What Can be Gained by Probabilistic Safety Analyses on Systems of Nuclear Installations?

J. Huber, P. Kafka, G. Reichart
Gesellschaft für Reaktorsicherheit (GRS) mbH, Forschungsgelände, D-8046 Garching, Germany

ABSTRACT

Probabilistic Safety Analysis (PSA) have been applied to various reactor concepts as well as to a great variety of systems. The scope of these analyses reaches from more general concept analyses to very detailed system analyses, as for the German Risk Study. This paper tries to illustrate on some examples typical outcomes, gained by the application of PSA-methods to these different levels. Depending on the depth of examination, examples are given for the PSA application in a full scope risk assessment, a risk oriented study, a precursor study and for concept evaluation. Main results of these studies like hardware modification improvements of test and repair strategies, and improvements of the operational manual are briefly commented.

1. INTRODUCTION

In the last years, the importance of Probabilistic Safety Analyses (PSA) have increased in parallel with improvements in methodology and applicability to a great variety of problems /1, 2, 3, 4/. This analysis technique has reached a level where standardized procedures for its use are available. Furthermore a lot of studies have demonstrated the practical applicability. PSA has been applied to various reactor concepts, as well as to a great variety of installations e.g. reprocessing plants or chemical plants. The detail and scope of the analyses reaches from more general concept analyses to very detailed system analyses as for the German Risk Study /1/. Depending on the depth of the PSA one can achieve information for design, construction or operation, for identification of weakpoints in systems or for decisions of backfitting actions for operating plants as well as for the evaluation of the risk of nuclear power plant operation.

Generally, four systematic and mostly quantitative analysis methods are applied for the PSA. These are:

- Event Tree Analysis
- Fault Tree Analysis
- Analysis of Dependent Failures
- Human Reliability Analysis.

Concerning the application, these methods and the appropriate data have to be adjusted to the various levels of analyses.

This paper discusses briefly typical results gained with the above mentioned methods. The examples presented here are taken from various applications in the GRS to demonstrate the flexibility of the PSA methodology.

2. FULL SCOPE RISK ASSESSMENT

The most detailed and extensive analysis is required by a full scope risk assessment /1, 3/ using all of the above mentioned methods. Furthermore, a plant-specific set of reliability data has to be prepared. The application of these reliability methods in the German Risk Study has led to a variety of modifications, ranging from modifications of test strategies over hardware modifications to improvements of the operation manual. The identified weakpoints had consequences for system improvements in the reference plant as well as for design aspects in new plants. In the following, some examples of improvements gained by this study are discussed in some detail.

2.1 Improvements of Test Strategies

In the ECCS some weakpoints were found. One of these is a weakpoint in the functional tests of the accumulator check valves. Examination of the detailed functional test procedure showed that no check of the position indicators of the check valves was included in the test procedure. Therefore, in case of a failure of the position-indicator a faulty open position of these valves could not have been detected. This undedected failure contributes significantly to the loss of ECC by failure of the containment integrity. To reduce this influence the test procedure and the test frequency have been modified.

2.2 System Improvements by Hardware Modification

The identification of weak points also led to several hardware improvements. Two examples are given here:

- Partial automation of the cool-down during small LOCA in the subsystem "feedwater steam supply system".

Initially, the cool-down of the primary system in case of a small LOCA had to be performed by the operator by manual operation of the main steam bypass valve or the relief valve. The operator was expected to follow the nominal value of the main steam temperature gradient of 100°K/h, which was supposed to be registered by a dotted line recorder. The cool-down with 100°K/h via secondary system was automatized. Now with pushing a button the plant can be cooled down automatically with the specified gradient by the main steam bypass or relief valves. It should be noticed that with this automation a main contributor to the core melt frequency was eliminated.

° Reconnection of the emergency power supply system to the grid.

In the case of a loss of preferred power with an additional failure of the diesel generators it was not possible to reconnect the emergency power supply to the grid, when the preferred power supply reoccurred. The reason for this was, that the pertinent reactor protection signal could not be resetted. Nevertheless, it was possible to supply two buses of the emergency power supply from the unit Biblis A. To improve the availability of the emergency power supply in this case the reactor protection system has been changed to allow a re-connection to the grid.

