Probabilistic Safety Analysis for the Post-Operational Phase

Gerben Dirksen[a*], Christine Bell[a], Heiko Kollasko[a]
[a] Framatome GmbH, Erlangen, Germany

Abstract: As more and more nuclear power plants reach the end of their operational lifetime, the post-operational phase increasingly moves into focus. The fuel damage frequency can be evaluated using probabilistic safety analyses (PSA). The main configuration of interest during the post-operational phase is the core fully unloaded and spent fuel stored in the spent fuel pool. PSA can be used to evaluate the safety level of the plant as long as there is fuel on site.
This paper focuses on the function residual heat removal from the fuel elements in the fuel pool.
The methodology presented in this paper takes into account the effects of decay heat decrease in the spent fuel pool as a function of time. The results of a probabilistic evaluation can be significantly improved by considering the time dependent effects of the continuous decrease of the decay heat on the grace period for recovery actions.

It shall be demonstrated that safety margins increase with decreasing decay heat, and from a PSA point of view, the fuel damage frequency decreases significantly over time.

This analysis can be used in particular to justify a reduction of the number of safety systems to be kept available as a function of time during the post-operational phase. This could lead to a significant cost reduction during the post-operational phase.

Keywords: Spent fuel pool, long term PSA

1. INTRODUCTION

As more and more nuclear power plants reach the end of their operational lifetime, the post-operational phase, i.e. the phase when the plant is decommissioned, increasingly moves into focus. As long as fuel remains on the site, PSA- methods should still be used to assess the remaining risk of fuel damage. The main configuration of interest during the post-operational phase is the one with the core fully unloaded and spent fuel stored in the spent fuel pool. The major costs for the operator are related to the maintenance of the safety systems. In this case, the PSA can provide insights on the risk of fuel damage as a function of the number of safety systems installed.

The post-operational phase is characterized by the absence of fuel in the RPV and by long grace periods due to the decreasing decay heat in the fuel elements stored in the spent fuel pool. In contrast, the grace periods in the PSA for the normal operation phase (power and shutdown states) are typically much shorter. The longer grace periods allows more reliable human actions and more possibilities to recover mitigation measures unavailable at the time of the initiating event. To use the PSA for assessment of fuel damage risk during the post-operational phase, adaptions must be made to the PSA to meet the altered conditions.

In many previous PSA for the post-operational phase [1,2], the decay heat has been assumed to be constant corresponding to its value at the start of the analysis. However, due to the significant increase of the grace period with decreasing decay heat, this assumption is very conservative.

A case study PSA for the post-operational phase is presented in this paper, which evaluates the fuel damage frequency as a function of the time elapsed after the core unloading. It will be demonstrated

[*] Gerben.Dirksen@Framatome.com

that after reactor shutdown, PSA can be used to show that the risk of fuel damage decreases significantly over time.

Such an analysis can be used in particular to justify that only the necessary safety systems are kept available, potentially reducing the number of systems as a function of time during the post-operational phase. This could lead to a significant cost reduction during the post-operational phase.

1.1 Comparison between Shutdown PSA and Post-operational PSA

Existing shutdown PSAs include the phase when the RPV is empty and all fuel elements are situated in the fuel pool. As this state is very similar to the plant state in the post-operational phase, the modelling of this phase can be used as base line case for the PSA for post-operational phase.

There are however several differences between shutdown PSA and a PSA for the post-operational phase. The shutdown PSA considers a period of several weeks, whereas the PSA for post operation considers the fuel elements stored in the spent fuel pool during the whole year while the decay heat is steadily decreasing. Therefore, scaling the results from the shutdown PSA to a whole year gives an overly conservative result.

Therefore, to reach meaningful results, the methodology shall take into account the time elapsed since reactor shutdown, which has an effect on the decay heat and from that on the grace periods in the PSA. In case of long grace periods, the PSA results can be significantly improved by including dynamic elements to properly evaluate the effects of the reduced decay heat.

1.2 Post-operational phase PSA case study

In the following a case study PSA for the post-operational phase is presented. The case study is based on an existing shutdown PSA of a 4-loop German PWR that has been expanded by dynamic elements to take into account the post-operational conditions. The following dynamic elements have been added:

- Time-dependent probability of taking trains which are in maintenance into operation.
- Time-dependent probability of repair of failed components.
- Human error probabilities dependent on the grace period available to conduct the operator action.

