.e. $U_{C_i}(t)$; $U_j(t)$) is the unavailability of the system (i.e. of the minimal cut sets C_i; of the component j) at the time t. By means of minimal cut sets the failure frequency of the system may be computed too.

Unlike the Monte-Carlo-Simulation, in the minimal cuts method the system reliability value doesn't play any role towards the achievable accuracy of the results. The disadvantage of this method is that special test strategies, common-mode-failures or cold redundancies often may be included only in a simplified manner. In large systems, difficulties may arise when determining the most important minimal cut sets, as the number of minimal cut set in those systems often amounts to several millions. Normally, however, the first 1000-2000 minimal cut sets determine the result.

In the computer code package RALLY, the essential minimal cuts may be calculated as follows:

- simulatively - using the programs CRESSC and CRESSCN;
- analytically - by means of the programs SALP-MP and KARI decomposing the Boolean structure of the fault-tree.

In order to consider additionally the scattering of component data gained from the evaluation of operational experiences, the simulative-analytical program STREUSL has been developed.

The calculation for multiphase systems, each phase based on a proper fault-tree, is possible by using the programs CRESS4 and SALP-MP.

In the following, a detailed description of the programs will be given.

2.1 Fault-tree preparing program TREBIL

TREBIL requires as input the logic structure of the systems and quantitative informations (failure rates, test intervals etc.) on the components of these systems. By means of this information, check lists are prepared, which facilitate the verification of the fault-tree. In addition, the fault-tree is examined for logical correctness as far as possible and potential error messages are printed out. The most essential task of TREBIL, however, is fault-tree optimization as well as preparation of specific data for the other programs of the code package. Morevoer, the program converts the logic structure of the fault-tree into a Boolean subroutine for use in CRESSEX and CRESSC(N).

2.2 Fault-tree plotting program TIMBER

The plotting program TIMBER is used for documentation purposes and allows the user to visual examination (display) of the input fault-tree. The drawing of a fault-tree depends on the input sequence of the functional components and gates, because TIMBER does not optimize the logical structure of a fault-tree. The optimization was intentionally dispensed with, because in complex fault trees an examination of input data after the optimization of a fault-tree is rather difficult. By means of control parameters, either comments or reliability parameters for the components can be inserted into the comment boxes. Figure 2 shows a plot drawn with the program TIMBER.

2.3 Fault-tree computer program CRESSEX

The simulation program CRESSEX allows to calculate the failure probability and the mean unavailability for complex engineering systems. The program simulates for the specified system function the failure behaviour of the individual functional elements without using variance-reducing methods. The following can then be taken into consideration:

- various strategies for carrying out functional tests (e.g. a staggered schedule for the functional testing of redundant components);
- failure behaviour of the component functions, which are expressed by either a constant failure rate or a constant failure probability per demand;
- detection time of a component failure (self-anounciating failure, i.e. immediately recognized failure or a failure not recognized before the functional testing); and
- constant repair times of the components.

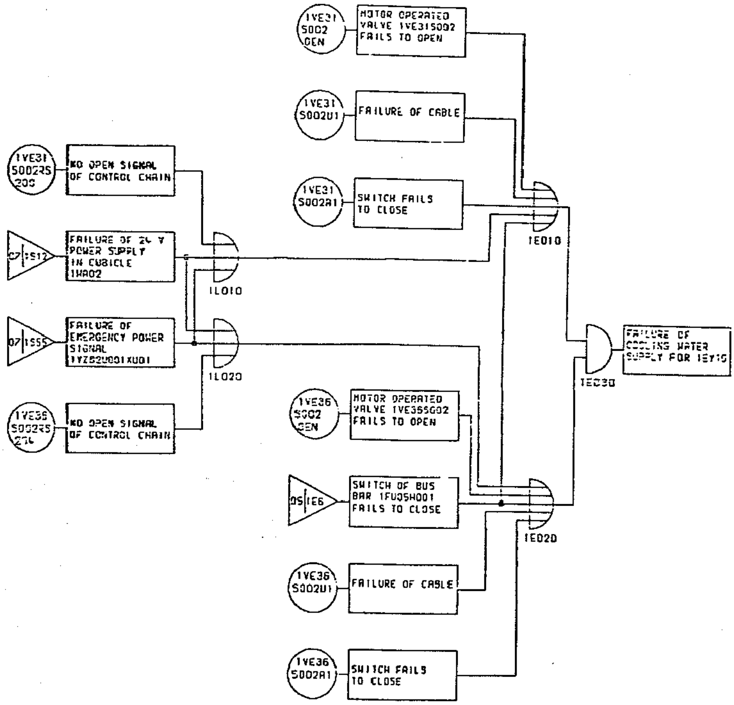
1VE31 S002 OEN
MOTOR OPERATED VALVE 1VE31S002 FAILS TO OPEN
1VE31 S002U1
FAILURE OF CABLE
1VE31 S002A1
SWITCH FAILS TO CLOSE
1E010
1VE31 S002RS 20S
NO OPEN SIGNAL OF CONTROL CHAIN
07 1S12
FAILURE OF 24 V POWER SUPPLY IN CUBICLE 1HA02
1L010
07 1S55
FAILURE OF EMERGENCY POWER SIGNAL 1YZ52U001XU01
1L020
1VE36 S002RS 27L
NO OPEN SIGNAL OF CONTROL CHAIN
FAILURE OF COOLING WATER SUPPLY FOR 1EY15
1E030
1VE36 S002 OEN
MOTOR OPERATED VALVE 1VE36S002 FAILS TO OPEN
05 1E6
SWITCH OF BUS BAR 1FU05H001 FAILS TO CLOSE
1E020
1VE36 S002U1
FAILURE OF CABLE
1VE36 S002A1
SWITCH FAILS TO CLOSE

