Enhancing Realism in a Spent Fuel Pool PSA: Incorporating the I&AB Method for Dynamic Repair Modelling and Realistic Mission Time Analysis

Anders Olsson[a*], Frida Olofsson[b]
[a]Vysus Group, Malmö, Sweden
[b]RiskSpectrum, Stockholm, Sweden

Abstract: The PSA of the spent fuel pool facility is evaluating the risk of boiling in the pool. Repair of certain components in the cooling system is modelled, which is important from a result perspective. Looking at the interpretation of a MCS containing a repair event, it can be concluded that the static PSA representation does not capture the dynamic features associated in a realistic manner. Consequently, this representation is associated with a great amount of conservatism. Another issue is the assigned mission time for the cooling system, which is derived from deterministic criteria, and an important contributor to the results. As the aim of the PSA is not aiming to verify deterministic design criteria, but rather to be a realistic representation of the spent fuel pool process and its safety functions, a question that consequently arises is; "What is the appropriate realistic mission time that should be used"?

To address these issues, the RiskSpectrum I&AB (Initiators & All Barriers) method has been incorporated in the PSA. An advantage of the I&AB method compared to the traditional static PSA approach is that it accounts for the fact that different types of initiating events can have different repair times. This means that the time window within which other safety functions must act to prevent an undesired consequence will also be different for each scenario. Furthermore, a main feature of the method is that it credits the dynamic aspects of repair processes, which introduces a more realistic representation than a static PSA approach. A method has been developed to estimate repair times with a higher level of detail and including a broader scope of component types and failure modes. The repair time data together with the I&AB method has been implemented in the PSA model for internal events and internal hazards (fire and flooding).

This new approach did not only enhance the realism of the model but also enabled the extraction of valuable insights and information, such as importance measures of repair times for different components, which can inform decision-making and optimize repair and maintenance routines. This paper is a continuation of the work presented at the ESREL conference in September 2023.

Keywords: PSA, Spent Fuel Pool, Mission Time, Dynamic Repair Modelling

1. INTRODUCTION

This paper aims to provide an overview of the PSA of a SFP facility and how implementing dynamic modelling of repair greatly improved realism. As a result, the model has been enhanced to a level where it is now possible to evaluate various aspects of repair through applications using the PSA.

This paper builds upon the work outlined in F. Olofsson & A. Olsson. (2023) which describes the initial phase that included internal initial events. In the subsequent phase of the works, that is also included in this paper, the scope was extended to also include the internal hazards fire and flooding.

Chapter 2 gives a brief introduction of the facility and the PSA. One of the main challenges related to modelling the SFP facility's safety performance is the long time window in some of the sequences. In Chapter 3, these challenges are briefly explored.

The implementation of the I&AB methodology as a solution to challenges is described in Chapter 4 as well as how repair times were derived for a large number of components in the model.

Lastly, in Chapter 5 the results from the updated model is presented. The updated PSA show a decrease in risk, as well as change in ranking of sequences.

The improvements made to the model make it a suitable tool for evaluating various aspects of repair in the facility which will contribute to better decision-making regarding safety aspects of the SFP facility.

2. GENERAL OVERVIEW

2.1. Description of the facility

The studied facility is an interim storage facility which primary purpose is to store spent fuel generated by various NPPs in storage pools before disposal in the final repository. The fuel is handled in two separate processes. Firstly, the spent nuclear fuel arrives and is properly prepared to be placed in the interim storage pool. Secondly, the interim storage pool itself where the spent fuel is kept cooled and under observation waiting for the final repository.

When the transport container with the spent fuel arrives at the facility it must first be cooled. The transport container is placed in a cooling cell where water cooling systems are connected to the container. Next, the transport container is transported via a bridge crane into a pool in which the process of unloading the fuel elements and placing them in a storage canister takes place.

The storage canister is transported underground to the long-term storage pools. The fuel is then kept in these pools about 30 meters below ground and covered with eight meters of water. An overview of the fuel handling process through its way in the facility is shown in Figure 1.