The analysis has been performed based on fault tree and event tree analyses, that is, without any specific tools for dynamic PSA.

The result is the fuel damage frequency as a function of the time elapsed after core unloading. It will be demonstrated that safety margins increase with decreasing decay heat, and from a PSA point of view, the fuel damage frequency decreases significantly over time.

2. MODELING ASSUMPTIONS

The modeled plant is a 4-loop pressurized water reactor (PWR) whose spent fuel pool is located inside the containment. In addition, low pressure injection can be used in fuel pool cooling mode.

The following initiating events are analyzed:

- Loss of Off-Site Power (LOOP)
- Loss of Residual Heat Removal (LORHR)

Initially, the following systems are available for spent fuel pool cooling to keep the spent fuel pool stable in a safe state:

- Two identical fuel pool cooling trains (FP1, FP2)
- Two identical low pressure injection trains which can be used in fuel pool cooling mode (LP1, LP2).

FP1 and LP1 can be cooled by one of two residual heat removal trains (RH1, RH2). Similarly FP2 and LP2 can be cooled by one of two residual heat removal trains (RH3, RH4).

One functioning cooling chain systems can be used to establish the closed-loop cooling of the SFP.

If the closed-loop cooling fails, the fuel pool can be flooded either using the demineralized water or with a mobile fire water pump. However, these options only inject water into the containment, which would lead to excessive containment loads. Therefore for open-loop cooling, containment depressurization shall be performed.

2.1 Analysis Dependent on Grace Period

Two important time points are considered in the analysis:

t_1: Time until the fuel pool water level is below the fuel pool cooling suction line. After this time, the closed-loop cooling is no longer possible.

t_2: Time until the fuel pool water level reaches the top of active part of the fuel elements. After this time, the fuel damage is assumed.

Based on the available water volume in the SFP, for the analyzed plant it can be considered that $t_2 \approx 4\ t_1$. This relation between the grace periods is assumed for the analysis. At the start of the post-operational phase, $t_1 = 8$ hours and $t_2 = 32$ hours.
The relation between grace periods t_1 and t_2 and the time after reactor shutdown is shown in Figure 1 below.

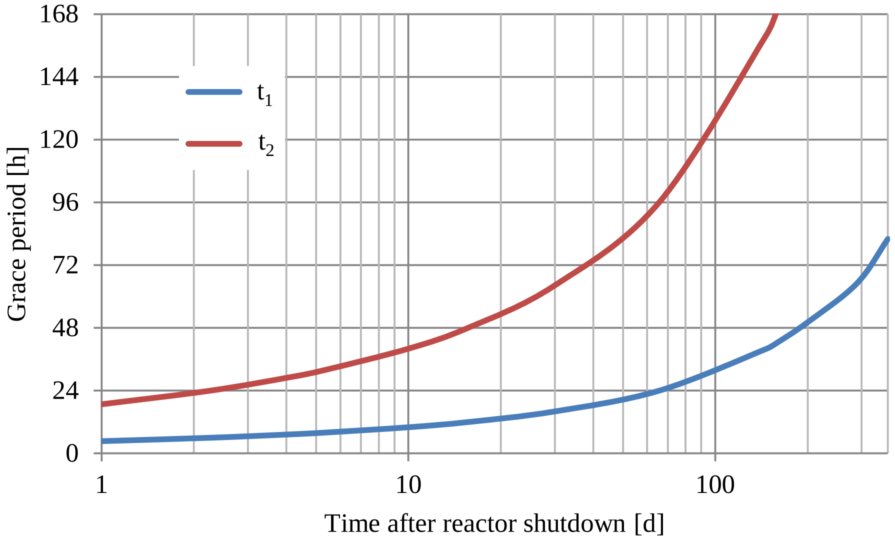

Figure 1: Relation between grace periods and time after reactor shutdown

Note that approximately 5 days after shutdown, the time until the suction line is uncovered t_1 is equal to 8 hours. This is considered as the starting point of the analysis. After approximately half a year after shutdown (approx. 180 days), the time until fuel damage occurs if the cooling of the fuel elements in the fuel pool is not recovered, has increased to 1 week. This marks the end of the analysis, as the grace period is now significantly longer than the repair period, the mission time and human action grace periods.