Fig. 2:
Plot of a fault-tree using the program TIMBER

The simulation process is repeated very often. The intermediate results, being dependent on chance in the trials, as for instance

- the occurrence of a system failure,
- the duration of failure of the system function and
- the components involved in the failure,

are stored and evaluated statistically at the end of the calculation. The estimated values of the failure probability $Q_s(t)$, of the failure frequency $H_s(t)$ and of the mean unavailability $M_s(t)$ as well as the associated variances (variance as a function of the number of trials or simulated dead times) are calculated as follows:

$$H_s(t) = \frac{\text{number of system failures in } (0,t)}{\text{number of trials}}$$

$$Q_s(t) = \frac{\text{number of first failures of systems in } (0,t)}{\text{number of trials}}$$

$$M_s(t) = \frac{\text{sum of system failure durations}}{\text{number of trials} \cdot t}$$

t = consideration period

Additionally, in CRESSEX the components are arranged according to the number of failures and their contribution to the mean unavailability. Furthermore, the minimal cut sets occurring in the simulation are indicated. This information can then be used to perform the weak-point analysis.

At the same time, reliability parameters may be calculated for selected subsystems in order to be able to estimate their contribution to the system reliability.

2.4 Fault-tree computer program FESIVARM

The program FESIVARM determines the failure probability and the average unavailability in a simulative way by means of "importance sampling". By introducing a priority factor the number of failures may be increased, thus leading to a reduced computing time, while maintaining the required accuracy. Thus, in most cases, even very reliable systems can be treated in a simulative manner. In addition, the program enables to provide a weak-point and sensitivity table on the basis of the failure combinations of the system. The further properties resemble those of the CRESSEX program.

Due to a different treatment of the logical structures of the fault-tree, the possibilities of gate-connections, however, are extended. So, emergency and standby gates with cold or hot standby components and non-perfect switch may be treated.

2.5 Program for a simulative determination of minimal cut sets -CRESSC, CRESSCN

- Program CRESSC

The CRESSC program determines in a simulative way the most important minimal cuts of a system for the program STREUSL.

Similar to CRESSEX, the failures of the system function are simulated in accordance with the failure behaviour of the functional elements. Since the task of the program is only the determination of the most important minimal cut sets (and not the calculation of reliability parameters), calculation of the failure time, the failure duration, etc. can be dispensed with, which leads to a substantial reduction of the computing time as compared with CRESSEX. In order to obtain sufficient system failures when performing the simulation, the period considered in the program is controlled in such a way that in about every other trial a system failure occurs. The evaluation of the minimal cut sets will be done by integration in the program STREUSL.

- Program CRESSCN

The CRESSCN program is used to determine minimal cut sets of system functions containing NOT-gates. The algorithm correspsonds to CRESSC, only the minimum cut sets containing incompatible events have to be eliminated.

2.6 Program for the analytical determination of minimal cut sets - SALP-MP

The analytical program SALP-MP (As et al. 80) has been developed by JRC ISPRA. In this program, all those minimal cut sets are determined, whose contribution to the unavailability is higher than a specific limit. The applied procedure, in addition, allows failure estimates concerning the minimal cut sets which are not considered. Thus, the inclusion of the complete set of minimal cuts is only a question of computing time.

The program calculates the reliability parameters for the considered period and for interim periods of interest. The results are arranged in the order of their contributions to the unavailability.

Furthermore, the program SALP-MP may be used for the treatment of multi-phase systems. These are systems, the configuration (in this case: fault-trees) of which vary during the scheduled successions in time. Here, the failure probability is of primary interest. However, as in the single-phase case, also the unavailability will be calculated for all of the specified times and will be output for all phases.

The application of SALP-MP requires to use first the program CONTRSAL. Its most essential function is to produce, on the basis of a special TREBIL output, a data structure that is compatible with SALP-MP.

2.7 Program for the analytical determination of minimal cut sets - KARI

Analogue to SALP-MP, in the program KARI (Ca, Ri 75) all those minimal cuts will be determined, the contributions of which to the unavailability (or failure frequency) is higher than a specified limit ε. As in the program SALP-MP, an error which results from disregarding any minimal cuts can be conservatively estimated. Both, the KARI and the SALP-MP-program, differ essentially in the way of treating the fault-tree to determine the minimal cuts. The algorithm implemented in KARI, is described in (Ca, Ri 75).

