
Comprehensive technical evaluation of an advanced German PWR by PSA - Objectives and main results

K. Köberlein

Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) mbH, 85748 Garching, Germany

Abstract: In November 1998 at the Eurosafe meeting in Berlin the concept of a Probabilistic Safety Analysis (PSA), level 2, for an advanced German PWR has been presented. This paper is summarising the results produced over the last two years and it is discussing the insights into PSA methodology and also into the safety features of the reference plant. Based on the experience from the current work the important role of PSA in the safety evaluation of nuclear power plants is confirmed.

1. OBJECTIVES

It was not the objective of the present PSA, to gain insights into the safety features of a specific plant. The aim was rather to evaluate the currently available PSA methods by applying them to an advanced PWR and performing – within about 3 years – a comprehensive level 2 PSA. A level 1 PSA calculates the expected frequency of a core damage, the main results of a level 2 PSA are the expected frequencies and the core inventory fractions of radionuclide releases to the environment after containment failure. “Comprehensive” in this context is to be interpreted not in an absolute sense, but as relative to the available methods.

As reference plant for the PSA we could use unit 2 of “Gemeinschaftskernkraftwerk Neckar” (GKN-II). GKN-II is a 1365 MWe PWR of the “Konvoi” (convoy) - design. The plant went into commercial operation in April 1989 and, with an average availability of 97 %, it is in the top performance ranks. The utility has supported our work by providing us with the very detailed information on plant design and operation required for a PSA. Furthermore, we could take advantage of a PSA performed on behalf of the utility by Siemens-KWU [1] for the periodical safety review according to the German PSA procedures guide [2]. We have used this PSA as a basis for our work.

It was not by chance that a plant with one of the highest safety standards has been used as a reference for the PSA. This type of plant is in full compliance with the current German nuclear safety regulations, in particular with the safety standards of the KTA (Kerntechnischer Ausschuss / Nuclear Safety Standards Commission). Therefore from the PSA results it may be concluded which level of safety can be reached by implementing the (nearly completely deterministic) requirements of nuclear safety regulations. Furthermore, the challenges for the PSA methods are increasing with increasing safety standards.

2. APPROACH

We have modified the basis-PSA provided by the utility according to our own PSA requirements mainly in the following features:

- First of all, we have replaced the model used in the basis-PSA for the evaluation of common cause failures (CCF) by a model developed by GRS. The GRS model is an extension of the modified binomial failure rate (BFR) model which has been applied already in the German Risk Study, Phase B [3]. The new “coupling model” [4], [5] applies expert judgement of the degree of functional degradation of each component within the group of components affected by a (potential) common cause failure instead of using fixed coupling parameters like the former model. The degree of degradation is evaluated according to a scale developed by the “International Common Cause Data Exchange” group respectively by the USNRC. For the application of the “coupling model” all common cause events, which are the basis of the GRS CCF data set, have been newly evaluated according to the requirements of the new model.
- We have replaced the set of generic reliability data used in the basis-PSA by plant specific reliability data based on the evaluation of four years of operation (1994 – 1997) of the reference plant. For components with too few events in this relatively short period of observation generic data had to be included into the data base generation. Dependant on the available information two different mathematical approaches have been applied. If sufficient information was available for a component the non-informative approach of Bayes has been applied. In other cases the generic data have been used as priors and updated with the available specific data using the superpopulation approach of Bayes [6], [7].
- The event tree and fault tree analyses have been modified and completed in many instances. In some cases additional thermohydraulic analyses have been performed and minimum system requirements have been modified. We have considered additional system functions especially in situations where the updating of the CCF model and data resulted in high system function unavailabilities.
- In the systems analysis also operator actions planned in the protection goal oriented part of the operating manual have been considered, while the basis-PSA took account only of the event oriented part of the manual.
- In former projects GRS has developed improved methods for the probabilistic evaluation of accident management measures [8]. These methods have been applied for the evaluation of secondary side bleed and feed and of primary side bleed and feed initiated after failure of design basis safety functions. The basis-PSA considers only secondary side bleed and feed.
- We tested the possibility to take into account the repair of failed components after accident initiation. For this purpose, we investigated – as an example – the probability that components required for steam generator feeding can be repaired after a loss of main feedwater, prior to the onset of criteria for AM measures. According to the German PSA procedures guide repair is not considered in the basis-PSA.
- We investigated the possible risk contribution from fires. As a representative example cable fire scenarios within the reactor building have been – in part quantitatively – considered.
- Contributions from external impacts (seismic, air-plane crash, chemical explosion, floods, extreme weather conditions including lightning stroke) and from the failure

