Living PSA and PSA Applications for the Optimization of Power Plant Operation

A. Gessler , Kernkraftwerke Gundremmingen, Germany
K. Götz, TÜV Süddeutschland, Germany

ABSTRACT

In addition to using a fundamental deterministic approach for the overall evaluation of safety, probabilistic analysis can also be regarded as a suitable tool. In this context PSA, and especially Living PSA, therefore gains increasing importance. This paper discusses the possible use of PSA as a decision making tool to address plant safety management issues, and as an aid for discussion of the regulatory authorities' supervision procedures. This paper is based on the Living PSA for NPP Gundremmingen.

INTRODUCTION

Since the early 90's, a German Guideline has enforced periodic safety reviews (within every ten-year period) for every Nuclear Power Plant. These reviews have included probabilistic safety assessments. At present, Level 1 PSA's (for power operation) for all plants in Germany have been undertaken. Level 1 PSA enables quantification of the overall number of endangering situations, the evaluation of the balance of the safety design and a list of weak points – under the boundary conditions of the German PSA-guide [1].

Funded by the Federal Ministry of Education, Science, Research and Technology (BMBF), Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) performed a probabilistic analysis for a boiling water reactor (BWR). The reference plant was Gundremmingen NPP Unit B (Siemens KWU 72-type twin unit plant). The first phase of the BWR-safety analysis [2] was completed in June 1993. Following this investigation a subsequent phase 2 analysis was undertaken. The investigation of events during power operation was completed in December 1995 [3]. Event sequences were analyzed, until conditions were identified which would lead to core damage if additional accident management measures were not taken. This intermediate stage was characterised as the 'hazard state' of the plant. The BWR safety analysis was used at NPP Gundremmingen for the previously completed periodic safety review.

The BWR safety analysis does **not** enable a risk or safety based optimization of plant operation and supervision to be undertaken (including maintenance and test strategies, evaluation of events and modifications in hardware and operational procedures). Therefore, the owner of NPP KRB II decided to perform a Living PSA, based on the PSA, in accordance with the Guideline. Living PSA is much more detailed in modeling important parts of systems (based on the results of the existing PSA), is much more realistic as regards efficiency conditions (but still conservative), and therefore gives a better view of the actual behavior of the plant.

Differences between BWR Safety Analysis and Living PSA

The main differences and additional requirements/characteristics of the Living PSA are:

- Plant specific component failure data are as wide as possible for independent failures
  For plant specific data collection, the relevant pumps, valves, analog signal modules, digital signal modules, drive control modules etc. were divided into data groups (e.g. 162 pumps in 11 data groups; 2884 valves in 44 data groups).

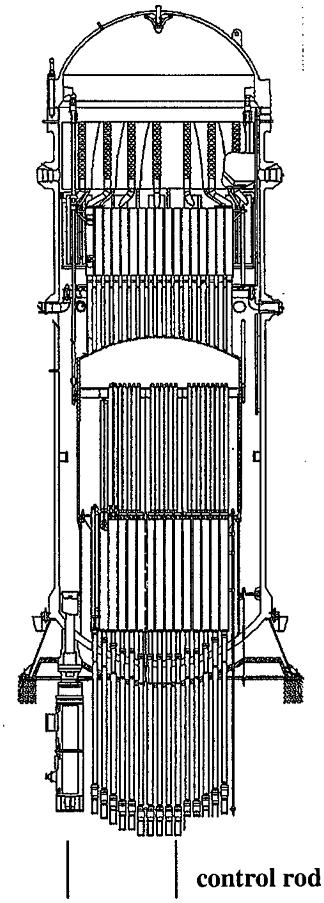
- e.g. pumps collective 1: re-entry-pumps
  2: single stage pumps
  3: main feed water pumps
  4: fuel pumps
  5: multistage pumps
  6: control rod pumps
  7: piston pumps
  8: gear-type oil pumps
  9: submersible pumps
  10: vacuum pumps
  11: control fluid pump

  The criteria for selection of the pumps were design, type, stages, flow rate, number of switching, operating hours and medium.

- Plant specific component failure data for common cause failures (CCF)
  The selection of components having CCF potential was identified as crucial and assessed newly. All events in the German database were checked on comparability.