2.3 Improvements of the Operation Manual

As to this topic, only one detailed example will be discussed here:

° Logic tree of the operational handbook: Shut-down of the HP-safety injection pumps, if pressurizer water level is higher than 8 m

In this logic tree of the operational handbook the following has been formulated:
At a pressurizer level > 3.15 m the reactor protection signals have to be manually overridden by actuating a key switch and the four HP-safety injection pumps are to be switched off individually. This information could have been interpreted such, that at a pressurizer water level > 3.15 m, each pump had to be switched off. This had caused the water level to drop below 2.85 m, thus an automatic restart of the HP-safety injection pumps is initiated by the reactor protection signals. The pumps would be turned on and off more frequently than they are designed for. Now, it is required that the pumps are not switched off before the pressurizer water level reaches 8 m.

3. RISK ORIENTED STUDY

In a risk oriented study, like the study of the 300 MW Fast Breeder Reactor /5/, the level of detail is necessarily lower than that of a full scope risk analysis. The reasons for this are, that a risk oriented study is used rather for risk comparison of reactor concepts than for a risk assessment of an already operating plant and that details of the system design and the operation are not fixed. The methods applied to risk oriented study include event tree construction and gross fault tree analysis, which means, that consideration of details of the system design is very often impossible. Moreover, also a dependant failure analysis and a gross human error analysis are performed. A gross human error analysis uses screening values for estimating the influence of the identified human tasks. Typical results were the identification of the initiating events and of the required system functions dominantly contributing to the risk.

4. APPLICATION OF PSA-TECHNIQUES IN THE "GERMAN PRECURSOR STUDY" (GPS)

The application of systemanalytic tools and expecially of probabilistic methods on the Licensee Event Reports (LERs) and on other operating experience can support

- a deeper understanding of event scenarios and the safety-related importance of events reported in reactor operation
- the identification of possible weak points
- generic conclusions to be drawn for design and operation of NPP's.

Additionally, such a study aimed at a comparison of its results for the severe core damage frequency with those of a Risk Study. The GPS /6/ is a plant-specific study. The reference plant is Biblis NPP with its very similar Units A and B. The study was restricted to initiating events, system and multiple failures as well as human actions which occured during the observation period. In comparison with the German Risk Study the operating experience of Biblis NPP has not revealed any new types of initiating events.

As precursors to potential severe core damage accidents, the following types of events were selected

- Events, which lead as initiators not only to a reactor scram but also to a demand on further safety systems or safety-related systems.
- Events, where
  - a total loss of a system function or
  - a multiple failure or a potential multiple failure.

  occurred.

The probability evaluations performed in the GPS for the different precursors were based on the fault trees at the German Risk Study. The individual event sequence were evaluated considering both, the frequency of the initiating event and the probabilities of system failures at the time, when the initiating event occurred.

The main results of the GPS with the trend in the overall frequency per reactor year of events selected as precursor in both units of Biblis NPP is shown in Fig. 1.

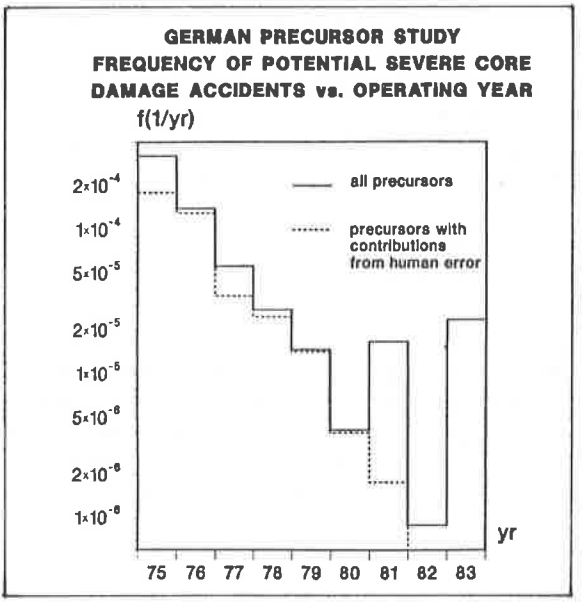

Fig. 1

The Fig. 1 shows the trend in the overall frequency per reactor year of potential severe core damage accidents. The main contributions to the severe core damage frequency come from the first years of plant operation; its decrease with increasing operating time is due to numerous system improvements. The mean value of the overall frequency of potential severe core damage accidents is $4.7 \cdot 10^{-5}$ per reactor year. The above mentioned results fit into the 90 % confidence interval for the core melt frequency which was obtained by the German Risk Study reaching from $1 \cdot 10^{-5}$ to $3 \cdot 10^{-4}$ per reactor year, with a mean value of $9 \cdot 10^{-5}$ per reactor year.