of large passive components have been qualitatively – and in part quantitatively – estimated.

Completely new analyses have been performed for

- a level 1 PSA for non full power states
- the level 2 part of a PSA for accidents during power operation .

Since these parts of the PSA are presented in separate papers [9], [10], this paper is concentrated on the results of the full power level 1 PSA.

3. MAIN RESULTS OF THE FULL POWER LEVEL 1 PSA

- Initiating events

In the full power part of the PSA altogether 22 initiating events have been considered, representing the full spectrum of plant internal initiating events possibly relevant for the expected frequency of damages states. Nine of the 22 initiators could be excluded from a detailed analysis since significant contributions to the results were not to be expected. For 13 initiators event tree and fault tree analyses have been performed. In this way possible system damage states have been identified and their expected frequencies have been calculated.

The plant is – by definition – in a “system damage state” (another word for the same condition is: hazard state), if after an initiating event the design basis system functions required to cope with this event are not available and core damage can be prevented only by means of accident management measures (including the repair of failed components). The expected frequency of system damage states can be seen as a measure for the level of safety reached by all safety functions within the design basis. In other countries the system damage state frequency is normally not explicitly displayed as a PSA result.

- System damage states

The total expected frequency of system damage states is $5.4 \cdot 10^{-6}$ per year. The main contributors are the loss of main feedwater (24 %), the very small primary leak (22 %), the loss of preferred power (16 %), the loss of main heat sink (15 %) and the pressuriser leak via a stuck-open safety valve (6 %). For the transients the loss of feedwater supply is the mainly responsible system function failure, for the LOCAs low pressure injection and high pressure injection failure are the main contributors. In all cases the common cause failures of redundant components play an important role (importance: 72 – 100 %). For the five dominating initiating events common cause failures are involved to 94 – 100 %. The influence of human failures is very low in most cases, for the very small LOCA human failures are involved to 18 %. The overall importance of common cause failures is 96 %, the overall importance of human failures is 6 %.

- Core damage states

In the next step of the PSA the potential of accident management (AM) measures (including repair) to prevent the progression from system damage states into core damage has been investigated. The conditional failure probabilities of AM measures depend on the specific circumstances of the various system damage states. The AM failure probabilities range from 100 % for LOCAs over 30 % for the loss of preferred power down to 2 % for the loss of main feedwater. This means that AM measures have a high

probability of success for transients and – for the current situation in the reference plant – no potential at all for LOCAs.

The average AM failure probability over all quantified initiating events is 0.43, resulting in a core damage frequency of $2.3 \cdot 10^{-6}$ per year. Since AM measure are not effective for LOCAs the ranking of contributions to the core damage frequency is different from system damage states. The main contributions now come from the very small leak (52 %), the pressuriser leak via a stuck-open safety valve (15 %), the loss of preferred power (10 %) and the steam generator tube rupture (9 %).

Main parameters influencing accident progression after core meltdown are the point of time of reactor pressure vessel (RPV) failure and the primary system pressure at this point of time. For the display of the level 1 PSA results core damage states are grouped into 7 categories, distinguishing the primary system pressure (low, medium, high) and the point of time of onset of core meltdown (between 1 hour and > 10 hours). For the accident progression analysis in the level 2 part of the PSA a more detailed differentiation considering further parameters is necessary. For this purpose 66 core damage states have been distinguished.