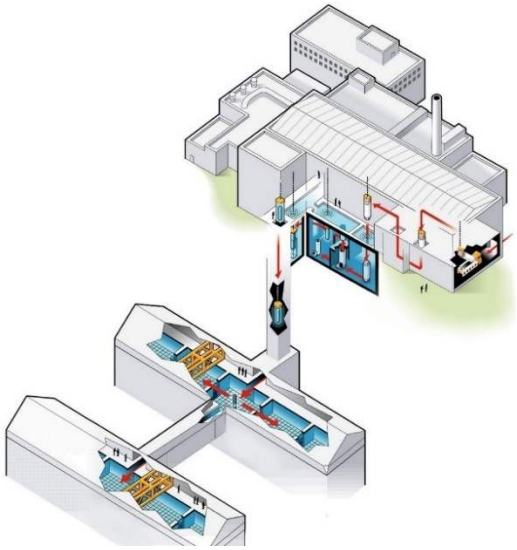

Figure 1. Overview of the fuel transportation process

2.2. General overview of the PSA

The PSA evaluates the risk both related to the process of the containers´ transport and fuel elements handling, as well as the long-term storage in spent fuel pools.

The operation is divided into different modes depending on where the fuel is located:

- *Storage* – No handling of fuel is in progress, but all fuel is located in the long-term underground storage pool.
- *Temporary storage* – No handling of fuel is in progress, but fuel is located in the intermediate pools above ground in the facility.
- *Operation* – Handling of fuel in any of the process steps.

Relevant initiating events are dependent on where in the facility the fuel is located. The analysis is divided into eight process steps following the fuel on its way through the process. In each step of the process the specific relevant initiating events are identified. Internal events, internal hazards (fire and flooding) and external hazards are covered.

The studied end-states and sequences are also dependent on which process step the fuel is in. The main consequences studied in the model are mechanical damage to fuel, overheating of fuel or uncovering of fuel as they can potentially lead to radioactive releases. In addition, another end-sate that is studied is boiling in the storage pool.

Due to the low grade of automatization and redundancies, the human actions are an important part of the PSA. Available time for recoveries and repairs is, generally, long in many of the studied sequences. HRA are performed with ASEP (NUREG/CR-4772, 1987) for category A and B actions and SPAR-H (NUREG/CR-6883, 2005) for category C actions.

3. CHALLENGES WITH THE STATIC PSA REPRESENTATION

Sequences that expand over a longer time frame brings several new aspects of modelling that will play a more important role in the SFP PSA compared to the NPP PSA

In traditional NPP PSAs, time frames of 24 hours for level 1 and 48 hours for level 2 are commonly considered (IAEA SSG-3, 2010, objective 5.49). These time frames are assumed to cover the time it takes to bring back the plant to a safe state and are therefore used as fixed mission times in the PSA, regardless of the specific initiating event that is analysed.

However, it can be acknowledged that the time it will take to bring the plant to a safe state after an initiating event is very likely dependent on what initiating event that has occurred. Consider for example two scenarios: one where there's a component failure, such as a spurious stop of a pump, and another involving a usually more severe and complex event like fire or flooding. The sequence of actions to restore the facility to its initial state is likely to vary significantly in terms of time required.

Another aspect that comes more into play for the SFP are the longer time window between the complete failure of barriers and the analysed end states. In the case of SFP sequences, the time windows are very extensive, often lasting several days, which allows plenty of time for recovery and repair actions. The model updates described in this paper have been focused on sequences related to the loss of cooling in the SFP and the subsequent boiling in the SFP, as these sequences have the longest time windows.

3.1. Repair

Crediting repair has a significant impact on the results. Looking at the interpretation of a MCS containing a repair event, it can be concluded that the static PSA representation does not capture the dynamic features associated with a repair process in real life. Consequently, this representation is associated with a great amount of conservatism as well as some potential optimistic assumptions.

One main dynamic feature that is not captured in a static PSA is the fact that a component can fail and be repaired several times during long time windows. Furthermore, a component may run for some time before it fails, which allows extra time for other actions or repairs during that time.

The previous approach to model repair and its challenges are discussed in more detail in Olofsson & Olsson (2022).

3.2. Safe State

A corollary of the previous static approach to repair modelling was that if a repair successfully re-established one train of the cooling system, it was considered a safe state. However, it's important to note that the system state after a successful repair may differ from the state just prior to the initiating event with respect to the risk level. Consider the following example:

The initiating event is a loss off off-site power (LOOP), which causes the emergency diesel generator (DG) to start and supply power to the SFP cooling system pumps. The diesel generator subsequently fails due to a spurious stop. If no actions are taken, this state will eventually lead to boiling in the storage pool.

In the static PSA, if we credit repair for the diesel and the repair is successful, this is considered a safe state. This means we are in a state where the diesel generator supplies power to the SFP cooling system, which is clearly not the same and may not be similar or comparable conditions as to the ones prior to the initiating event.

