NKS-444
ISBN 978-87-7893-536-6

Prolonged Available Time and Safe States

Tero Tyrväinen[1]
Ilkka Karanta[1]
Terhi Kling[1]
Xuhong He[2]
Frida Olofsson[2]
Salvatore Massaiu[3]
Erik Sparre[4]
Carl Eriksson[4]
Erik Cederhorn[4]
Stefan Authén[4]

[1]VTT Technical Research Centre of Finland Ltd
[2]Vysus Sweden AB/Lloyd's Register Consulting – Energy AB
[3]IFE (Institute for Energy Technology), Norway
[4]Risk Pilot AB, Sweden

February 2021

Abstract

Definitions for accident states and safe states are decisive for both deterministic and probabilistic safety assessments (DSA & PSA) of nuclear facilities. For instance, the IAEA's guides on the performance of deterministic and probabilistic safety assessments state that determination of mission times should take into account the time it takes to reach a safe, stable shutdown state. Fundamentally, it is a matter of finding an appropriate balance between the level of realism of models and practicality of the modelling approach. One cross-cutting modelling issue in this respect is the choice of mission time and related success criteria for systems, and the possibility to realistically include recovery and repair for long time windows. In DSA, it is often adopted from the previous praxis justifying what is sufficient. In PSA, the modelling approach itself forces to simplify treatment of mission time, and repairs are mostly not considered.

Use of single time window simplifies modelling, but in the light of occurred events (Fukushima Daichii), implementation of new technology in the nuclear power plants (e.g. independent core cooling), consideration of non-reactor nuclear facilities (e.g. spent fuel pools) and decommissioning phase reactors, such a simplified approach may need justification and/or to be reconsidered. In any case, the definition of a mission time is dependent on the definition of safe and stable state.

Since selection of mission time has an impact on many modelling aspects, and hence on the PSA results, it is important to study possibilities to treat mission times more realistically. For longer time windows, it becomes evident to consider e.g. time-dependent success criteria and possibilities for recovery and repair. However, for these issues there is not yet a consensus on how they should be addressed.

The PROSAFE project started 2019 with financial support from NKS, NPSAG and SAFIR, with the objective to improve the quality of safety assessment methods with respect to safe and stable state definition and assessment of long time windows, including human reliability analysis in long time window scenarios, use of dynamic success criteria, crediting repairs and modelling of different time windows.

This report presents the second and final phase of the project which was performed during 2020. Although further work is needed within several of the investigated areas, PROSAFE have provided important findings and some of the keys needed for a more realistic consideration of long time windows in future PSA:s.

Key words

PSA, HRA, Mission Time, Repair, Long Time Windows, Safe State, Dynamic Success Criteria.

NKS-444
ISBN 978-87-7893-536-6
Electronic report, February 2021

NKS Secretariat
P.O. Box 49
DK - 4000 Roskilde, Denmark
Phone +45 4677 4041
www.nks.org
e-mail nks@nks.org

Prolonged Available Time and Safe States

Final Report from the NKS-R PROSAFE activity

(Contract: AFT/NKS-R(20)128/3)

Stefan Authén[1], Erik Sparre[1], Carl Eriksson[1], Erik Cederhorn[1]
Tero Tyrväinen[2], Ilkka Karanta[2], Terhi Kling[2]
Xuhong He[3], Frida Olofsson[3]
Salvatore Massaiu[4]

[1]Risk Pilot AB
[2]VTT Technical Research Centre of Finland Ltd
[3] Vysus Sweden AB/Lloyd's Register Consulting – Energy AB
[4]IFE (Institute for Energy Technology)

Table of contents

Acronyms & Abbreviations

Acronym/Abbreviation	Description
AOP	Abnormal Operating Procedures
ASEP	Accident Sequence Evaluation Program
BE	Basic Event
BWR	Boiling Water Reactor
CBDT	Cause Based Decision Tree
CCF	Common Cause Failure
CDF	Core Damage Frequency
DG	Diesel Generator
DIGREL	Research project concerning digital I&C
ECC	Emergency Core Cooling
EDG	Emergency Diesel Generator
EFET	Enhanced Fault/Event Tree
ELAP	Extended Loss of AC Power
EOC	Error Of Commission
EOP	Emergency Operating Procedure
EPRI	Electric Power Research Institute
ERO	Emergency Response Organization
ET	Event Tree
FAB	Feed And Boil
FC	Fractional Contribution
FD	Fuel Damage
FIF	Failure In Function
FLEX	Diverse and Flexible Coping Strategies
FOD	Failure On Demand
F/R	Forsmark/Ringhals
FSG	FLEX Support Guidelines
FT	Fault Tree
FTR	Fail To Run
HEP	Human Error Probability
HFE	Human Failure Event
HMI	Human Machine Interface
HRA	Human Reliability Analysis
HVAC	Heating, Ventilation and Air Conditioning
I&AB	Initiators and All Barriers
ICC	Independent Core Cooling
ICCS	Independent Core Cooling System
IE	Initiating Event
LERF	Large Early Release Frequency
LOCA	Loss Of Coolant Accident
LOOP	Loss Of Offsite Power
LPSD	Low Power and ShutDown
LUHS	Loss of Ultimate Heat Sink
MCR	Main Control Room
MCS	Minimal Cut Set
MMI	Man Machine Interface
MTTF	Mean Time To Failure
MTTR	Mean Time To Repair
MU	Make-Up
NPP	Nuclear Power Plant
NRC	U.S. Nuclear Regulatory Commission
ORE	Operator Reliability Experiments
PFD	Potential Fuel Damage
POS	Plant Operating State
RHR	Residual Heat Removal
RIF	Risk Increase Factor

PPE	Personal Protective Equipment
PROSAFE	PROlonged time window and SAFE states
PRA	Probabilistic Risk Assessment
PSA	Probabilistic Safety Assessment
PSF	Performance Shaping Factor
PWR	Pressurized Water Reactor
RCS	Reactor Coolant System
SBET	Simulation-Based Event Tree
SFP	Spent Fuel Pool
SFPC	Spent Fuel Pool Cooling
SFPMU	Spent Fuel Pool Make-Up
SPAR-H	Standardized Plant Analysis Risk-Human Reliability Analysis
SC	Success Criteria
SSC	Systems, Structures and Components
SSES	Safe and Stable End State
ST	STeaming
SWS	Service Water System
THERP	Technique for Human Error-Rate Prediction
TRC	Time Reliability Curve
TSC	Technical Support Centre

1. Introduction

Probabilistic safety assessment (PSA) models are mostly very simplified with regard to mission times of safety functions, timings of events, recovery of safety functions and repair of components. The simplifications are often conservative, but also non-conservative simplifications are used, while the overall results are believed to be conservative. Typically, a mission time of 24 hours is assumed for most safety functions in level 1 PSA. Longer time windows are considered rarely, except in some level 2 PSAs and spent fuel pool analyses. The Fukushima nuclear power plant (NPP) accident however pointed out that it might be relevant to consider longer time windows in some accident scenarios (Burgazzi et al., 2014).