- Limitations of scope

The influences from external impacts and from the rupture of large passive components with high energy content have not been quantified. Although we do not expect significant contributions to the frequency of damage states, this judgement should be further examined mainly with respect to seismic events and extreme weather conditions. In table 1 the current results of engineering judgement are compiled.

Table 1: Judgement of influences from external impacts and structure failures

Event	Expected frequency of risk relevant events (1 / year)	Frequency of events considered in plant design (1 / year)	Expected contribution to the frequency of plant damage states (1 / year)
Earthquake	$< 10^{-4}$	not evaluated	not evaluated
Air-plane crash	$10^{-5} - 10^{-9}$	$> 10^{-8}$	$< 10^{-8}$
Chemical explosion	$5 \cdot 10^{-7} - 5 \cdot 10^{-8}$	$> 10^{-8}$	$< 10^{-8}$
Extreme floods	$< 10^{-2}$	$> 10^{-4}$	low
Extreme weather conditions	$< 10^{-2}$	$> 10^{-3}$	low partly unknown
Rupture of passive components	not quantified	not quantified	low

Furthermore the consequences of a boron dilution in the primary coolant after a small leak has not been finally analysed, since the simulation of such an event is not feasible with the currently available computer codes. A significant boron dilution could occur, if the decay heat is transferred from the primary to the secondary system in the “reflux-condenser mode” after a small leak and failure of additional system functions. Similar

situations play a role mainly in the non full power PSA, therefore this topic is discussed in more detail in the following paper [9].

We do not expect significant risk contributions from such events, but the problem should be further investigated first of all because credit is given to the reflux-condenser mode of heat transfer to cope with design basis accidents.

- Main contributors to core damage frequency

For the small leak in the primary system (2 – 25 cm²), which is contributing 52 % to the frequency of core damage states, the failure of low pressure injection is responsible to more than 70 % for the unavailability of system functions required to cope with the initiator. The importance of common cause failures is 94 % and the importance of human failures 18 %.

The situation is similar for other leaks in the primary system and for pressurise leaks. For a steam generator tube rupture (< 6 cm²) mainly the unavailability of the steam generator isolation and of the long term decay heat removal are responsible for the core damage frequency. In this case CCF are involved to 99 %.

For a loss of preferred power, contributing 10 % to core damage frequency, loss of feedwater and unavailability of secondary and primary bleed and feed are causing 96 % of the contribution to the core damage frequency. CCFs are involved to 100 % in system function unavailabilities. The importance of human failures in this case is 11 %.

Altogether system function unavailabilities are very strongly influenced by common cause failures. This fact is not surprising for highly redundant systems using very reliable components. The only way to reduce the influence of CCF – should this be considered necessary - would be by implementing component and/or system diversity.

Summarising, it can be stated that the reference plant – as to be expected – has a very high level of safety. Nevertheless, even for the highest safety level design features can be identified which are dominating the expected frequency of damage states and, hence, can be considered as (relative) “weak points”. With other words: even the strongest chain has its weakest link. These are the most important examples:

- Significant contributions to the unavailability of systems functions to cope with the small primary leak come from the CCF of the three-way-valves of the decay heat removal system, which are required for switching from injection to recirculation mode
- The CCF of steam relief valves (failure to open) is a significant contributor
- Important contributions to system function unavailabilities result from failures of high pressure injection pumps and water level measurement of the cell-type cooling towers of the decay heat removal system. There are no recurring tests of the high pressure injection pumps in the sump recirculation mode. The water level measurement of the cooling towers which is required for the decay heat removal has no redundancy and the test interval of one year is too long.
- The CCF of the 48 V accumulators of the emergency power grid 2 prevent the automatic switchover to the diesel generators of both emergency power grids.