- Detailed modeling of the complex reactor protection system for reactor shutdown
  e.g. with scram and by control rod drive operation and different resulting minimum requirements for high pressure injection

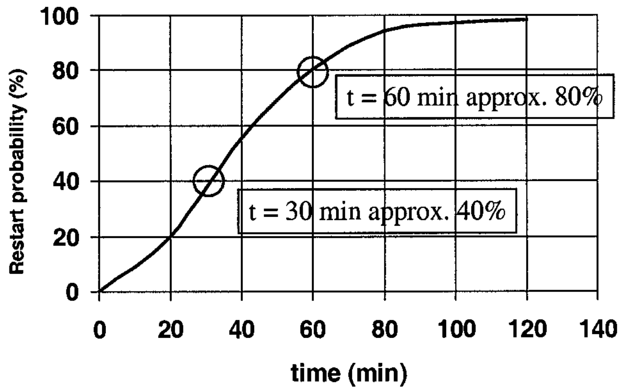
- Taking into account operational systems for safety functions



For instance, the high pressure control rod flushing injection system (2 trains, 2 train independent injection rate control systems, 2 pumps with 2 different drive motors each) and the recirculation pump sealing water system (3 trains, 3 train independent injection rate control systems, 3 pumps) were modeled. During power operation, both systems permanently feed into the RPV. The injection rate of the systems can be increased by manual accident management actions. These manual actions were assessed. The injection rate is dependent on the RPV-pressure and the availability of the trains, pumps and the injection rate control systems. The RPV-pressure and the additional minimum requirements depend on the sequence in the event tree. For instance at scram failure (shutdown only by control rod drive), both systems are not able to keep the filling level above the top of the core. The variety of possible combinations was summarized efficiently in the modeling of fault and event trees.

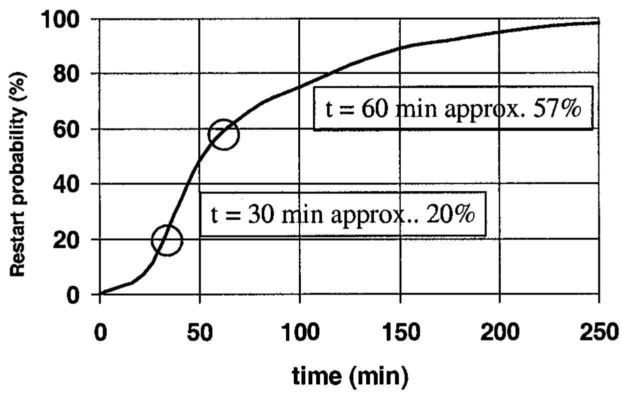
Fig. 1: Operational RPV-feeding systems

- Taking into account the time factor for recovery for some initiating events



The inclusion of the feedwater restart system was realized by function recovery after system failure. How much time is available depends on the event tree sequence. The probability for recovery of the main feed water is based on real operational experience and data.

Fig. 2: Restart of feedwater system function



The restart of the main heat sink was taken into account analogously.

Fig. 3: Restart of main heat sink function

- Inclusion of operational experience and consideration of plant specific boundary conditions
  Relevant disturbances were investigated at the simulator and new thermohydraulic analysis with the code ATHLET have given information about plant behavior after the initiating events and about the success criteria. The latest findings and statistical data were taken into account as regards the minimum requirements of the residual heat removal systems and the relevant temperature curve for the river Donau relative to recent years.

- Inclusion of unavailability due to maintenance
  Maintenance, leading to temporary unavailability of specific systems, are represented as events and "house events" in the fault tree, and are taken into account in the analysis by the corresponding boundary conditions.

- Reassessment of human reliability
  A reassessment of the human reliability of staff during accident sequences was undertaken with THERP [4] and ASEP [5].

- New determination of initiating events and their frequencies
  For the determination of initiating events, the operating experience was evaluated and additional information from existing PSA's (and also the theoretical considerations) were used. All events that occurred at the twin unit plant in the period 1988 to 1998 were analyzed. With this evaluation, the frequency of initiating events were determined, and the accompanying event trees examined. Two coolant loss accidents with generic frequencies were examined. The internal events (internal fire, flooding by leakage of systems, explosion in the plant, high-energy vessel-failure) and the external events (earthquake, external fire, external flooding, lightning strike, explosion shock wave and air crash) were only examined within the periodic safety review.

- Taking into account an electrical power increase
  The actual, planned increase of electrical power was taken into account in the Living-PSA. The minimum requirements were adapted according to new thermohydraulic analyses (undertaken with ATHLET). Because the increase of electrical power is also accompanied by a higher target pressure, the minimum requirements for the safety and relief valve systems were checked. At this point, it must be remembered that a definite pressure may not be exceeded and that the designed injection pressure of the injection systems is reached in time.