This report presents the final results of the Prolonged available time and safe states (PROSAFE) project, which was initiated by the Nordic PSA group. The project was started in 2019 by a literature survey on topics relevant to long time windows in PSA, such as definition of safe and stable end state, mission time, success criteria, component repairs, recovery actions, human reliability analysis (HRA) with long time windows and time-dependent failure rates (Tyrväinen et al., 2020). The literature related to long time windows appears to be very limited, because PSA is typically limited to the mission time of 24 hours. Scenarios with long mission times have been generally recognized as a challenging area that needs to be studied more. A questionnaire to stakeholders was prepared. Answers to the questionnaire highlighted spent fuel pool (SFP) accidents, HRA in long mission time scenarios, modelling of different time windows, repairs and dynamic success criteria as important topics to be studied.

Later in 2019, research on PSA methods for long time windows was started by performing hypothesis testing with four real spent fuel pool PSA models and one reactor PSA model (Tyrväinen et al., 2020). The purpose of this hypothesis testing was to identify important issues where a different modelling approach could significantly improve the realism. Mission times, repairs, time windows, success criteria and manual actions were examined in the hypothesis testing. The results indicated that the models could particularly be improved by more realistic modelling of repairs and time windows. After the hypothesis testing, a set of requirements was formulated for PSA methods with regard to modelling repairs, time windows and dynamic success criteria. Requirements for HRA methods concerning long time windows were also developed.

This report presents PSA and HRA methods developed in the PROSAFE project in 2020. The methods are tested in pilot studies with a fictive and simplified PSA model covering both spent fuel pool and reactor accidents and with a full scale spent fuel pool PSA model. Three PSA methods are presented and compared: Initiator and all barriers (I&AB), an enhanced fault/event tree (EFET) method and a simulation-based event tree method. Three HRA methods are also presented and compared: the Forsmark/Ringhals HRA method, SPAR-H, and the HRA method used in Accident sequence evaluation program (ASEP).

The report is structured as follows. Section 2 presents the definitions of the concepts that are most relevant for this work. Section 3 presents a summary of the previous work performed in the PROSAFE project. The PROSAFE model that is used in pilot studies to test the methods is presented in Section 4. Methods, pilot studies and benchmark studies for HRA and PSA are presented in Sections 5 and 6. Section 7 addresses briefly timings of failures in common cause failures. Section 8 discusses the definition of safe and stable state. Uncertainties related to PSA with long time windows are briefly discussed in Section 9. Finally, Section 10 presents the main conclusions of the report.

2. Definitions

Time available
Time available is the time period from the presentation of a cue for human action or equipment response to the time of adverse consequences if no action is taken.

Required time
Required time is the time needed by operators to successfully perform and complete a human action.

NUREG-1921 (U.S. NRC, 2012) provides a timeline illustration diagram (Figure), and shows the definitions of start time, time delay, available time, cognition time, execution time and required time.

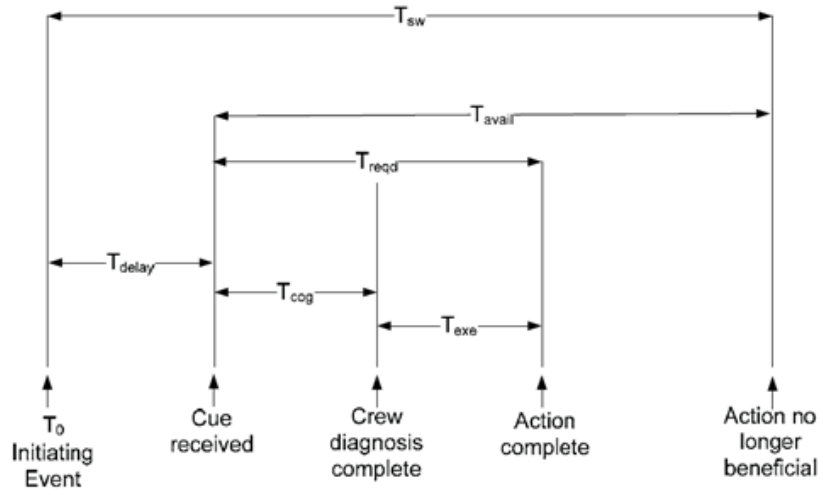

Figure 1. Timeline illustration diagram (NUREG-1921)

The terms associated with each timing element are defined mathematically.

- T_0 = start time = start of the event
- T_{delay} = time delay = duration of time it takes for an operator to acknowledge the cue
- T_{sw} = system time window, is the time from the start of the event until the action is no longer beneficial (typically when irreversible damage occurs, such as core damage or component damage). The system time window represents the maximum amount of time available for the action.
- T_{avail} = time available = time available for action = (T_{sw} - T_{delay})
- T_{cog} = cognition time consisting of detection, diagnosis, and decision making
- T_{exe} = execution time including travel, collection of tools, personnel putting on protection equipment (PPE), and manipulation of components
- T_{reqd} = time required = response time to accomplish the action = (T_{cog} + T_{exe})

Time margin
In addition to the above terms, time margin is used in several HRA methods. Time margin can be defined as the ratio of time available for the action to the time required to perform the action (T_{cog}+T_{exe}) and is calculated as follows:

$$Time\ Margin\ (TM) = \frac{T_{avail} - T_{reqd}}{T_{reqd}} \times 100\% \quad (1)$$

Recovery action: restoration of a function lost as a result of a failed system, structure or component (SSC) by overcoming or compensating for its failure. Generally modeled by using HRA techniques.

Please note failures of recovery actions to restore functions, systems or components are usually modelled as new basic events that would be added to the PSA. These should not to be confused with the "recovery" of an human failure event (HFE) for which credit is given within the specific HFE. Recovery mechanisms (factors) are typically considered in the evaluation of the human error probability (HEP) for the HFE, and not modelled explicitly as separate basic events in the PSA model. Such recovery mechanisms include peer checking, unexpected instrument responses to an action, and new alarms that potentially correct a response error and would lower the HEP of the HFE (NUREG-CR 2199, U.S. NRC, 2017).

Repair: restoration of a failed SSC by correcting the cause of failure and returning the failed SSC to its modeled functionality. Generally modeled by using actuarial data.

Repair time: the period from identification of a component failure until it is returned to service.

Mean time to repair (MTTR): a basic measure of the maintainability of repairable items. It represents the average time required to repair a failed component or device.