The key question that needs to be answered to determine the risk level of this state is; *What is the likelihood of the emergency diesel (or other critical components) failing again before the external grid is restored?* Hence, by overlooking to address this question, the static approach may be overly optimistic and fail to accurately assess the potential risks involved.

3.3. Mission time

The assigned mission time for the SFP cooling system is currently set to 30 days, which is derived from deterministic design criteria. As can be expected, sensitivity analysis reveals that this mission time significantly influences the PSA results.

As the aim of the PSA is not to verify the deterministic design criteria, but rather to be a realistic representation of the spent fuel pool process and its safety functions, a question that consequently arises is; what is the appropriate realistic mission time that should be used?

4. MODEL ENHANCEMENTS

To address the above discussed challenges the I&AB method was implemented in the PSA. As a part of this update the repair modelling was significantly enhanced by extending the scope of components considered and refining the estimation process of repair times to a higher level of detail.

4.1. Initiators & All Barriers (I&AB)

The I&AB methodology is developed and described by M. Bouissou et al. (2014). Implementation of the methodology in RiskSpectrum PSA was subsequently performed by O. Bäckström et al. (2016).

In short, I&AB is a methodology for calculating the reliability of repairable and reconfigurable systems. The method is also extended with possibility to credit grace times and deterministic times. A grace time is defined as the time between a certain event and the point in time when the undesired consequence will occur. During this time window it is possible to initiate actions and repairs to avoid the consequence. A deterministic time refers to a function that has the ability to “buy” a finite amount of additional time, similar to a water tank with a finite amount of water or batteries which can supple power for a limited time period.

The I&AB methodology relies on two key approximations. The first approximation assumes that when an initiating event occurs, all standby components will immediately start functioning, or alternatively refuse to start, after the initiating event. Once activated, these components may fail and be repaired independently from each other until the initiating event is successfully repaired.

The second approximation assumes that once an initiating event is repaired, the system cannot fail again. This means that when the initiating event is repaired, the facility is considered to be in a safe state.

An early pilot study applying the I&AB methodology on the SFP facility in question was performed by A. Olsson (2016). The I&AB method has also been applied in various pilot studies within the joint Nordic research project PROSAFE (2019-2020).

4.2. Repairable components screening

The screening process for important components covers two types of component failures: initiating events and barrier failures (i.e. failure of systems functions that act as barriers once the initiating event has occurred). All component failures that are modelled as initiating events are included. For barrier failures, a screening process is conducted to identify basic events with importance measures fulfilling either FC (Fractional Contribution) > 0.5% or RIF (Risk Increase Factor) >2.

A total of 188 basic events were identified. In the next step 35 of those basic events were screened out due to inapplicability of repair. This was for example CCF-events (Common Cause Failures) or manual actions. Repair for CCFs is handled directly through basic events if they are part of a CCF-group, hence specific CCF-events does not have to be assigned with a repair time separately. Recovery of manual actions are already handled in other ways in the model. The screening process can be iterated if needed once the model is updated.

For fire and flooding events the initiating events may involve damage to multiple components and cables. Other aspects connected to the impact from the fire or flooding on the facility itself needs to be considered as well. The barrier failures are similar with those for internal initiating events, with possible additional aspects that may be different due to the sequence following the specific fire- or flooding event.

The result of the screening is a list of components with information about which type of failure (initiating event or barrier failure) and the failure mode, as the repair time can be different depending on those factors. For fire and flooding, also scenarios for each initiating event including damage of multiple components within the affected part of the facility is listed. The next step is to assign repair times to these failure events.

4.3. Estimating repair times

A methodology was outlined and applied to estimate repair times. The total repair time for a component is divided into five time intervals defined as follows:

- **Failure detection** - The time between the initiating event and detection of the fault.
- **Diagnosis** - The time between detecting a fault and determining the cause for the malfunction, as well as making a decision on what actions or measures to take. This may for example include reporting the fault to the maintenance department.
- **Call-out time** – The time between reporting a fault until maintenance personnel arrive on site.
- **Troubleshooting** - The time needed from the maintenance personnel to identify the root cause of the fault and to decide how to conduct the active repair.
- **Active repair** - This step refers to the active repair time of the component, which involves several tasks such as shutting down the system, conducting the actual repair, restoring the system to operating condition, and restarting it. Repair can also involve alternative measures that enable the system to be restored and restarted, returning the facility to a safe state. For instance, if a fault is due to some kind of I&C related failure the I&C system can be bypassed and replaced by manual control and supervision.