- Uncertainty analysis

An important part of a PSA is the uncertainty analysis, propagating the uncertainty of input parameters to the uncertainty of results.

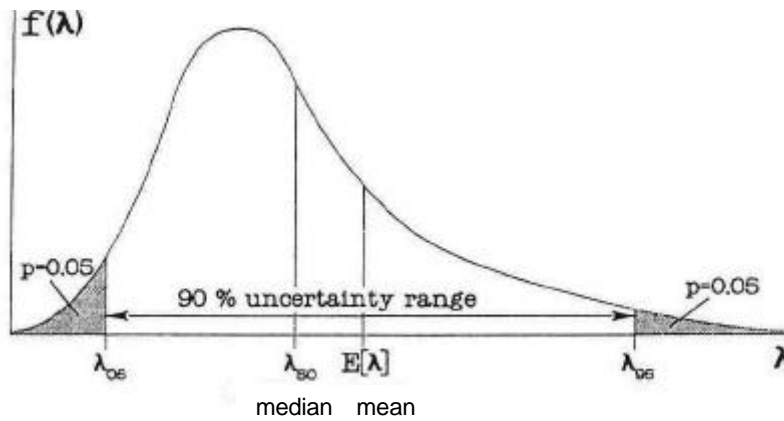


Fig. 1: Schematics of a probability density function

The input parameters of the PSA, like the failure rates of components are, or at least can be considered as, fixed values which are not exactly known. The uncertainty about the true value can be described quantitatively by a probability density function (fig. 1). From this function the probability can be derived that the true, but not exactly known value (of λ) lies within a certain interval, e.g. within the “90 % uncertainty range”. Dependent on the characteristic of the parameter, different types of density functions can be used. In the PSA the most common type of density function used for component reliability data is the lognormal distribution, which is a normal (Gaussian) distribution applied to the logarithm of the uncertain value. A lognormal distribution can be defined – like a Gaussian distribution - by two values, e.g. the median (50 % fractile) and the 95 % fractile. A fractile gives the (subjective) probability that the true value does not exceed the parameter value at this fractile. Another important point in a probability distribution is its mean value. The mean value is equivalent to the centre of gravity of the distribution. For a lognormal distribution the mean value is always higher than the median value. The distance between mean and median will increase with increasing uncertainty. If the result of the uncertainty analysis is to be described by one single figure, in our view the mean is the most appropriate choice, because it reflects to some degree also the uncertainty range of the distribution.

Table 2: Results of the uncertainty analysis for the expected frequencies of system damage states and core damage states

	Expected frequency of system damage states	Expected frequency of core damage states
	(1 / year)	(1 / year)
50 % fractile (median value)	$4.5 \cdot 10^{-6}$	$1.5 \cdot 10^{-6}$
„point value“	$5.4 \cdot 10^{-6}$	$2.3 \cdot 10^{-6}$
mean value	$1.1 \cdot 10^{-5}$	$7.0 \cdot 10^{-6}$
95 % fractile	$2.2 \cdot 10^{-5}$	$1.1 \cdot 10^{-5}$

Table 2 shows the results of the uncertainty analysis of the PSA for the system damage state frequency and the core damage frequency. Additionally to the characteristic values of the distributions “point values” are shown. In the PSA the quantitative evalua-

tion of fault and event trees is first performed using the mean values of the distributions of the input parameters, since a calculation applying the distribution itself would be much more time consuming. The results, gained with the mean values of the input parameters, are called “point values”. If the modelling of the PSA is completed, the probability distribution of the results (including the mean values) is calculated applying an approximate approach.

Ideally the point value should be very near to the mean value. In this PSA we found high factors between point values and mean values, a factor of 2 for the system damage state frequency and a factor of 3 for the core damage frequency (see table 2). The underlying reason for the difference between point and mean values is the “coupling” of reliability data. For the uncertainty analysis the distributions are considered as dependent – and therefore coupled - as far as the data for the same type of component are derived from the same pool of experience. For the point value calculation the distributions implicitly are considered as independent.