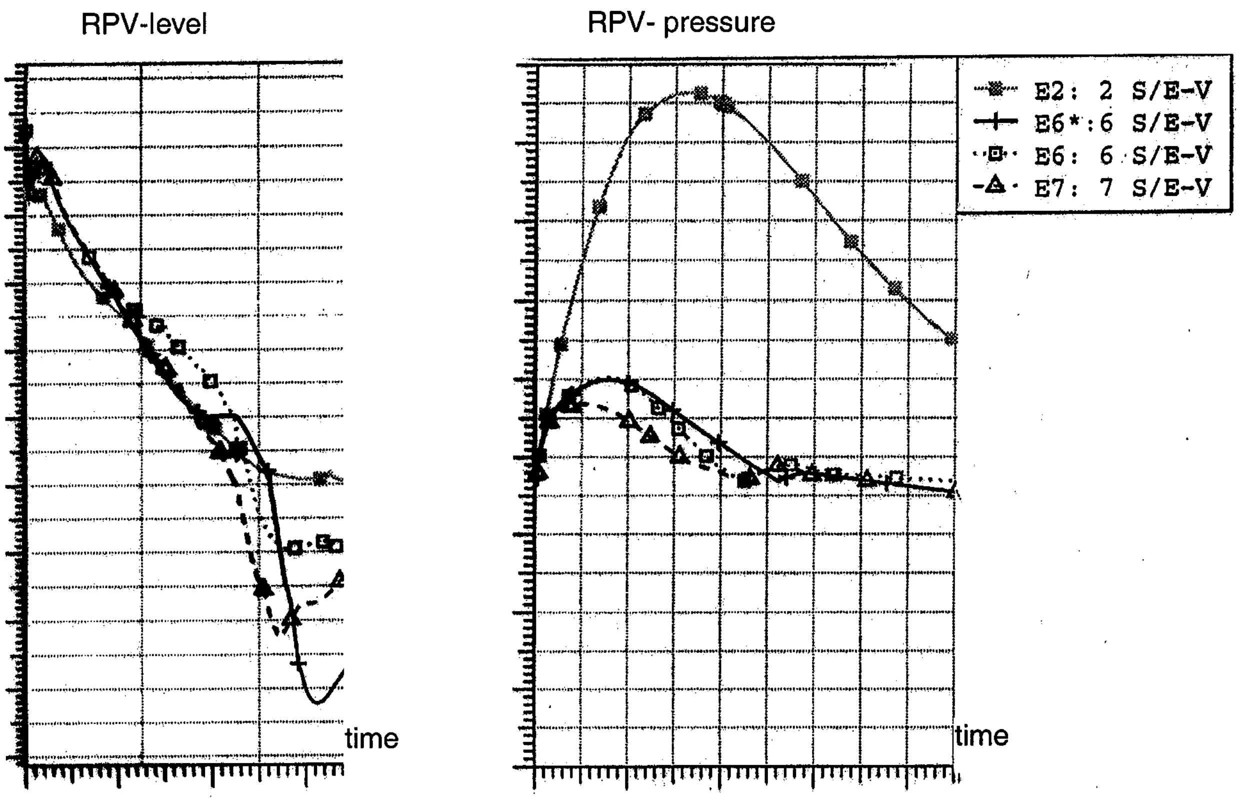
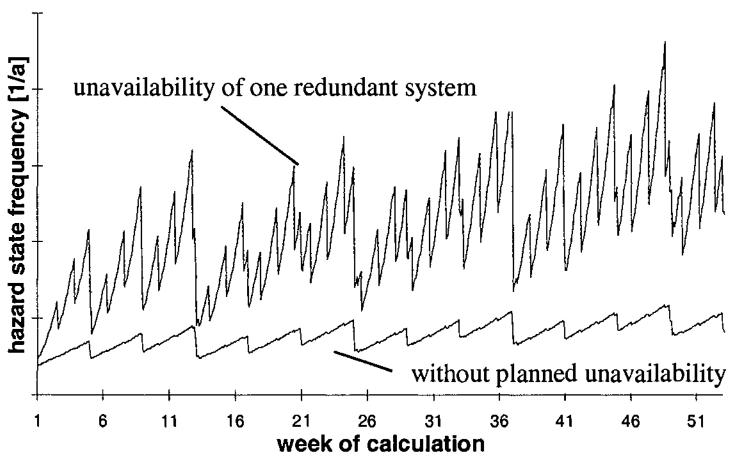