2.8 Program CRESS4 (Two-phase computer program)

The two-phase program CRESS4 calculates the failure probability of a system, the function of which, when demanded (standby-phase), must be maintained over a specified period of time (long-range phase). Both phases my be described by different fault-trees (e.g. varied efficiency conditions) and by different failure data (e.g. failure to start-up on demand and failure to operate in the functional phase. If the same components are functional in both, the standby and the long range phase, the simulation failures of these components in the first phase (determination of the unavailability of the system) will be taken over into the second phase.

2.9 Uncertainty program STREUSL

The programs considered up to now only calculate point values of the reliability parameters, i.e., statistical uncertainties or variances in the input data are not taken into account. However, when determining representative failure rates or failure probabilities per demand, uncertainties may occur, which can be described by means of distribution functions (mostly log-normal distributions).

The program STREUSL calculates the expected values, distributions, and the confidence intervals for the unavailability or the failure probability of the system function, considered as a function of the distribution of the input parameters (failure rates or failure probabilities per demand). In doing so, the following distributions can be treated in STREUSL: normal and log-normal distribution, uniform and log-uniform distribution, Beta- and χ^2-distribution.

The calculation of the mean unavailability or the failure frequency of the system as a function of the distributions for the input data is performed in the program STREUSL in a simulative and in an analytical part. In the simulative part, because of the parameter distributions, a combination of values for the failure rates or the failure probabilities per demand of the functional elements will be calculated. By means of this combination, the mean unavailability or the failure frequency of the investigated system function is then calculated in an analytical way. The basis for the analytical calculation is the minimal cut sets.

This procedure - the simulation of random numbers and the calculation of reliability parameters, the so-called "trial" - is repeated very often. This way, STREUSL yields a random sample of mean unavailabilities or failure frequencies (the size of the sample should be ≧ 200). The mean unavailabilities or failure frequencies obtained will then be evaluated in the last section of the program by means of various statistical methods, namely:

- calculation of the median, espected value and variance of the distribution, and determination of the density function,
- evaluation by mean of "order statistics" (confidence intervals for specified fractiles) and
- evaluation by means of approximation distribution functions (AVAGS).

For the investigation of common mode failures, STREUSL offers the possibility of failure-rate coupling. For those redundant component functions to be coupled in the failure behaviour, only one random number per trial is simulated for the failure rate or the failure probabilitiy per demand.

2.10 Program AVAGS for the approximation of a given random sample by different distributions

The program AVAGS allows the approximation of a given random sample by means of different distributions (normal, lognormal, Johnson-SL-, Beta-, χ^2-, Weibull-, Extrem-1-, Gamma- and exponential distribution). In addition, the factors (expected value, variance slope, excess) and the histogram of the random sample will be computed. AVAGS has been developed for the variance range program STREUSL in order to evaluate the random sample of mean unavailabilites or failure frequencies (Fig. 3).

Furthermore, AVAGS offers the possibility to evaluate statistically the components data taken from the literature or operational experience. These results can then be used as input data for the other programs of RALLY.

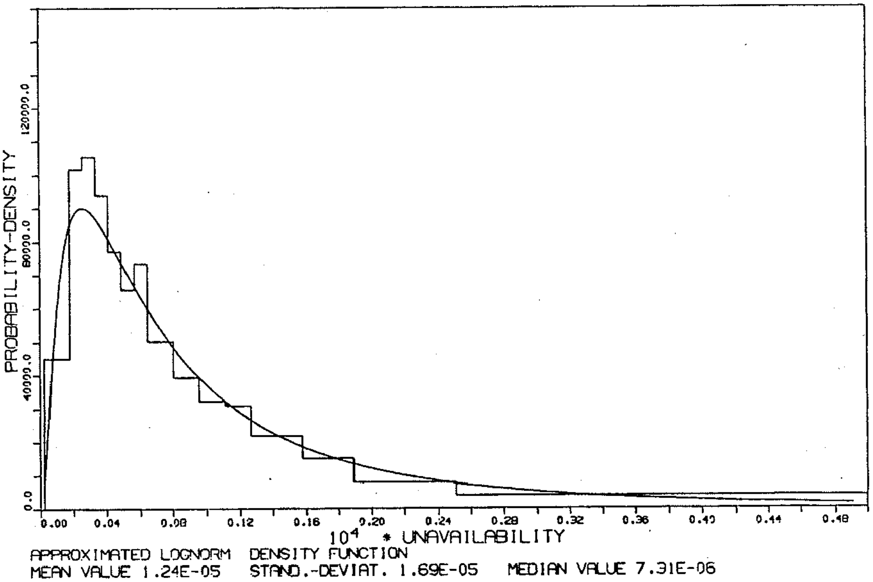

Fig. 3:

Plot of the best approximation of a random sample, generated by the program AVAGS

3. PURPOSE AND APPLICABILITIES OF THE COMPUTER CODE PACKAGE RALLY

After having introduced the individual computer codes of the package RALLY, the purpose and applicabilities of the program system shall be discussed in detail now in this chapter. As RALLY primarily has been developed for the calculation of fault tree and event tree analyses, the following section explores these topics first.