In PSA, there is a clear distinction between actions to repair components or systems and actions to recover components or systems (NUREG/CR-6823, U.S. NRC, 2003).

- Recovery actions involve the use of alternate equipment or means to perform a safety function when primary equipment fails, or the use of alternate means to utilize equipment that has not responded as required. Examples of recovery actions include opening doors to promote room cooling when an HVAC system fails, recovering grid-related losses of offsite power by rerouting power, manually initiating a system when the automatic actuation signal fails, bypassing trip logic using jumper cables, and using a hand wheel to manually open a motor-operated valve when the motor fails to operate.
- Repair actions involve the elimination or mitigation of the faults that caused a component or system to fail, and bringing it to operable state. Examples of repair actions include repairing weather-related losses of offsite power, repair of a pump that failed to start, or replacement of a failed circuit breaker.

Regard should be taken to whether the repair is ongoing or if the repair cannot be done for whatever reason resulting in a waiting time to start repairing (reasons including diagnosis, missing spare parts etc.). Regard should be taken to whether the repair has started or if the repair cannot be done for whatever reason resulting in a waiting time to start repairing (reasons including diagnosis, missing spare parts etc.).

Safe and stable state

There are different definitions for safe and stable state for core damage that are used. Some definitions focus on specific instances of plant/core configurations (e.g. shutdown and establishment of core cooling) and others have a stronger focus on the plant reaching desired plant conditions whatever those might be.

STUK Y/1/2018 (STUK, 2018) definition:

"Safe state shall refer to a state where the reactor has been shut down and is non-pressurized, and removal of its decay heat has been secured."

and

"Controlled state shall refer to a state where a reactor has been shut down and the removal of its decay heat has been secured."

SSMFS2008:8 (SSM, 2009) provides a similar definition regarding safe state of nuclear reactors:

"Assured sub-criticality and a temperature below 100 degrees Celsius in the reactor pressure vessel.."

NUREG-2122 (U.S. NRC, 2013) definition:

"Safe stable state: Condition of the reactor in which the necessary safety functions are achieved."

and

"In a PRA, safe stable states are represented by success paths in modelling of accident sequences. A safe stable state implies that the plant conditions are controllable within the success criteria for maintenance of safety functions."

The definition by IAEA-TECDOC-1804 (2016) is also concerned with the long-time availability and says the following:

"Safe stable state: A plant state, following an initiating event, in which plant conditions are controllable at or near desired values and within the success criteria for maintenance of safety functions. A safe stable state is achieved when the following criteria are met:"

- "All required safety functions are successfully performed during the defined mission time."
- "The safety functions are not expected to be lost at a point close-in-time after the specified mission time (i.e. there is compelling evidence that the successful safety functions have adequate operating capacity to be maintained for an indefinite period following the end of the specified mission time, or that there are adequate alternative means of performing the safety functions that can be implemented with high confidence after the specified mission time)."

These definitions and others in the state-of-the-art review (WP1) (with a focus on the definitions that STUK and SSM) can be aggregated as requiring:

Controlled state (core damage): Successfully performed reactivity control and long term secured residual heat removal.

Safe state (core damage): Successfully performed reactivity control, long term secured residual head removal and a non-pressurized vessel.

In addition, the safe state for the spent fuel pools can be considered from the more general descriptions of safe state. But to make the definition analogous to core damage, safe state for fuel damage is defined as follows:

Safe state (fuel damage): Successfully performed reactivity control and long term secured residual heat removal.

Success criterion
Success criterion is the criterion for establishing the minimum number or combinations of systems or components required to operate, or minimum levels of performance per component during a specific period of time, to ensure that the safety functions are satisfied.

Dynamic success criterion
Dynamic success criterion is a success criterion that changes during the mission time.

Mission time
Mission time is the time period that a system or component is required to operate in order to successfully perform its function.

3. Summary of previous work in PROSAFE

3.1. Information collection

The PROSAFE project was started in 2019 with an information collection task (Tyrväinen et al., 2020). Information was collected from literature and through a questionnaire from the stakeholders. The topics covered were: safe, stable state; success criteria; mission times; recoveries and repairs; HRA methods; risk and reliability analysis methods; reliability data; and epistemic uncertainty. The literature related to long time windows appeared to be very limited, because PSA is typically limited to the mission time of 24 hours. Scenarios with long mission times are generally recognised as a challenging topic that should be studied more. The main findings of the information collection task are next described briefly area by area.

Safe and stable state

Ideally, successful PSA sequences should lead to a safe, stable end state (IAEA, 2010). Therefore, the definition of the safe, stable state can affect success criteria and mission times. However, in practise, that does not seem to be usually the case. Success criteria analyses focus typically on avoiding core damage within fixed time window rather than reaching safe, stable state. Different safe (stable) state definitions found from the literature (see Section 0) and specified by the stakeholders of the PROSAFE project vary significantly, and there does not seem to be common way to define successful PSA end states. Some also apply the concept of a controlled state in PSA instead of safe state.

Success criteria

Success criteria are in general calculated, and applied, in the PSAs with a conservative approach, i.e. by using conservative acceptance criteria while not addressing partial core damage, and assuming time independent success criteria during the accident sequence. This agrees with state-of-practice in the international PSA community, though several literature sources identify the need for consideration of time dependencies, both within 24 hours mission time and beyond. The collected opinion from the questionnaire is that the PSA will benefit from an advance in methodologies in order to reach a more realistic consideration and modelling of time related dependencies of success criteria.

Mission time

In level 1 PSA, mission time of 24 hours is usually applied for most safety functions and components. In level 2 PSA, the mission time is typically 24 hours or 48 hours, but in some cases, even 72 hours has been applied. In spent fuel pool analyses, longer mission times may also be used, e.g. 72 hours. It is usually not accurately analysed how long it takes to bring the plant to a safe, stable state. Extending the mission time is however generally recommended if plant conditions are not stable at the end of normal mission time. Modelling of different mission times is considered challenging because it increases the model complexity and the number of basic events.

Recoveries and repairs

Some recovery actions are usually modelled in PSA, e.g. for offsite power, emergency diesel generators and emergency core cooling. Repairs are usually not modelled in PSA, except when long mission times are modelled. Probabilities of recoveries and repairs are estimated based on HRA methods, plant data or expert judgements depending on the case. Dependencies between

recoveries, repairs and other human actions are usually not taken into account. Modelling of recoveries and repairs is considered a challenge because it significantly increases the model complexity.