Fig. 4: ATHLET results for safety and relief valves

Use of the living PSA

Thus a PSA was performed that is very detailed, where necessary, and this is now the basis for different procedures. In detail, the Living PSA will be used for:

- Risk based optimization of maintenance strategies
  Probabilistic proof/evidence is required to obtain permission to perform preventive maintenance on the safety system during full power operation. To get permission, it is necessary to prove that plant safety integrity will not be impaired by the implementation of these measures. Various different compensation measures, such as additional tests, are necessary and must be considered under probabilistic aspects. Not only is the duration of non-power operation reduced by preventive maintenance, but a decline of unavailabilities caused by failures can be achieved. Through the increase of the availability of parts of the safety system during the outage (by using preventive maintenance) safety integrity will be influenced in a positive way. Since no detailed investigations about the safety of conditions outside power operations presently exist, this impact on the integral plant safety remains relatively insignificant and, in a conservative way, is therefore not considered. Usually the observation time period in a PSA is a year and is focused on the power operation. In this case, a time-dependent calculation is not necessary. Because the influence of the unavailability is dependent on the period of time, and compensation measures such as the reduction of test intervals, time-dependent calculations must be implemented. By using the time-dependent analysis function of the PSA program, Risk Spectrum, a calculation, which considers unavailabilities and different test strategies, is possible. In Risk Spectrum, it isn't possible to define planned unavailabilities for determined periods, so separate calculations about the entire time are necessary for these periods.



This diagram shows the idealized course of the time -dependent hazard state frequency with respect to time, for a plant with and without unavailability of one redundant system. The falling levels after every 4 weeks are caused by tests of a diverse residual heat removal and injection system. The rising levels during the course of the year is the result of the increasing unavailability of annually tested components; for instance safety and relief -valves.

Fig. 5: Time dependent hazard state frequency curve

- Risk based optimization of the inspection strategies
  Proof is also necessary for the optimization of test intervals for periodically tested components. By using the time-dependent analysis function of the PSA-program Risk Spectrum, a calculation is possible giving consideration to unavailabilities and different test strategies.

- Optimization of single test procedures
  For instance, for a reactor pressure vessel test with fuel, probabilistic proof was required that the endangering frequency is negligible compared with the power operation. This evidence was furnished in 1999 with an intermediate stage of the Living PSA. For the complete time period of the pressure test, a probabilistic analysis of relevant initiating events was carried out and compared with the results of the BWR safety analysis for the power operation.

- Evaluation of events and precursors
  Events in other plants must be checked, by comparison, and possible effects in this plant and remedial measures must be planned and carried out in the plant, if necessary.

- Preparing decisions for hardware and operational procedures.
  For instance, in the context of optimization of single test procedures, it was established that a rearrangement of the shift teams (to 7-week intervals as regards single redundancies tests), brings advantages in terms of fault detection and training, because every shift checks every redundancy by undertaking tests.

- Safety assessment for retrofitting measures

- Risk based optimization of working sequences
  plant operating manual

- Structuring of accident management measures according to probabilistic priority

- Planning and optimization of training programs according to safety-relevant event sequences

Conclusions

PSA, and especially Living PSA, is gaining increasing importance in supporting decision making as regards safety management questions, and as an aid for discussion of the regulatory authorities supervision procedures. Therefore, in addition to a fundamental deterministic approach, probabilistic analysis is a suitable tool for the overall evaluation of safety. It enables realistic safety evaluation and decision criteria for different request cases. Living PSA has proven to be an effective decision making tool for plant operation and supervision.

References

[1] BfS, Periodische Sicherheitsüberprüfung für Kernkraftwerke, Leitfaden PSA, Dez. 1996.

[2] GRS, SWR-Sicherheitsanalyse, Abschlußbericht, ISBN 3-923875-52-5, Köln 1993

[3] GRS, SWR-Sicherheitsanalyse, Phase II, Abschlußbericht,
Band 1: Untersuchungen von Ergebnissen aus dem Leistungsbetrieb, Köln 1995

[4] Swain, A. D. & Guttmann , Handbook of Human Reliability Analysis with emphasis on nuclear power plant applications, Sandia National Laboratories, NUREG/CR-1278. Washington DC

[5] Swain, A. D., Accident Sequence Evaluation Program on Human Reliability Analysis Procedure. NUREG/CR-4772. NRC. Washington DC.