Human error has influenced 50 % of the events selected as precursors. These events contribute 67 % to the total result. However, one has to be aware that the present situation of documentation of operating experience is not sufficient for cause-oriented evaluation of human errors.

5. APPLICATION OF PSA-TECHNIQUE FOR CONCEPT EVALUATION

Concerning design and safety analysis of nuclear installations, PSA-techniques even can be used as a valuable tool in the concept phase. Here, reliability analyses aren't carried out in the same depth as the formerly reported analyses. For a given system lay-out, the order of

magnitude in reliability is elaborated with regard to the need of redundancies, the influence of auxiliary systems or the importance of instrumentation or control, even knowing, that essential reliability aspects as human error or maintenance are not exactly to be quantified. For this reason rough-meshed reliability evaluations are done (event tree and fault tree analysis) with generic reliability data and simplified dependent failure and human error analysis, based on the general methodical and empirical background of reliability techniques.

Recommendations in system improvements and the importance of certain procedures towards a balanced system concept can be derived. The feasibility of systems to fulfill prescribed reliability goals are checked.

The following example is mentioned to show the application of PSA-technique for concept analysis of a reprocessing plant. Here, the reliability of the cooling system of vessels with self-heating solutions is a well known matter of interest. The cooling system a.o. has to assure with high reliability, that an unadmissible release of radioactive material (aerosols) out of the self-heating solutions (e.g. high active waste) can be classified as hypothetical event.

There are first of all the operational primary and secondary cooling systems. In case of an interruption of the vessel cooling, several measures of recovery of the cooling function are foreseen before boiling is reached. The potentials for transmission in spare tanks of the inventory of interest, its delution, the emergency feed of water in the initially failed system or its repair have to be analyzed by means of event tree and quantified by fault tree techniques. Finally, a diverse passive cooling system allows the recondensation of vapour on the vessel off-gas side if boiling under extreme and rare conditions will be reached.

The probabilistic evaluation of the multiple and flexible cooling concept shows, that for all categories of initiating events or unavailabilities (failures of active or passive components, failure of power supply, external events) the frequency of loss of cooling function can be expected well below 10^{-5}/a. Certainly, this forecast based on a rough concept has to be reanalyzed later on the basis of the final system design, specifications and the associated operational requirements.

6. CONCLUSION

As a result of the wide spread application of PSA and its technique, the following can be summarized:

- The PSA has reached a wide and scientifically approved state.
- There is a worldwide common understanding, common terminology, and similarity of procedures.
- The significant parts of the PSA technique, namely, the probabilistic analysis of damage or failure possibilities, are applied widely.
- Particularly this significant parts can be usefully applied for the optimization and evaluation of the system design and operation with all relevant technical specification.
- For different plants or systems with various design characteristics the PSA-technique provides measures for comparing or improving of the safety level.

References

/1/ GESELLSCHAFT FÜR REAKTORSICHERHEIT (GRS) MBH, "Deutsche Risikostudie Kernkraftwerke", Hauptband und Fachbände, Verlag TÜV-Rheinland, 1979, ISBN 3-921059--67-4

/2/ "Probabilistic Risk Assessment (PRA): Status Report and Guidance for Regulatory Application", NUREG 1050, DRAFT Report, February 1984

/3/ Seabrook Station, "Probabilistic Safety Assessment", PLG-0300, December 1983

/4/ SCIENCE APPLICATIONS INC.: "Status Report on the EPRI Fuel Cycle Accident Risk Assessment", EPRI-Rep. NP-1128, Palo Alto, Cal., July 1979

/5/ GESELLSCHAFT FÜR REAKTORSICHERHEIT (GRS) MBH, "Risikoorientierte Analyse zum SNR-300", GRS-51, Köln, Garching, 1982, ISBN 3-923875-00-2

/6/ H. HOERTNER, W. FREY, J. V.LINDEN, G. REICHART, "German Precursor Study, - Methods and Results -", ANS/ENS Topical Meeting on Probabilistic Safety Methods and Applications, San Francisco, February 1985