HRA

Category C HFEs with long time window usually exist in PSA. Examples are human actions that are required late in level 1 PSA, actions in PSA level 2 or actions/repairs related to spent fuel pools. Their available time windows are different, with a range from a few hours to a few days (or even a few weeks for spent fuel pool). Time reliability curve (TRC) from the THERP/ASEP method (NUREG/CR-1278) (or a modified curve, or combined with a low cut off value) is still commonly used to derive the diagnosis HEPs of these HFEs. The SPAR-H method (NUREG/CR-6883) uses the performance shaping factor (PSF) available time as one of the eight PSFs and the maximum multiplier for available time PSF is 0.01. In general when the available time is long, the HEPs will reach the applicable boundary of the HRA methods and there is no further guidance available to consider the effects of the extra time and the related issues e.g. shift change, fatigue, coordination and communication, etc. Thus there is a clear need of better guidance on how to estimate the effect of the long available times on the HEPs.

Methods to model time-dependencies

A large number of references on dynamic PSA methods can be found from the literature (Aldemir, 2013). Such methods could potentially make PSA more realistic. However, according to the questionnaire answers, current PSA methods, event trees and fault trees, are considered sufficient to produce the required results. Some time-dependencies, like dynamic success criteria, have however been considered challenging to analyse using the current methods, and there may be need to study suitable approaches for modelling such time-dependencies.

Failure data

It has been shown in a few different studies that failure rates of some components are not constant over time (Grant et al., 1999). Time-dependencies in reliability data are often not considered in PSA. It is a challenge especially when long mission times are modelled as the probability of failure is perceived as being much too conservative if these kinds of dependencies are not considered.

Uncertainties

Epistemic uncertainty is by the Nordic PSA community in general considered to be an important area of improvement within the PSA, which concur with the result of the literature survey. The answers to the epistemic uncertainty area of the questionnaire was however few, which may be an indication that the area is pre-maturely addressed and that the other areas addressed by PROSAFE, and which the uncertainty area concern, must first be further elaborated. The literature study also shows that there are rather few references available on the subject and that it is recognized as a difficult area to address.

3.2. Hypothesis testing, requirements specification and methods

This section presents a summary of the results of the work conducted in 2019 in the PROSAFE project (Tyrväinen et al., 2020). It includes hypothesis testing performed using PSA models of the stakeholders, requirements specification for the methods and preliminary considerations of the methods.

3.2.1 HRA Requirements Specification

3.2.1.1 Definition and HFE identification

The definitions of the system time window, required time, available time, time margin, etc. should be provided from HRA perspective. These definitions should be defined in the PSA context as every human failure event (HFE) is analysed in the scenarios of PSA and is related to the other PSA elements e.g. success criteria, event sequences, etc.

The types of post-initiating (Category C) HFEs related to prolonged time window and safe states (PROSAFE) should be identified, e.g. from the stakeholder PSA/HRA studies as well as literature reviews.

3.2.1.2 Qualitative analysis

For Category C HFEs with long time window, there could be large uncertainties in the quantitative human error probability (HEP) results as the scenarios and performance shaping factors (PSFs) could have large variances. Assumptions must been taken to get results in the quantitative analysis. It is important to discuss the assumptions and their uncertainties in the qualitative HRA.

Scenario description should be provided to highlight the information that is relevant for the qualitative HRA. The scenario description documents the assumptions made and creates a common understanding of the scenario between the different people involved in the HRA and PSA processes. It provides information on the location of event, the environmental conditions, the operational mode, the safety system involved, the initiating event, the event sequence and the end states.

Task analysis should be performed on the scenario description to identify the critical steps and the driving PSFs. The personnel involved, the potential operator errors and recovery mechanisms should be discussed.

Timeline analysis is suggested for estimating and illustrating the times for all steps included in the task. When the available time is large, the personnel shift switch-over and the impact should be evaluated. A new shift might increase the opportunity to recover the diagnosis errors of the previous shift but could also commit a new error due to misleading/missing information received from, or communication problems with, the previous shift.

For events that involve collaborative teamwork across multiple entities, a teamwork diagram is suggested to represent the task sequences of the teams and the required teamwork activities, such as communications, coordination, command and control, distribution of decision-making and authorization chains. A teamwork diagram delineates how the various teams work together.

3.2.1.3 Quantitative HEP Evaluation

Appropriate HRA quantification method(s) should be used to estimate the likelihoods of the failure in cognition as well as failure in execution. Uncertainty ranges should be provided together with the estimated HEPs.

The assessment of the probabilities of the post-initiator HFEs shall be performed using a well-defined and self-consistent process that addresses the plant-specific and scenario-specific PSFs and addresses potential dependencies between human failure events in the same accident sequence.

These PSFs should include those listed in ASME/ANS PRA standard (ASME/ANS RA-Sa-2009) as well as HRA Good Practices (NUREG-1792) for category C HFEs.

There could be several different types of human actions related to the prolonged available times. The existing quantification methods used in the plant might be capable to perform the estimation. Modification or improvement will be suggested. Options will be suggested with the intention that the proposed HRA methods or modification are simplified. This also means the quantification method will not go down to a detailed level such as the different macro-cognitive functions involved in each critical task, their failure modes and the failure probabilities. The quantification should however be able to find the driving PSFs for the analysed conditions and consider their effects in the quantification.

Anything else being the same, the probability of an HFE (including cognitive part and/or execution part) will be in general lower when the available time is longer. However, long time windows HFEs might have specific complicating features (as discussed above) and it is particularly important to evaluate the plant conditions, the operators/organisational differences, the relevant PSFs and the impact of the large uncertainties in the long time window scenarios.

It is foreseen that some sort of limiting HEPs will be defined, considering the uncertainties for individual HFE as well as multiple HFEs in one scenario (i.e. in one minimal cut set, MCS). The limiting HEPs should be defined to prevent extremely low HEP values as outcomes from the quantification methods. The limiting values should be defined for different situations considering the whole contextual conditions besides the prolonged available time and consider the uncertainties.

As situational uncertainties in long time windows scenarios (all the specific event sequences that are within the bounding conditions of the nominal scenario) have a stronger impact on HFE than intrinsic human performance variability, any lack of explicit treatment of situational variations should be accounted for in the quantification stage.

Potential dependencies between human failure events should be properly characterized and taken into account to ensure that the accident sequence frequency estimations are performed correctly taking into account any commonalities and relationships among the category C HFEs.

When there are much longer available times, the potential new human actions should also be discussed, e.g. recovery actions, repair actions and their dependencies with existing actions.

3.2.1.4 Reasonableness check

Evaluate the reasonableness of the HEPs obtained from the proposed method. The HEPs should be reasonable from two standpoints: (1) first and foremost, relative to each other (i.e., the probabilistic ranking of the failures when compared one to another), and (2) in absolute terms (i.e., each HEP value), given the context and combination of positive and negative PSFs and their relative strengths.