The relatively high factors between point values and means in this PSA are caused by such failure combinations for which the reliability data for several components have to be “coupled” for the uncertainty analysis. Especially important are components with relatively high failure rates (or failure probabilities) connected with high uncertainties. This is the case mainly for the high pressure injection pumps in the function of sump recirculation ($p_{50} = 0.15 / k_{95} = 7,2$), because no empirical evidence from functional tests is available. High pressure recirculation is requested by the protection oriented operators manual, if after a small LOCA steam relief via the turbine by-pass and the relief valves are not available. The failure combinations containing the operational failure of the high pressure injection pumps in the sump recirculation mode are responsible for a factor of about 2 between point value and mean of the core damage frequency. This means, that these failure combinations are much more important than it is concluded from the point values. The situation is similar for the water level measurement of the cell-type cooling towers required for the decay heat removal.

4. INSIGHTS FROM THE LEVEL 2 PART OF THE PSA

Starting from the results of the level 1 PSA for accidents during power operation the plant response to a core damage has been investigated in the level 2 part of the PSA. Methods and main results of the level 2 part are presented in [10].

The accident progression analysis has shown that even after a core meltdown there is a potential to prevent the failure of the containment and thus to mitigate the consequences of the accident considerably. This goal, however, can only be reached if the molten core can be retained in the reactor pressure vessel. If the pressure vessel fails, it has to be assumed – according to present knowledge – that the core debris in the long run will melt through the containment foundation and get into contact with the soil.

The conditional probability for a large early release is about 10 %. 3 % come from a reactor pressure vessel failure under high primary system pressure, which leads to the highest release, 7 % come from a containment by-pass via a steam generator tube rupture. In this case the release is considerably lower, if the damaged steam generator is filled with water.

From the analysis it can be concluded, that at least for plants with current design it will not be possible to completely exclude scenarios with large early releases. As a consequence, the safety evaluation should concentrate on the prevention of core damage also under changing conditions concerning the operation of nuclear power plants. In this way, the overall accidental risk can be minimised. The consequences of a core melt accident would be extremely serious even with an intact containment.

5. COMPARISON WITH THE LEVEL 1 PSA FOR NON FULL POWER STATES

The level 1 PSA for non full power operation comes up with a system damage state probability of $3.5 \cdot 10^{-6}$ per refuelling phase. This probability is equivalent to an expected frequency of $3.5 \cdot 10^{-6}$ per year under the realistic assumption of one plant shut-down for refuelling per year, comparable to – and in the same order of magnitude as – the expected frequency of $5.4 \cdot 10^{-6}$ per year for system damage states from accidents during full power operation. Because accident management measures and repair have not been considered in the non full power PSA, core damage frequency was not calculated.

6. INSIGHTS CONCERNING PSA METHODS

Main insights concerning PSA methods are the following:

- The evaluation of (internal and external) area events is still – and will remain – a difficult task for the PSA. Methods to evaluate potentially important events, mainly seismic events and fire, are available. The application of these methods is very costly, if it is not possible to restrict the analysis to the essential aspects and plant areas.
- The potential consequences of a boron dilution have to be further analysed. The necessary accident simulation tools have still to be developed.
- PSA results should be interpreted and discussed on the basis of mean values. This requires that PSA computer codes are able to calculate importance measure on this basis. Up to now point values are used for this purpose.
- Contributions from low-power/shutdown states to the expected frequency of system damage states are not negligible. Methods should be developed to extent the scope of non-full power PSA.