3.1 Event-tree and fault-tree analysis

In the event-tree analysis the various potential consequences of a defined initiating event (e.g. rupture of a main coolant line) is determined by the success or the failure of needed countermeasures (system functions). Depending on the extent of the required countermeasures a varying number of possible event sequences result, which are compiled in the so-called event-tree diagrams.

As an initiating event, a leak in the main coolant line is assumed in figure 4. This event leads to a reactor scram, triggered by the reactor protection system. Depending on the success or failure of this safety measure, two different event sequences result. In the further course of the accident, the ECC (emergency core cooling) and RHR (residual heat removal) systems automatically go into action, so that additional branching points result. Hence, in the above example eight different event trees have to be studied.

After preparation of the event-tree diagrams, quantitative evaluation will be performed by determining the occurrence frequency of the initiating events and the failure probability of the required system functions by means of RALLY. In doing so, possible interdependencies between the different systems have to be taken into consideration.

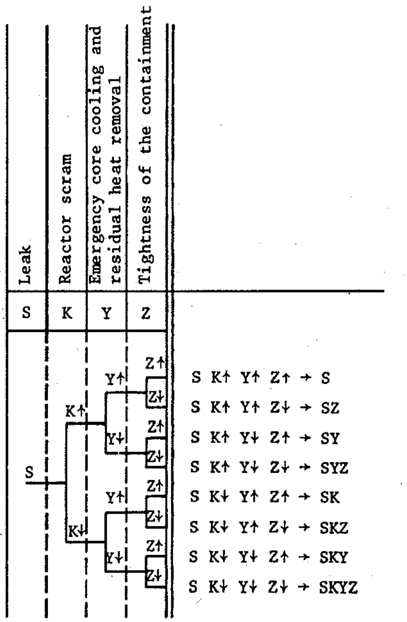

Fig. 4:

Simplified event-tree for a loss-of-coolant accident

To resolve the explained event-trees up to the components level, in most cases, the fault-tree is used. The starting point in this method is the definition of the (mostly undesired) system condition to be analyzed (e.g. failure of the emergency core cooling and the residual heat removal). Proceeding from this "TOP-event", systematically all combinations of events are sought that lead to the undesired event (see figure 2). The event combinations are described by the way of graphical representation, the fault-tree, in which linkage of the events takes place by means of the logic operators AND, OR and NOT.

As already mentioned, interdependencies between the initiating event and/ or the various systems that cope with the accident must be taken into consideration, when coupling the event-tree and the fault-tree method. Only in the case of statistically independent systems, the occurrence frequency of an event-tree path can be determined simply by multiplication of the corresponding probabilities. In dependent systems, the entire event-tree path - often including the initiating event - has to be calculated in the failure. This means, that, e.g. in figure 4, in case of interdependencies not only the events S, K, Y and Z can be separately calculated but also for each event-tree path an individual fault-tree must be drawn up.

3.2 Risk and reliability analyses

In a risk analysis, the frequencies are derived from the event trees. Starting from an initiating event, the functioning or the failure of the required safety relevant systems are taken into consideration. For this purpose, the occurrence frequencies of the initiating event and the failure probabilities of the systems required to cope with the accident must be determined. For the determination of the failure probabilities, reliability analyses are required, because operating experiences usually are not sufficient for a direct evaluation of the system reliability. Reliability analyses are therefore a basic prerequisite for the performance of risk analyses.

Reliability analyses are primarily aimed at evaluating quantitatively the quality of a technical system. The reliability of the system is determined using the corresponding reliability data of the components, whereby the combination of components are given due consideration. Normally, the components have different functions, e.g. the switching in or out of a diesel generator. It therefore has to be determined, which failure of the component function contributes to the failure of the system. For this reason, instead of a component failure, frequently, the failure of a function (or failure of a function element) is spoken of. The same applies to the use of the term "Function" in connection with the systems. Both, the composition of a system and its mode of operation have to be considered in the reliability analyses. Thus, for example, the emergency power generating systems will only be switched on when required; whereas, particular cooling water supplies are continuously in operation.

To describe the above mentioned quality of a technical system, the mean unavailability $M_s(t)$ will be used for systems, which have to function on demand. The corresponding descriptors for the quality of operational systems are the failure frequency $H_s(t)$ or the failure probability $Q_s(t)$. If the moment of demand is distributed evenly within the interval $[0,t]$, then the mean unavailability is equal to the probability that the system fails on demand. While the failure frequency indicates the expected number of failures within the interval $[0,t]$ and occassionally may be > 1, the failure probability $Q_s(t)$ is equal to the probability that the system fails at least once within the interval $[0,t]$, that means $Q_s(t) \leqq 1$.

Point values for this reliability parameters can be determined simulatively by the programs CRESSEX or FESIVARM or, analytically, by the program STREUSL. By using the program FESIVARM, because of the possibility of "importance sampling", even highly reliable systems can be calculated simulatively. If the distribution of $M_s(t)$ or $H_s(t)$ as a function of the distribution of the input data (failure rates, failure probability per demand) is of interest, the program STREUSL can then be applied.