3.2.2 Hypothesis testing with PSA models

There are several features related to long time windows modelling that may be non-trivial or even impossible to represent in a realistic way with static event tree and fault tree modelling. The potential importance of these features were investigated through elaboration with several PSA models and gave an indication of the potential importance of a feature. Conclusions from the extensive testing that were performed during the early phase of this project are given below.

Mission time

Mission times are typically important parameters that have large impacts in results. Only in one spent fuel pool model, the impact was relatively small, because hazard impacts and human failure events dominated over normal component failures. In many cases, less conservative mission times could improve PSA models significantly. Mission times are generally not defined based on how long it exactly takes to reach a safe and stable state.

Crediting of repair

Repair is both possible and significant for the long time windows considered in the spent fuel pool models and the core event model. Repair is already considered in some of the models but there is a large potential for improvement and more realistic modelling because the current repair modelling is undesirably conservative in some respects. One aspect that should be considered is to increase the realism with regard to dependencies with for example manual actions. Another way to increase the realism could be to model the repair for initiating events in the models where it has not been modelled. It is also possible to consider repair in a model with the current time windows. In the cases where CCF events are of greater importance because of more redundancy in the model (for example in the core event model), they need to be handled appropriately if realism is strived for.

Time windows

Time windows are generally defined conservatively based on the worst case. Models could be made more realistic by modelling relaxed time windows, e.g. if a primary component operates some time before it fails, a back-up component has shorter mission time and there is longer time available for repair. The mission time of a safety function could also depend on when the safety function is started, because e.g. the status of a spent fuel pool can be very different after one hour compared to two days. Impacts of failures that occur at different times on consequences and success criteria of other safety functions have been modelled in some scenarios, but not widely. In addition, limited delays that can allow extra time e.g. for manual actions could be of importance and would be good to evaluate with a method that allows the analyst to credit these.

Time-dependent failure rates have not been modelled, except for diesel generators in one model. Since the mission times are very long in the spent fuel pool models, it is relevant to study the applicability of the currently used failure rates to such long accident scenarios.

Success criteria

Dynamic success criteria were identified to be relevant only for reactor PSA, not spent fuel pool analysis. Also, in reactor PSA, only one significant modelling case was identified. Therefore, it seems that dynamic success criteria may need to be modelled in some specific scenarios, but not widely.

Manual actions

Available times for manual actions are typically estimated conservatively based on the worst case, i.e. that safety functions fail at the time of the demand. In reality, available times may be longer, if the preceding safety functions operate some time before they fail. In many cases, such scenarios contribute significantly to the risk, so it worth to consider more realistic modelling of available times.

3.2.3 PSA Method requirements specification

The findings from the hypothesis testing constitute as a base to formulate requirements on modelling approaches and methods. In addition, some requirements are formulated based on earlier literature review and questionnaire answers. Repair and time window modelling requirements are prioritised over dynamic success criteria modelling requirements based on the hypothesis testing. Below the main requirements are presented. The complete set of requirements is presented in (Tyrväinen et al., 2020). It should not be interpreted that a method should necessarily satisfy all the requirements, but a good coverage would be desirable. It depends on the scope of the analysis and the method which requirements need to be satisfied.

The main requirements for repair modelling are:

- A process shall be developed to screen and identify the most important repairable components in a PSA model, e.g. through dominant MCSs and/or component (basic event) importance, etc.
- The repair analysis method shall take into account the time available for the repair and the time it takes to perform the repair, as well as possible failures to perform the repair (e.g. related to HRA: fail to detect the failures, diagnosis, decision making and repair execution) and missing spare parts.
- Repair probability estimates shall consider different possible failure causes of the repaired components.
- It shall be possible to model dependencies between multiple repairs, as well as dependencies between a repair and other human actions.
- It shall be possible to model the impact of different possible failure times on the available time for repair and the repair probability. In this case, it can make difference whether a single failure, a CCF or multiple single failures are repaired.

The main requirements for time window modelling are:

- It shall be possible to model multiple different time windows in the same scenario.
- It shall be possible to model different mission times for the same component in different scenarios.
- It shall be possible to model time windows varying dynamically based on some conditions. For example, failure times of components/safety functions can affect the time available to perform manual actions.
- It shall be possible to model mission times of back-up components as dependent on the failure times and/or failure modes of the operating components.
- It shall be possible to model non-constant failure rates.
- It shall be possible to model impacts of different recovery times, e.g. different loss of offsite power recovery times.

Requirements for dynamic success criteria modelling are specified as follows:

- It shall be possible to model the case where a success criterion of a safety function changes at a fixed time point. It shall be possible to model the risk of failure of both the success criterion before the change and after the change.
- The dependencies between time intervals with different success criteria shall be possible to model. This refers particularly to early component failures that remain in effect after the success criterion changes.
- The modelling approach shall be applicable to large fault tree structures (or other large model structures) that include multiple failure modes of many different components and linked fault trees of support systems.
- Modelling of SSC repairs shall be possible in combination with dynamic success criteria modelling.
- Modelling of different time windows shall be possible in combination with dynamic success criteria modelling.

3.2.4 Methods

PROSAFE HRA focuses on the Category C HFEs. A number of Category C HRA quantification approaches were reviewed and some of them were then proposed to be tested in the pilot studies. An important factor in the quantification of category C HFEs with long time window is how to consider recovery mechanism (factors) within the HFE quantification. Error recovery will be likely if there is a long time window and there is clearly additional personnel who can be assumed to be rather independent controllers of the situation. One idea to be tested in pilot study is to check if additional error recovery is necessary for extended time window situations. On the other hand, some HFEs with a long time window might have other challenges, for example multiple crews, parallel actions, decision from outside MCR, etc. These relevant factors will be further tested in the pilot study.

Dependency treatment is another element for the multiple HFEs in one MCSs. When the recovery actions and repairs are considered in the dominant MCSs, the possible dependencies are expected to have influence on the result. An important question is to assess the dependency level and also justify the dependency level is reasonable in the PROSAFE scenarios.

Estimation of repair failure probabilities require input from the HRA part when considering diagnosis, decision, etc., and for example the dependencies to other repair events are important

to consider. The execution part should be analysed with failure data and will require a distribution for repair time and will also depend on the specific available time. For Nordic plants the repair time parameter that is used is the Mean time to repair (MTTR). For more complex cases like several independent failures and CCF there are many assumptions and situations to consider.

Crediting repair in PSA-modelling can be done in a few different ways, each with different pros and cons. If the state of possible repair situation of the systems is well understood and the time put into the modelling is considered necessary, it is possible to use event tree and/or fault tree techniques to credit repair. Since the complexity of the models increase with these methods it is easiest applied to models that are not that complex i.e. the spent fuel pool model. There it is often used in current (but often limited) modelling. Techniques using manipulation of the MCS-list are probably more suited for models that require more complexity.