2.2 Human Reliability Modeling

As the recovery of fuel pool cooling requires manual countermeasures, the assessment of the human reliability is a key factor of the analysis. The human actions evaluated in this analysis are performed using the THERP method [3]. The probability of human error decreases with the increasing grace period available to conduct the action. The impact of the increasing grace period on the failure probability of the human action can be subdivided into several factors:

Increase of diagnosis time:

> The available diagnosis time is a major factor in the evaluation of human reliability. The THERP method gives a median diagnosis error of 1.0E-04 for a grace period of 60 minutes, which decreases to 1.0E-05 for a grace period of 25 hours (Table 20-1 in [3]).

Human action recovery:

> After the diagnosis has been made correctly, the operator performs the required action and its effect on the plant can be evaluated. If the required action is not performed in the foreseen time but the grace period allows a repetition, the action can be performed again (recovery actions), for example using a different train or system and performed either by the same or a different operator.

Shift change:

> If the grace period exceeds the length of one shift, a second shift will have the opportunity to recover a non-successful action performed by the previous shift.

As the grace period increases, dependencies between different human actions and their potential recovery decrease. Nevertheless, it is noted that even considering all these effects, there is a limit to the total human reliability that can reasonably be assumed in PSA. As the assumed failure probability for human actions decreases, more intangible factors will become relevant. For this reason, the analysis ends six months after reactor shutdown, for which the grace period can be considered to be one week (see Figure 1). After this time, no increase in the total human reliability is assumed.

2.3 Duration of the LOOP

A LOOP event is generally a condition with a limited duration of the loss of electrical power supply itself. The probability that a LOOP ends before either t_1 or t_2 are reached increases as the grace period increases (see for example [4] Figure A.1). In the analysis, it is assumed that the LOOP ends after 24 hours (a short-term LOOP is not relevant for the analysis as the grace period is under all circumstances longer than 2 hours). It is noted that in the analyzed plant, fuel pool cooling can be supplied by the emergency power supply system.

2.4 Availability of Systems

As decay heat can be removed by one train, the other trains are considered to be in standby. After a failure of the first train, one of the remaining stand-by trains can fail to start or to run without affecting the availability of the residual heat removal system. In addition, there may be common cause failures (CCF) between redundant components of identical trains.

With increasing grace period however, there are several other possibilities, which improve the availability of the residual heat removal system such as:

- Taking a train in maintenance back into operation
- Repairing a failed train.

For the present analysis, it is assumed that a train in maintenance can be returned into operation within 10 hours. For the initiating event LORHR, a mean time to repair of 24 hours is considered (lognormal distribution with an error factor of 5).

For systems modeled in the fault tree analysis, the effect of repairing is considered by reducing the CCF potential between the train in operation and the trains in standby for large grace periods.

4. QUANTIFICATION RESULTS

Quantification of the fuel damage frequency has been performed for the following grace periods t_1:

- 8 hours – initial grace period at the start of the post-operational phase.
- 10 hours – components in preventive maintenance can be repaired before the end of the first grace period t_1.
- 16 hours – decreased CCF potential and increased recovery potential for failed human actions.
- 24 hours – LOOP is considered to have ended before the end of the first grace period t_1.
- 40 hours – final grace period at the end of the analysis.

The PSA results are shown in Figure 2, each point corresponding to a specific grace period t_1.

In addition to the analysis with four trains for the fuel pool cooling (FP1, FP2, LP1, LP2), also sensitivity analyses are performed assuming three (FP1, FP2, LP1) and two (FP1, LP1) trains available.