In addition to this purely quantitative calculation, the weak-point analysis is another important task of reliability analyses. Hence, on the basis of the programs CRESSEX and FESIVARM, those components can be identified which contribute largely to the mean unavailability or failure frequency and therefore are the most important risk contributors. The minimal cut sets (critical quantities) derived by the programs CRESSC, CRESSCN, SALP-MP or KARI also offer a good possibility to perform weak-point analyses. When arranging the minimal cut sets according to their contribution to the mean unavailability or the failure frequency of the system, the most important critical sets (weak-points) can be identified. By a modification of the system or by the improvement of the component of such an essential critical set, the system often can be significantly improved (for the treatment of common-mode-failures, failure rate coupling, see chapter 3.10).

3.3 Licensing procedure

The Safety Criteria for Nuclear Power Plants (Federal Ministry of the Interior), the Guidelines for Pressurized Water Reactors (Reactor Safety Commission) and the instructions given by the Nuclear Steering Committee of the Technical Inspection Agencies require for the licensing procedure of certain systems the performance of reliability analyses (see chapter 4.2). First of all, the harmony of the systems has to be proved, i.e. predominant weak-points should be identified and eliminated.

A significant facility to identify such weak-points is provided by the program system RALLY. Fault trees, for example, may be plotted very clearly using the program TIMBER (see figure 2). Drawings like this, very often enable an early recognition of critical paths, which lead to the TOP (undesired event). In addition to the visual control of the system, a weak-point analysis can be performed for the system with the aid of the programs already mentioned in the above chapter. On the basis of the results obtained by using these programs, shut-down and test strategies of components and systems can be determined (see chapter 3.4).

3.4 Comparison of systems

The design structure of a system, in most cases, can be chosen from several possibilities. For example, a redundant system is assembled either in lines that are independent from each other, or else the individual lines are intermeshed in order to increase the reliability of the system. For a comparison of such different design possibilities the RALLY code package can be used. RALLY renders the possibility to evaluate and to compare reliability parameters of different designs. In doing so, also weak-points can be revealed. The problems arising between intermeshed and demeshed systems, particularly in large systems, can hardly be recognized without the aid of electronic data-processing programs.

RALLY is just as well suited to evaluate the effects, different test strategies may have on the failure probability or the mean unavailability. The results may then be taken into consideration when deciding (e. g. for standby-systems) in which time intervals certain components should be tested or which functional failures can be designed as potentially self-anounciating.

3.5 Computation of importance parameters

The reliability features of a system are generally influenced by the components to various extents.

Because of their particular arrangement within a given system, some components are more important than others with respect to how well they function. Thus, in general, a component connected in series with the remaining system is more important than if it would be connected in parallel with the remaining parts of the system.

Another essential factor, which determines the importance of components, is their reliability. The question on the importance of a component can be formulated in very different ways depending on the problem of interest.

- How does the reliability feature of the system vary with a certain change in a relevant component feature? The answer to this question leads to the identification of those components, the reliability improvement of which has its most intensive effect on systems (optimization of systems, identification of weak-points).
- The failure of a system always coincides with the failure of a system component. The probability, that a component causes the system failure in the above sense, may therefore be used for the component as a further determining feature.
- Significant for the failure detection and diagnosis is the order in which the components of the system will be tested. Particularly with respect to a minimization of the repair time, it is important, after a system

failure, to begin the repairs with that component the reparation of which restores the function of the system with the highest degree of probability.

Besides this system-dependent evaluation of the components, a system-independent evaluation of the components may often be advantageous. Thus, for example, the failure frequency provides interesting informations on the number of repairs to be performed and on the necessary provision of spare components.

The above mentioned questions may partially be answered by means of the computer code package RALLY. So, in the programs CRESSEX and FESIVARM, components will be arranged and printed out according to the number of failures and dead times respectively the failure probability and the unavailability. For components being involved in the failure of the system, the program SALP-MP computes how much these components contribute to the unavailability of the TOP. By means of these determinants from the variation in the components unavailability, the extent of variation in the system unavailability may easily be evaluated. More differentiated importance parameters require a further development of some programs in the RALLY package.

3.6 Combination of distribution functions

In practice, often the problem arises, how to evaluate the distribution of a function Y of random data $Y = f\ (X_1, X_2,...,X_n)$. In many cases, the distribution function F(y) of Y can hardly be calculated in an analytical way; therefore, one has to rely on simulative methods.

To determine the distribution F(y), the program STREUSL may be used. In parts the algorithm has already been described in chapter 2.8. Based on the distributions of X_i, i=1,...,n and with the aid of random number generators, values x_i^k for X_i are computed. With this combination of values, the Function $y_k = f(x_1^k, x_2^k,...,x_n^k)$ will then be calculated. This process - the computing of random numbers and the calculation of $f(x_1^k, x_2^k,...,x_n^k)$, - will then be repeated as much as possible. This way a random sample $y_1, y_2,...,y_n$ of Y will be obtained, which may be statistically evaluated by means of the program AVAGS (see chapter 2.9).

3.7 Accident simulator

It is the task of a(n) (accident) simulator to illustrate appropriately on a computer structure the interaction between the physical processes and the function or failure of the components. The realization of such a concept depends significantly on the definition of the extent of simulation.