Modelling time windows can be performed to some extent utilizing ET/FT techniques. Some types of time windows can be represented with relatively simple modelling in ET/FT models. Other types of time windows would require solutions that still must involve a great amount of simplifications as the models quickly would become much too complex. Yet some time window types may not be possible to model in a static ET/FT representation at all.

It is evident that if a higher level of detail in the time windows modelling is required ET/FT tools are associated with limitations. A semi-dynamic/dynamic approach would then be more advantageous as an ET/FT model would not be reasonable due to the level of complexity. These findings raise the questions:

- When is it necessary to consider certain time windows?
- Under what circumstances would a semi-dynamic/dynamic approach be beneficial/necessary compared to using ET/FT techniques?

The advantage of using a more dynamic approach is the improved realism. In order to perform a dynamic analysis, additional information beyond already existing information in a FT/ET PSA tool is required. This conclusion identifies the following question:

- What additional information is required if a semi-dynamic/dynamic add-on tool could be used for existing ET/FT models?

A simple example of dynamic success criteria modelling using fault trees was presented in (Tyrväinen et al., 2020). The modelling is not logically difficult but may significantly increase the complexity of a large PSA model. If there is need to model dynamic success criteria for several safety functions, it would be convenient to have some of the modelling or analysis process automated, e.g. automatic generation of needed fault trees based on one master fault tree. Modelling of repairs and dynamic time windows are issues that can also potentially make dynamic success criteria modelling more complicated and should be studied more in this context. Modelling of dynamic success criteria may require more comprehensive success criteria analyses than normally used, e.g. more thermo-hydraulic simulations to determine the time windows.

4. PROSAFE model

PROSAFE model represents a fictive boiling water reactor (BWR), and it covers both reactor and SFP accidents. For a summary of the general features of the PROSAFE SFP model see (Tyrväinen et al., 2020).

The primary function of the spent fuel pool cooling system is to remove decay heat, generated by the spent fuel elements stored in the pits. The system consists of four redundant trains with separate pumps and heat exchangers. One train (1-out-of-4) in the spent fuel pool cooling (SFPC) system is assumed to be required for cooling of the SFP. The model is simplified so that failures in the service water system (SWS) that cause loss of the SFPC system are not considered.

During power operations one train is assumed to be in operation, other trains are available in standby. Activation of trains in standby (start of standby pump/heat exchangers of the system) is done locally.

Moreover, the PROSAFE spent fuel pool model also includes system for feed water to the spent fuel pool, in case cooling with the SFPC system has failed. A system is used for spent fuel pool make-up (SFPMU) and is assumed to consist of two diverse systems that can be utilized in case of total loss of spent fuel pool cooling. The two systems for make-up are:

- SFPMU:1 – Make-up of spent fuel pits by feedwater from internal water storage (Demineralized water storage) tank with two redundant pumps.
- SFPMU:2 – Make-up of spent fuel pits by feedwater from external water storage tank (make-up with one mobile FLEX pump)

The core model is a modification of the earlier DIGREL model (Authén et al., 2015). This model has been modified with some additional safety systems (most notably the independent core cooling).

The initiating events that have been considered are:

- Transient (SFP)
- Loss of offsite power (SFP)
- Extreme snow (both SFP and core)

4.1. Transient

The transient will cause loss of cooling of the spent fuel pool. A redundant train of the spent fuel pool cooling system can be started to regain cooling and that can fail by mechanical or human failure modes. If the recovery of a redundant train of the spent fuel pool cooling system fails, then the spent fuel pool make-up system 1 or make-up system 2 will have to be used. Make-up system 1 uses the internal power grid while make-up system 2 uses a separate FLEX (diverse and flexible coping strategies) diesel generator. Figure 2 shows the transient event tree.

Transient in Spent Fuel Pool	Recovery SFPC via train 2, 3 or 4	SFP Make Up system 1	SFP Make Up system 2				
SFPC-T	SFPC-R	SFPMU:1	SFPMU:2	No.	Freq.	Conseq.	Code
				1		OK	
				2		OK,FAB,LTW	SFPC-R
				3		OK,FAB,LTW	SFPC-R-SFPMU:1
				4		FD	SFPC-R-SFPMU:1-SFPMU:2

Figure 2. Event tree for SFP transient.

4.2. Loss of offsite power (LOOP)

The modelling of the loss of offsite power event is similar to the transient but the diesel generators (or gas turbine) are always required to work to provide power to safety systems. The spent fuel pool cooling system and spent fuel pool make-up system 1 are provided power from the outside power grid and diesel generators, and power to make-up system 2 is provided by the FLEX diesel generator. Figure 3 shows the LOOP event tree.

Loss Of Offsite Power	Spent Fuel Pool Cooling	SFP Make Up system 1	SFP Make Up system 2			
LOOP	SFPC	SFPMU:1	SFPMU:2	No.	Freq.	Conseq.
				1		OK
				2		FAB,FAB1
				3		FAB,FAB2
				4		FD

Figure 3. Event tree for SFP LOOP.

Extreme snow is a relatively slow event and warning from weather services and personnel on site can be obtained prior to the event. Whether the warning is received or not will affect the preparedness of the plant personnel and if countermeasures are likely to succeed. If removal of snow succeeds the sequence will look like transient and if snow removal fails it will have additional consequences. There is also a risk that outside power supply will be unavailable for a longer period. Figure 4 shows the extreme snow event tree.

Snow	Initial manual actions	Spent Fuel Pool Cooling	SFP Make Up system 1	SFP Make Up system 2			
EXT_SNOW	EXT_IMA	SFPC	SFPMU:1	SFPMU:2	No.	Freq.	Conseq.
					1		SFPC_OK
					2		FAB,FAB1
					3		FAB,FAB2
					4	1,43E-10	FD
					5		FAB,FAB2
					6		FD

Figure 4. Event tree for SFP extreme snow.

The worst-case scenario of the event will cause collapse of structures containing ventilation for diesel generators and it might cause blocking of the sea water cooling intake. In the analysis it is assumed that the collapse of ventilation buildings is a relatively fast event, but this assumption can be questioned if a more detailed and realistic analysis regarding the real situation at a plant is performed. These assumptions and their impact on repair modelling can be seen in Table 1.

Table 1. Some external event alternatives for repair depending on assumptions.

Assumption	Fail sequence (Cons: CD)	Success sequence (Cons: LW)
Collapse of diesel building	Repair of independent core cooling (ICC)	Mobile diesel generators?
Blocking of ventilation	Repair of ICC or recovery of snow clearing	Recovery of snow clearing

4.3. Core model

The core model is the DIGREL model (Authén et al., 2015) modified with two extra function events, U2 independent core cooling and W2 residual heat removal. In PROSAFE this is only considered for the external event (heavy snow). Figure 5 show the extreme snow core model.