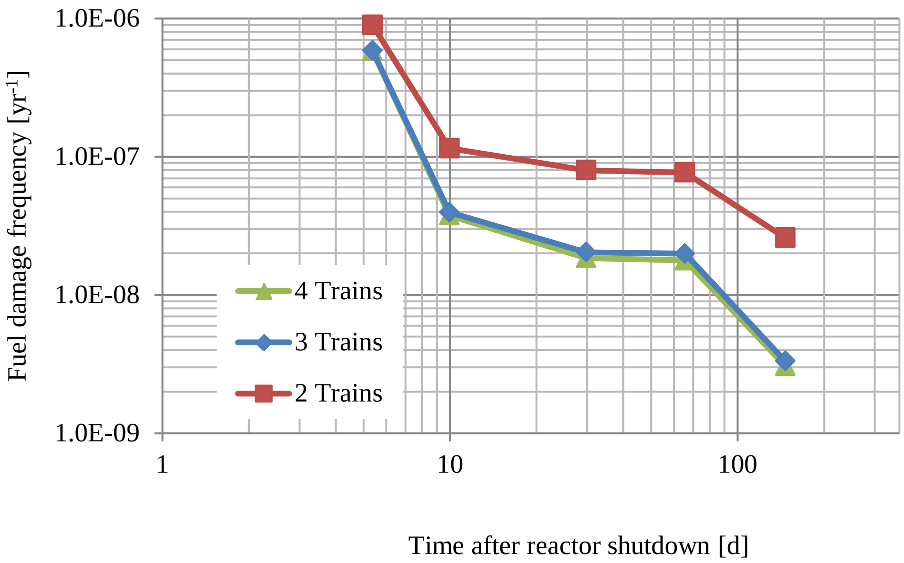

Figure 2: Fuel damage frequency as a function of time after reactor shutdown and number of trains available

It can be seen that the largest risk reduction is reached with t_1 between 8 and 10 hours. This is mainly due to the assumption that a train in preventive maintenance can be taken into operation within 10 hours.

The second largest effect is reached with t_1 between 24 and 40 hours. This is mainly due to the reduced CCF potential (not only for the fuel pool cooling trains but also for supporting systems) for 40 hours grace period.

With respect to system unavailability compared to human error probability, in this case study the increase in grace period from 8 hours to 40 hours has a larger effect on the system unavailability, as human actions with grace periods of significantly above one hour are already evaluated with a low failure probability.

Furthermore it is observed that reducing the number of trains from four to three has only a small effect on the fuel damage frequency. Reducing from three trains to two trains has a large effect on the fuel damage frequency. Nevertheless, after 6 months the fuel damage frequency with two trains is lower than the fuel damage frequency after 10 days with three trains.

4.1 Equipment Reduction Potential

The post-operational PSA can also be used to justify a reduction of the number of safety systems to be maintained. For this purpose, a PSA-based safety goal can be defined. If for example, the studied plant defines a safety goal, e.g. the fuel damage frequency must be below 5E-08 / year for the post-operational phase, the PSA would recommend reducing the number of trains to three after 10 days, and to two after 6 months.

Although the analysis was limited to the reduction of the number of trains of front line systems, the analysis can be extended to all supporting systems. For example, the PSA can be used to show that the number of standby emergency diesel generators may also be reduced.

The extension of the analysis beyond 6 months after reactor shutdown is unlikely to provide more insights. Indeed, from classical PSA one might come to the conclusion that there is no more risk for fuel damage after this time. However in this case, common sense will still require the availability of at least one safety system for the fuel pool cooling as long as there is any potential for fuel damage.

4.2 Active Risk Management During the Post-Operational Phase

As it can readily be observed from the results, the shutdown PSA results are highly conservative when the decay heat is significantly reduced. Therefore, it is advantageous to use a dedicated model for the post-operational phase that shall also be used in risk monitoring, as the conservative shutdown PSA model may lead to misleading conclusions.

5. CONCLUSION

A PSA case study for the post-operational phase of a nuclear power plant, using dynamic effects in a static PSA model using only fault trees and event trees, has been performed. It can be seen that simply applying the analysis of the shutdown PSA during operation to the post-operational phase is extremely conservative. Due to the increasing grace periods, the fuel damage frequency is significantly reduced. For the analysed plant configuration, a reduction of the number of safety systems required to be kept available can be justified in the long term during the post-operational phase using the PSA results. This could lead to significant cost reductions while keeping the fuel damage risk below acceptance limits.

References

[1] D. Mercurio et al. "*Integrated Level 1 – Level 2 decommissioning probabilistic risk assessment for boiling water reactors*", Nuclear Engineering and Technology 50, 627-638 (2018).
[2] "*Gutachten zum Stilllegungsprojekt des Kernkraftwerks Mühleberg*", ENSI 71/39 (2017).
[3] A.D. Swain, H.E. Guttmann. "*Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications*", NUREG/CR-1278 (1983).
[4] "*PSA Methodology*", European Utility Requirements for LWR Nuclear Power Plants, Volume 2, Chapter 17, Rev. B (1995).