Figure 2. illustrates the time intervals for an example scenario in which a pump in the A train experiences a spurious stop, which also represents initiating event. This is followed by a barrier failure which is another spurious stop in a pump located in the B train. The figure highlights the various time intervals involved in the repair process.

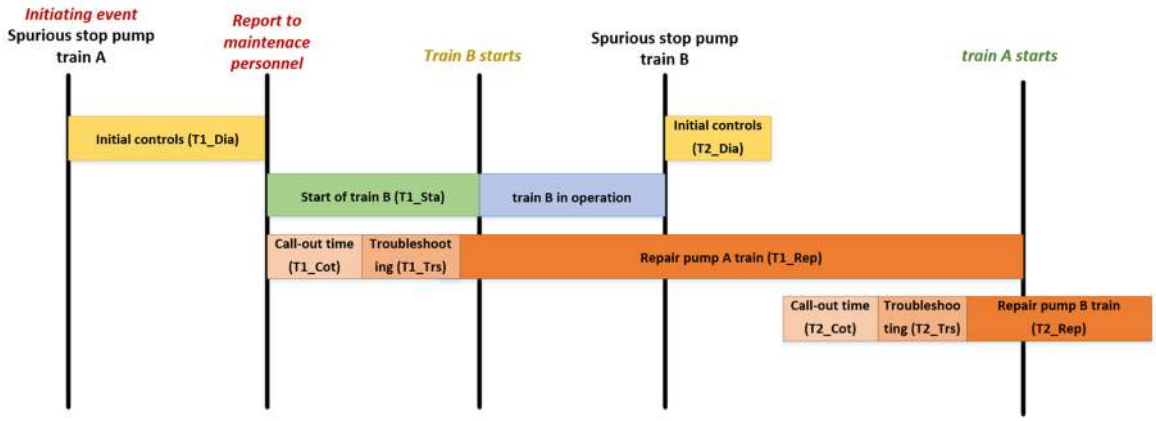

Figure 2. Illustration of the different time intervals for an example with spurious stop for a pump in the A train as an initiating event followed by a barrier failure with a spurious stop of a pump in the B train.

For the initiating event, the following applies:

- Failure detection is assumed to be immediate after the initial event. If the operating train in the cooling system stops, an alarm is triggered.
- The total repair time thus consists of diagnosis, call-out time, troubleshooting and active repair. These times are illustrated in Fig. 2 (T1_Dia + T1_Cot + T1_Trs + T1_Rep).

For the barrier failure, the following applies:

- The failure detection will occur at a certain time after the initiating event. The failure detection occurs either when attempting to start up the B train or when it stops due to a malfunction after a certain time in operation. The time that has passed before the failure detection is the time for diagnosing the first fault and the time for switching over and starting the standby train. These times correspond to T1_Dia and T1_Sta in Fig. 2. This is true regardless of whether the standby train starts and operates for a certain time before the fault occurs or if the fault occurs at startup. The time that the standby section may be in operation should not be counted in the repair time since cooling is provided during that time.
- The total repair time thus consists of failure detection, diagnosis, call-out time, troubleshooting and active repair time. These times are illustrated in Fig. 2 (T1_Dia + T1_Sta + T2_Dia + T2_Cot + T2_Trs + T2_Rep).

The process of estimating repair times and the separate time intervals is done with input from both operational and maintenance personnel through interviews. In addition, maintenance personnel maintain detailed documentation on the estimated active repair time for a wide range of components that serves as a valuable source.

As a starting point, the same time intervals should also be taken into consideration for fire/flooding scenarios, with the addition of a few more specific aspects that must be taken into consideration. One main difference is, for instance, that the diagnosis may be more complex and also involves other personnel such as the fire brigade. Moreover, the active repair time is likely to be more complex as the initiating event may have caused damage to multiple components. In the case of flooding there may also be a need to isolate or repair a pipe break. Thus, the active repair time for all necessary equipment in total has to be estimated.

The estimated repair times are subsequently used as the “Sequence MTTR” (mean time to repair) parameter in the I&AB module within RiskSpectrum PSA.

5. RESULTS

The I&AB method together with the new repair time data was implemented in the model for internal initiating events as well as the internal hazards fire and flooding.