This definition will be specified gradually, proceeding with determining the classes of incidents and accidents intended to be simulated; system functions and systems which are relevant in this context up to subsystems, components and operator interventions, which contribute to the development and the control of the incident or accident. To this purpose, a systematic method is provided by reliability analyses using the fault-tree method. Since the fault-trees, e. g. in the German Risk Study, are resolved down to the component level, can, by means of the results achieved by the computer code package RALLY, be classified down to the components, subsystems or systems corresponding to their importance for the control of accidents.

By combination of these informations with the general simulation requirements for normal operation and for accidents, the extent of conditions to be simulated may then be clearly defined.

3.8 Supervision of nuclear installations

When fulfilling their control functions during the operation of a nuclear power plant, the supervisory authority may require additional assessments, as a consequence of operational experiences or in view of new developments in the reactor safety technology. Such an assessment may lead to modifications of system functions or of operating instructions; the degree of the modification/ improvement has to be verified quantitatively.

The computer code package RALLY is suited for re-analyses when modifying regulations and rules, the subsystems of a plant or its mode of operation (e. g. a modified test- or repair strategy). RALLY may be used additionally for re-analyses of upset conditions or emergency conditions occurring during the operation of a plant. Furthermore it may compare systems in the framework of "backfitting" measures.

3.9 Coupling of RALLY and data bank

Informations on variances and parameters in reliability analyses are of special importance for the safety of nuclear power plants. In licensing procedures, the choice of appropriate evaluation data (mean, expected value) gives rise to vivid discussions at present. By providing the distribution function of the reliability data, a higher degree of informations may be achieved.

For such cases, the program STREUSL has been developed, which furnishes a random sample of the reliability parameters taking into consideration the distributions of the basic data. The various distribution functions may be adapted to the random sample or to its data (median, uncertainty factor, expected value, variance, slope, excess etc.) by means of the program AVAGS.

AVAGS can additionally be used to determine distributions for failure rates and failure probabilities per demand on the basis of data taken from literature. Furthermore, component data gained by operational experiences may statistically be evaluated with the aid of this program.

The coupling of computer code package RALLY or part of it with a data bank, in which the plants and failure data of nuclear power plants are stored, enables an easy access to latest scientific findings concerning the operational experiences.

The connection of the fault-tree method with a data base may also be a valuable tool in the scientific-technical field. So, a weak-point detected during operation (e. g. unsuitable material, constructional error) may systematically be checked in order to find out what other components of the same type or material could be affected by the same failure mechanism. In addition, it would be possible to determine components which are of special importance for the safety and functioning of a system. In the case of a failure, it may be asked too, which additional failure combinations are to be expected and what is the probability for the occurrence of a particular undesired event.

3.10 Consideration of common-mode-failures and human error

Of special interest are the common-mode-failures (CMF), as they are responsible for the lower limit of system reliability data: After all, every system is expected to show mutually dependent functional failures, either as a consequence of a single functional failure or due to a common cause in redundant components. Special attention should be given to events occurring simultaneously or within a very short time interval, so that the failed conditions because of the limited detection time exist concurrently.

Those interdependencies - even with regard to the extent of dependency - will be modelled ("failure coupling") and can then be treated in the fault-tree as an independent component. Thus, the treatment of common-mode-failures in RALLY is not submitted to any further restriction.

Common influences during the design and manufacturing of comparable components, but also during operational tests, maintenance or repairs may not necessarily lead to higher failure rate values. An outstanding quality assurance program or strict maintenance requirements, for example, may even contribute to a decrease of these values. In any case, the common influences cause a certain interdependence between the failure rates or the failure probabilities per demand when comparable components are used.

The kind of dependency may be treated in reliability studies by coupling the failure rates or the failure probabilities per demand. This method is used in variance range calculations and does not lead to simultaneous, but rather to staggered failures. The failure rate values of such comparable components will not be calculated independently from each other in the computer program STREUSL, but will be varied commonly. Thus, this failure rate coupling uses in each simulation trial only one value of the failure rates for the functional failures of all comparable components.

Additionally the program package assesses the influence of human errors. Errors committed during maintenance or adjustment, or when performing inspections or during actions specified in the instruction manual, may be introduced into the fault-tree. They then will be treated like every other component function. However, when interpreting the results of such reliability analyses, it should be taken into consideration that the pertinent basic data only are rough estimates, because it is very difficult to quantify the failure probabilities due to human errors. When evaluating the human reliability, furthermore, it must be taken into account, that the interdependence of human actions is an importance influencing factor. This again can only be done by introduction of an appropriate model into the fault-tree. The treatment in the computer code package RALLY will then be the same as it is in the case of common-mode-failures.

Although in most cases only rough evaluation can be achieved (because of the existing uncertainties in the basic data), human actions may be considered in order to determine their influence on the development and control of accidents as well as to recognize possible overstrain of the personnel. After the occurrence of an incident it may be investigated, at which point the operator intervention had been necessary and to what degree the actual behavior of the operator corresponds to that required theoretically. So, if necessary, the relevant written instructions be corrected systematically.