7. INSIGHTS CONCERNING PLANT SAFETY

Although the objective of the PSA was not the safety assessment of the reference plant, insights concerning plant safety can be derived. The PSA results allow the following conclusions:

- The PSA has shown a high safety level of the reference plant.
- The dominating influence of common cause failure could be reduced by means of component or system diversity.
- In some cases independent failures of components with high failure rates, connected with large uncertainties, contribute significantly to the unavailability of system functions.
- The operation of the high pressure injection pumps in sump recirculation mode as a design basis safety function (as planned in the protection goal oriented operator manual) is problematic.
- Accident management measures have the potential to reduce the expected frequency of core damage states also for LOCAs, provided the emergency response manuals are extended accordingly.

8. CONCLUSIONS RELATED TO THE REGULATORY APPLICATION OF PSA

For a discussion of the regulatory application of PSAs the uncertainty of PSA results is an important issue. With this respect the following conclusions can be drawn:

- The uncertainties quantified in this PSA are not unusual for situations in which low probability events have to be considered.
- There are, however, uncertainties which have not been quantified or which cannot be quantified (modelling uncertainty, completeness uncertainty).
- From the PSA results it can be concluded that – in spite of full compliance of the reference plant design with the valid nuclear regulation - there exist system deficiencies, which have not been identified – or even cannot be identified – by a purely deterministic safety evaluation. The uncertainties of bottom line results are less important with respect to such – relative – insights.
- The uncertainties of the PSA results are not caused by the probabilistic approach, but by knowledge limitations concerning the analysed system.
- The probabilistic approach makes such knowledge limitations evident and provides insights into their relative importance.
- When applying deterministic methods, the knowledge limitations also exist, but they are not made evident.
- At the current state of the art PSA is an essential supplement to the deterministic safety evaluation, even if there are no absolute probabilistic safety criteria.
- Risk-informed decision making is more sophisticated than decision making on the basis of deterministic criteria alone. However, it is also more difficult and requires additional efforts from the decision maker.
- The problems to apply PSA results originate not only from the uncertainty of these results. Even if the PSA could provide exact figures, risk-informed decision making would not be a straightforward task.

9. REFERENCES

1. Siemens-KWU
Probabilistische Sicherheitsanalyse für das Gemeinschaftskernkraftwerk Neckar, Block II
NDS4/09.98, September 1998
2. Methoden zur probabilistischen Sicherheitsanalyse für Kernkraftwerke
Facharbeitskreis Probabilistische Sicherheitsanalysen für Kernkraftwerke BfS-KT-16/97, BfS Salzgitter, 1997
3. Gesellschaft für Reaktorsicherheit (GRS) mbH
Deutsche Risikostudie Kernkraftwerke Phase B
ISBN: 3-88585-809-6, 1990

4. Kreuser, A.; Peschke, J.
Common Cause Failure-Model with Consideration of Interpretation and Projection-
Uncertainties
Jahrestagung Kerntechnik 1997
Aachen, 13 - 15. Mai 1997
5. Kreuser A.; Peschke, J.; Versteegen, C.
Consideration of Interpretation Uncertainties in the Determination of
Common Cause Failure Probabilities
PSAM 4
New York City, USA, 1998
6. Hofer, E.
On two-stage Bayesian modelling of initiating event frequencies and failure rates
Tecnote
Reliability Engineering and System Safety 66, 1999, S. 97-99
7. Hofer, E.; Peschke, J.
Bayesian modelling of failure rates and initiating event frequencies
Proceedings of the European Conference on Safety and Reliability (ESREL),
Garching, Germany, 13.-17. September 1999
8. Untersuchungen der Sicherheitsreserven von Kernkraftwerken bei auslegungs-
überschreitenden Ereignisabläufen
GRS-A-2588, April 1998
9. Müller-Ecker, D.
The PSA approach for the safety assessment of low-power and shutdown states
Eurosafe 2000, Cologne, 6./7. November 2000
10. Löffler, H.; Sonnenkalb, M
Correlation of initiating events with the PSA Level-2 results
Eurosafe 2000, Cologne, 6./7. November 2000