The frequency for the consequence boiling, represented by internal initiating events, in the SFP decreased in total with 98 %. The main reason for the significantly lower results is the implementation of the I&AB calculation method with the dynamic representation for the repair processes. Hence, the main reason to the decrease is removing conservatism and having a more realistic representation for sequences that extends over a long time window. The second factor that affected the results is also modelling repair for a wider range of components. Apart from a lower boiling frequency some changes in the ranking of sequences was also observed.

For the internal hazard fire, the boiling frequency decreased with 14%. While the boiling frequency did not change significantly, there are major differences in ranking for individual fire scenarios. In general, the updated fire analysis reveals that in scenarios similar to those involving internal events, where only one train is affected by an initiating event, the extended available time and possibility to credit repair makes a very strong barrier against boiling. The predominant contributors to boiling from a fire event are cases where both trains are affected by fire. The difference in ranking of sequences is mainly due to the more realistic treatment of the I&AB calculations that considers dynamic repair aspects. It can thus be shown that taking these dynamic aspects into account significantly reduces the contribution to the boiling frequency for certain sequences.

The conclusions and insights are similar for flooding where the boiling frequency decreased with 38 %.

The main conclusion from the overall results is that the facility is very robust against boiling in scenarios where only one train is affected. Thus, initiating events impacting only one train with strict sub-separation represent a small fraction of the contribution to the total boiling frequency. Fire and flooding events affecting equipment in both trains are the ones that are most significant.

The total results for fire and flooding are expected to decrease in the future as some conservative assumptions and simplifications were made in this first implementation of I&AB.

The updated PSA for internal events was also used in an application where different design solutions to strengthen the SFP cooling function where evaluated. It could be concluded that compared to other types of measures, such as the introduction of new safety systems or the strengthening of physical barriers, the impact of organisational measures which can reduce the repair times may be just as significant, particularly for a facility like this where the time window (Grace Time) between the initiating event and the undesired consequence (boiling) is long.

The methodology for estimating repair times will undergo further development in the upcoming phases of the PSA update. The focus will be on refining aspects such as concurrent repairs, including the availability of maintenance personnel and spare parts, as well as dependencies between repair tasks. The identification, quantification and evaluation of various uncertainties will also be included in the future development of the PSA.

6. CONCLUSIONS

The implementation of the I&AB calculation method in the SFP PSA has greatly increased the realism of repair modelling in the sense that both conservatisms and potential non-conservatisms associated with the modelling of repair and mission times have been reduced with the dynamic features in the I&AB methodology. In principle, the I&AB methodology allows for critical components to fail and be repaired as many times as the defined time window (Grace Time) allows.

Improvements were conducted in the repair modelling by extending the scope of components considered for repair as well as the level of detail of estimating repair times. The level of detail in the repair modelling is now at a level where the PSA can be used to various applications to evaluate different aspects of repair. One example is to identify important repairs and communicate these with maintenance personnel. It is also possible to evaluate the impact of organisational measures such as maintenance and repair strategies including readiness of the maintenance organization.

It is important to recognize that organizational measures are not a replacement for physical safety barriers and other engineering controls, but rather should be used in conjunction with them to create a comprehensive safety management system.

References

F. Olofsson & A. Olsson. (2023). *Enhancing Realism in a Spent Fuel Pool PSA: Incorporating the I&AB Method for Dynamic Repair Modelling and Realistic Mission Time Analysis*. Paper #523 at ESREL2023

A. Olsson. (2018). *Leaving mission times backstage and taking repair into account in long term scenarios*. Paper #145 at PSAM14

IAEA SSG-3 (2010), *Development and Application of Level 1 Probabilistic Safety Assessment for Nuclear Power Plants*

F. Olofsson & A. Olsson. (2022). *Challenges and Lessons Learned from a PSA on a Spent Fuel Pool*. Paper #99 at PSAM16

M. Bouissou, O. Hernu. (2016). *Boolean approx-imation for calculating the reliability of a very large repairable system with dependencies among components*. ESREL 2016 proceedings, (ISBN 978-1-138-02997-2)

NUREG/CR-4772 (1987). *Accident Sequence Evaluation Program,* Open resource.

NUREG/CR-6883 (2005). *The SPAR-H Human Reliability Analysis Method*, Open resource.

O. Bäckström, M. Bouissou, et.al. (2018). *Intro-duction and Demonstration of the I&AB Quantification Method as Implemented in RiskSpectrum PSA*. Paper #203 at PSAM14.

PROSAFE (2019-2020). *Prolonged Available Time and Safe State.* Joint research project between Nordic PSA Group, NKS and the SAFIR programme.