4. REALIZED APPLICATIONS OF THE RALLY PROGRAM PACKAGE

After having discussed the possibilities given by RALLY, the analyses already performed with the aid of this program system will be described in the following chapter.

4.1 Application of RALLY in risk studies

A main field for the use of the computer code package RALLY was the German Risk Study of Nuclear Power Plants (GE 79). One of the essential tasks was the quantification of event trees for the accidents "large leak", "medium leak", "small leak", "loss of emergency power" (ATWS) and "pressurizer leak during ATWS". By standardizing the data sets for all computer codes in the program package RALLY, it has been possible to computer in a single run per program the unavailability of the demanded system functions with a given initial event. For these cases it could be shown, that the applied simulative programs - unlike analytical programs - could treat these very large and complex systems within a reasonable computing time.

Another problem to be solved was the calculation of variance ranges for the conditional accident probabilities, because of the uncertainties in the input data. In doing so, the minimal cuts had to be determined using the program CRESSC. By means of these minimal cuts and the distribution of the component failure rates, the uncertainty in the total result has then to be calculated with the program STREUSL, while doing so, the correspondence of the expected values from STREUSL and CRESSEX has to be verified as a check.

In order to take into account the dependency of failures of comparable components in the same system, but of different redundancy, a computer run with the program STREUSL has been performed applying the so-called "coupling of failure rates". By means of this method the following items may be treated: dependencies due to common manufacturing, corrosion failures, certain maintenance errors and failures as a consequence of difficult environmental conditions. As an example for the run with "failure rates coupling", the event-tree loss of emergency power has been chosen, in which comparable hardware failures, as for instance, starting failure of a pump, starting failure of the emergency diesel set, or opening failure of motor driven valves, have been combined in coupling groups.

The computer run revealed, that the expected value and the variance range of the original results did not significantly increase. Viewing through the minimal cuts, it was ascertained, that combinations of comparable component failures do not determine the result. But rather the influence of the common-mode-failure of emergency diesel sets and of human error (during start-up of the emergency system) was dominating.

Another step in the Risk Study was the coupling of the system fault-trees with the fault-trees for the failure of containment integrity, in order to determine the various categories of radioactive releases and to evaluate them quantitatively. With the program package RALLY the frequencies of release after a core melt have been calculated for the categories β_1 (large leak, e. g. by a failure of the ventilation valve or the containment weldings), β_2 (medium leak, e. g. by failing the isolation of the building drains), β_3 (small leak, e. g. by failing the active isolation of measurement lines in the ventilation system) and η (failure of the annulus exhaust air handling system). These results are the basis for the following dispersion calculations and evaluations of accident consequences.

Besides the determination of the collective and individual risks arising from possible accidents in nuclear power plants, the determination of weak-points and the elaboration of proposals for improvements of the system have been an important "product" of the German Risk Study, in which the computer code package RALLY was employed mainly. So, the results of calculations revealed, that in case of a medium leak in a main coolant pipeline the unavailability of the urgently needed high pressure injection system is determined 33 % by the failure of the 3-way-valve in the bursten loop. Another example may be the loss of emergency power (ATWS), in which the common-mode-failure of the emergency diesel generator contributes 80 % to the unavailability of the system function "emergency feedwater supply and main-steam discharge". As a consequence, already in August 1978 a grid re-switch mechanism has been installed in the reference plant Biblis B. This system improvement reduces the frequency of a core-melt down due to loss of emergency power by 10^{-5}/y. As a whole, a series of system improvements resulted, for instance, resistance of measuring converters for the automatic feedwater control against the largest assumed accident, as well as the partial automation of the shutdown process (100 °C/h) in the case of a "small leak". Both improvements have been performed already in the reference plant.

In the risk oriented HTR-study (KE, GE 81) the contribution of GRS concerning the reliability analysis by means of RALLY is restricted to the evaluation of the event sequences "ATWS". The quantification of the event sequences - related to a 1160-MW-temperature reactor - has been done analogous to that in the PWR-study, i.e. the safety and support systems required following an ATWS have been analyzed by means of the fault-tree method and their reliability has then been evaluated with the aid of the programs CRESSEX, CRESSC and STREUSL. The resulting destributions of the unavailabilities - related to the individual event sequences - have been coupled with the failure possibilities of the containment integrity, in order to determine the frequencies of releases categories caused by the initiating event "ATWS".

Another GRS-study is the Risk Oriented Analysis for the Fast Breeder Reactor 300. Since the analyses have been started only a few weeks ago, no results are yet available. It is intended, however, to apply the computer code package RALLY in a similar manner as used in the above described studies.

4.2 Application of RALLY in the licensing procedure

As stated in the criteria of the Federal Ministry of the Interior (BU 77), the reliabilities of safety relevant systems and components have to be determined by means of probabilistic methods - as supplement to an overall safety evaluation of the nuclear power plant performed in a deterministic way. This reliability analysis should be done with an accuracy that corresponds to the recent state of art in science and engineering.