No.	Freq.	Conseq.	Code
1		OK	
2		OK	Q
3		LTW,LTW1	Q-W2
4		LTW,LTW2	Q-W2-W1
5		CD	Q-W2-W1-W3
6		OK	Q-U
7		LTW,LTW1	Q-U-W2
8		LTW,LTW2	Q-U-W2-W1
9		CD	Q-U-W2-W1-W3
10		OK	Q-U-U2
11		LTW,LTW1	Q-U-U2-W2
12		CD	Q-U-U2-W2-W1
13		CD	Q-U-U2-V
14		CD	Q-U-U2-X
15		CD	C
16		LTW,LTW2	EXT_IMA
17		CD	EXT_IMA-W3
18		CD	EXT_IMA-U2
19		CD	EXT_IMA-C

Figure 5. Event tree for core model extreme snow.

5. Human reliability analysis

5.1. Methods

5.1.1 Introduction

In the PROSAFE SFP model for Transient, Loss of Offsite Power, and Extreme Snow, the identified HFEs can be grouped in the following types:

- 'Normal' Category C HFEs with long time window, e.g. start up the standby SFP cooling train when the operating train is lost
- Diverse and Flexible Mitigation Strategies (FLEX) actions, e.g. start the portable SFP water make-up pump (make-up system 2), snow removal in extreme snow scenario
- Repair actions, e.g. repair the make-up system 1, repair the diesel generators

Both FLEX actions and repair actions are also category C HFEs, i.e. human actions performed after the initiating event (with some exceptions with regard to some FLEX action). They are listed as separated types to emphasise their specific modelling and quantification challenges. FLEX actions were seldom modelled before Fukushima accident but can now be credited when the portable safety equipment is implemented at the plants, which is the case for many plants after the stress tests. Some FLEX actions could also include pre-initiator actions as preparations and arrangements that might take place before initiators. Snow removal is such a type of FLEX action that needs to be prepared before the precipitation and performed continuously and repeatedly under a heavy snow storm.

Repair actions are usually not modelled so far in the reactor PSA as repair is relatively time consuming and not credible within 24 hours. Repair becomes credible when there is extensive time window for SFP events and even for some reactor events. As there are three different PSA approaches used in the pilot study, the inclusion of repair actions are different in different PSA approaches. The main difference is in the way the repair actions are modelled in the PSA models, see section 6. In the Swedish PROSAFE HRA pilot study, the Forsmark/Ringhals HRA method (Holmberg, 2019) is selected as the main HRA method for the quantification of all identified human failure events (HFEs). For comparison purpose, SPAR-H method is used in the quantification of a selected HFE.

For both Forsmark/Ringhals HRA method and SPAR-H method, all the above operator actions are divided into two parts (1) identification, diagnosis and decision making (hereafter we use **diagnosis** to represent all these three cognitive activities), and (2) post-diagnosis action (hereafter we use **execution**). Each part is modelled by a basic event of its own. See Figure 6. For both parts, the Forsmark/Ringhals HRA method can include recovery.

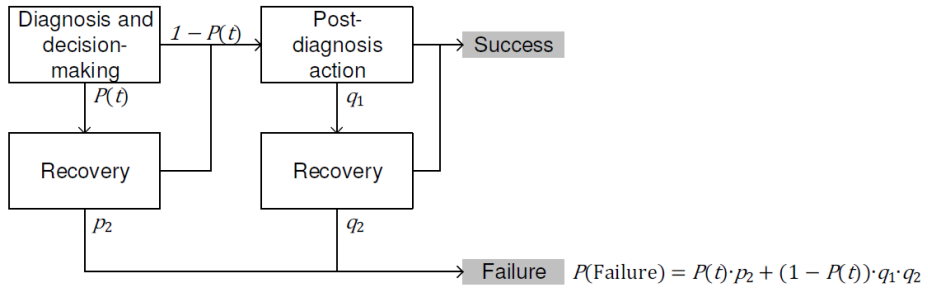

Figure 6. Basic model for the quantification of post-initiating HFEs (NPSAG 53-002)

In the Forsmark/Ringhals (F/R) HRA method, the basis diagnosis probability is read from time related curve (TRC, see Figure 7) and adjusted with 5 PSFs (see Figure 8) and possible recovery factor. The recovery of failed diagnosis and decision making can be considered if there is a long time window and additional personnel who can be assumed to be rather independent from the original decision makers. To assume support from other personnel, the available time to recover a scenario should be long (several hours). Given that the above conditions for recovery can be justified, a simple quantification of the recovery failure probability is provided as 0.1. This value is reference to cause based decision tree (CBDT) method as its initial estimate.

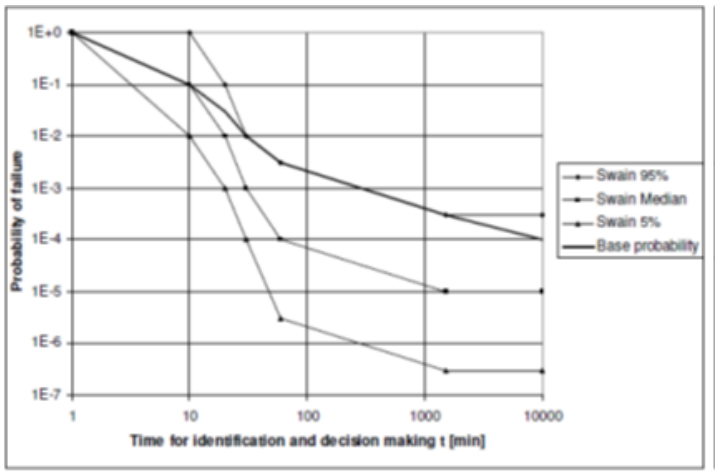

Figure 7. Time-dependent human error probability curve in F/R method (NPSAG 53-002)