The safety analysis of smaller systems or subsystems performed with the aid of probabilistic methods in the framework of licensing procedures, may often be done by means of estimations on the basis of the prepared fault-trees. An example for this is the reliability analysis carried out by the GRS concerning λ-pipe feeding of emergency power bus-bars in the Fast Breeder Reactor-300 (SNR-300).

In large systems with various time intervals between the functional tests of the components, a numerical determination of the reliability parameters (mean unavailability, failure probability) is only possible with the aid of computer programs. In this case, GRS normally uses the programs TREBIL, TIMBER and CRESSEX when doing computations for licensing procedures.

For the SNR-300 licensing procedure, a probabilistic analysis of the residual heat removal has been performed applying the computer code package RALLY. In this context, for the both diverse systems (loop specific heat removal system, immersion cooling system), the unavailability per demand as well as their failure probability during the subsequent longterm phase have been calculated. For the long-term phase, the program CRESS4 has been applied.

The calculations show, among others, that during the long-term phase it is more favourable, not to wait for the automatic start up of the immersion cooling system, but to put the system into service manually immediately after the failure of the loop specific residual heat removal and without demanding the function of the emergency recirculation system.

For the nuclear power plant Grafenrheinfeld, reliability analyses have been performed on the accidents "small leak" and "large leak" in the primary circuit. In these investigations, emphasis has been placed on the following items:

- search for weak-points,
- calculation of parameters,
- influence of test intervals,
- influence of subsystems on the overall results,
- comparison with the results of the German Risk Study and
- influence of repair times.

For the treatment of the last item, parameter studies have been performed to take into consideration the influence of additional tests on all redundancies. Such additional tests may be performed, when component failures are determined or maintenance work is to be done. In order to calculate the influence of additional tests, the program CRESSEX had to be modified, which was possible with a relatively small effort.

Questions similar to those considered in the Grafenrheinfeld plant, have to be treated as well for the nuclear power plant Gundremmingen (KRB II), concerning the initiating events "ATWS" and "rupture of the main-steam line".

In addition to the above mentioned tasks, the failure probability of the turbine overspeed protection system has been calculated for the Grafenrheinfeld plant. As the failure probability of this system is very low, the application of the simulation program CRESSEX was not suitable in this case. Therefore, the approximated system function (minimal cuts) has been determined by means of CRESSC and the point-value of the result been calculated with STREUSL.

In the reliability studies of the emergency core cooling system for the nuclear power plant Krümmel, the maximum unavailabilities had to be determined - contrary to the up to now cited tasks in the framework of the licensing procedure, where only the determination of mean unavailabilities has been required. For the determination of maximum unavailabilities, the program FESIVAR has been applied.

4.3 Users of the computer code package

The program package RALLY is not only applied within GRS for the assessment of system reliability. The following institutes and firms have obtained the program as a whole or at least parts of it:

- Bayer AG, Leverkusen
- BBR (Babcock-Brown-Boveri Reaktor GmbH)
- CNEN (Comision de Energia Nuclear), Brasilien
- Dornier-System, Friedrichshafen
- KFA Jülich (research center)
- KWU (Kraftwerk Union AG)
- TÜV Bayern (Technical Inspection Agency)
- TÜV Rheinland (Technical Inspection Agency).

Persons or installations interested in the computer code package are requested to contact GRS, Dept. Data-processing.

REFERENCES

(As et al. 80) Astolfi, M., C.A. Clarotti, S. Contini und F.R. Picchia:
SALP-MP, A Computer Program für Fault-tree Analysis
of Complex Systems and Phased Missions
P.E.R. 389, 1980 - JRC Ispra Establishment

(BU 77) Der Bundesminister des Innern:
Sicherheitskriterien für Kernkraftwerke
Bundesanzeiger Nr. 206 vom 3. Nov. 1977

(Ca, Ri 75) Camarinopoulos, L., und G. Richter:
KARI - ein neues analytisches Programm zur Berechnung
von Zuverlässigkeitsmerkmalen technischer Systeme
Angewandte Informatik 12/75

(GE 79) Gesellschaft für Reaktorsicherheit:
Deutsche Risikostudie Kernkraftwerke
- Hauptband -
Hrsg.: Der Bundesminister für Forschung und
Technologie, Bonn,
Verlag TÜV-Rheinland, Köln, 1979
ISBN 3-921059-67-4

(GE 80) Gesellschaft für Reaktorsicherheit:
GRS-Jahresbericht 1980

(GE 81) Gesellschaft für Reaktorsicherheit:
Deutsche Risikostudie Kernkraftwerke,
Fachband 2: Zuverlässigkeitsanalyse
Hrsg.: Der Bundesminister für Forschung und
Technologie, Bonn,
Verlag TÜV-Rheinland, Köln, 1981
ISBN 3-88585-013-3

(KE, GE 81) Kernforschungsanlage Jülich und
Gesellschaft für Reaktorsicherheit:
Sicherheitsstudie für HTR-Konzepte unter deutschen
Standortbedingungen
Jül-Spez-136/Bd.1, Dez. 1981
ISSN 0343-7639

Gesellschaft für Reaktorsicherheit (GRS) mbH

Schwertnergasse 1
5000 Köln 1

Forschungsgelände
8046 Garching

ISBN 3-923875-05-3