	Performance shaping factors				
	Quality and importance of procedures	**Quality and importance of training**	**Feedback from process, quality of MMI**	**Mental load**	**Communication and coordination**
Factor	$K_{procedure}$	$K_{training}$	$K_{feedback}$	K_{stress}	$K_{coordination}$
Questions	*Are there procedures? Are they needed? Do they give support?*	*Has the situation been trained? What kind of training? How often it has been trained? Is the action well known?*	*Is critical information available for the operators? How easily, understandably, rapidly? Is there redundant information? Can there be misleading signals?*	*Is the situation or action unusual? Are there any special uncertainties in the situation?*	*Is it a scattered disturbance? Are actions needed inside/ outside of control room (CR)? Does communication work? Is coordination of actions needed?*
$K_i = 5$	No instructions or misleading instructions, instructions would be needed	No training or misleading training, training would be needed	No feedback from process or misleading information or too late feedback	Mental load is so high that it nearly hinders to make a rational decision, situation is chaotic, an extreme decision needs to made	Information must be obtained from inside and outside of CR, coordination of many activities, poor conditions for communication
$K_i = 2$	Instructions are important, but they are imperfect	Some training has been given but it is not fully applicable for the situation	Feedback is obtained but there are defects in the presentation of the critical information	Mental load is considerable, situation is serious, a serious decision needs to be made	Information must be obtained from inside and outside of CR, coordination of many activities, good conditions for communication
$K_i = 1$	Instructions are sufficient, or they do not play a major role in the situation (e.g. due to sufficient training)	Training for the particular situation is sufficient, or it does not play a major role because of sufficient basic training	Feedback is sufficient, or it does not play a major role in the situation	Mental load plays no major role in the situation	Need for communication and coordination is minor, or it is relatively easy to coordinate activities
$K_i = 0{,}5$	Good instructions, applicable for the situation and they support well the selection of correct actions	Situation has been trained (in a simulator), an important theme in the training	Symptoms can be easily observed and identified	NA	Operator(s) can act directly based on available information without further communication
$K_i = 0{,}2$	Very good instructions, operators should not make any mistake	Situation is often trained in a simulator, a very important theme	It is practically impossible to miss the symptoms, several redundant indications	NA	NA

Figure 8. Explanation of the scales for the performance shaping factors (NPSAG 53-002)

The quantification of the post-diagnosis execution is rather simple in the Forsmark/Ringhals HRA method. Criteria are provided and the probabilities can be chosen from six probability scales (see Figure 9). Recovery is also possible for the four of six probability scales, with the recovery failure probability of 0.1.

Grade	q_1	Action types and interpretation of the grades	
		Conditions for the initial error	Recovery
Very easy	1E-4	It is practically impossible to fail this action. 1. Instructions are optimal 2. Action is well-trained 3. Human interface (ergonomics) are optimal 4. No stress 5. There are truely resources available for this action. No problems with communication and coordination of activities. Detailed analysis required. It should be noted that very easy tasks may be left out of the model if the diagnosis part dominates the results.	If possible to recover q_2 = 0,1, otherwise **1,0**
Easy	0,002	Easy manoeuvres. Failures unlikely or easy to detect. Good conditions. 1. Clear instructions 2. Has been trained 3. Excellent interface (ergonomics), very low probability for confusion error 4. No stress 5. Enough resources. No problems with communication and coordination of activities. No problems to transport tools to the location (if needed).	If possible to recover q_2 = 0,1, otherwise **1,0**
Normal	0,01	Some possibility for a failure. More complex than the case above. This can be assumed as the default case (somewhat conservative screening value) 1. Not perfect or somewhat ambiguous instructions 2. Some training has been given 3. Not perfect or somewhat ambiguous interface 4. Some stress 5. Coordination and communication problems may exist. Concurring activities and lack of resources may exist. Tools needed for the action may be difficult transport to the location.	If possible to recover q_2 = 0,1, otherwise **1,0**
Somewhat difficult	0,05	Clear possibility for a failure. Complex manoeuvre. Difficult conditions. 1. Far from perfect or ambiguous instructions 2. Not much trained 3. Somewhat difficult interface 4. Some stress 5. Concurring activities and lack of resources will probably exist. Tools needed for the action are difficult transport to the location.	If possible to recover q_2 = 0,1, otherwise **1,0**
Medium difficult	0,1	As above but 0.05 is considered too optimistic. There is a considerable chance to fail. Conditions are difficult. High chance for lack of resources and concurrent actions.	Not credited
Very difficult	0,5–1,0	Prerequisites to succeed are very low. Use of 0,1 (as above) is considered optimistic. Use of p_1=1 may be related to interim analysis cases, and the effect of crediting the operator action can be studied by means of a sensitivity study.	Not credited

Figure 9. Probability scale for the post-diagnosis action (NPSAG 53-002)

In the SPAR-H method, 8 PSFs are to be evaluated for both diagnosis and execution HEPs. The available time is one of the eight PSFs in both diagnosis and execution HEP estimation. With the expansive time, the multiplier can be 0.01 for the diagnosis (nominal diagnosis HEP is 1E-2) and 0.01 for the execution (nominal action HEP is 1E-3). Using the SPAR-H for low power and shutdown (LPSD) condition as an example, when all PSFs are at the most optimal conditions, the lowest diagnosis HEP could be 1E-6 and the lowest execution HEP could be 1.25E-6. In the best situation, the lowest total HEP would be 2.25E-6.

The consideration of the error recovery in SPAR-H framework is not clearly developed and usually not considered besides its normal quantification. SPAR-H (NUREG/CR-6883) provides two possible means to represent the error recovery by, e.g., additional steps in procedures, additional alarm information, or additional personnel. The first is to perform more detailed

modelling. This means the recovery can be modelled as a separated HFE or explicitly considered in the HFE logic structure. The second (SPAR-H suggested option) is to make adjustment to the nominal HEP by assigning the appropriate positive levels to the appropriate subset of PSFs. The work process PSF (for additional personnel being present), procedures PSF (if additional steps strongly indicate to the operator that misdiagnosis has occurred), and ergonomics (for new cues that will strongly shape the operator or crew sense that misdiagnosis has occurred) can be used by the analyst to indicate that these factors are likely to produce a situation where the nominal value for diagnosis is overly conservative.

5.1.2 HRA method for 'Normal' Category C HFEs with long time window

5.1.2.1 Diagnosis HEP

In the PROSAFE pilot study the total time windows for 'normal' Category C HFEs are quite long, e.g. 24 hours for SFP cooling before boiling and 72 hours to initiate make-up before uncovered fuel in SFP.

According to the time-dependent HEP curve in the Forsmark/Ringhals HRA method, the base probability for diagnosis would be between 1E-4 (the lowest base HEP) and 1E-3 (when the available time for diagnosis is about 4.5 hours).

The scale factors (ki) or multipliers for the five PSFs are still applicable and are used to adjust the base diagnosis HEP. Each performance shaping factor can receive a value 1/5, 1/2, 1, 2 or 5. It is important to make sure that the important factors in PROSAFE scenarios can be properly reflected in these five factors and the scale factors are reasonable. Some observations are listed for the selection of the scale factors in PROSAFE scenario:

- No need to change the scale factors and the guidance of the selection for four PSFs: Quality and relevance of procedures; Quality and relevance of training; Quality and relevance of feedback from process (MMI); Mental load in the situation (stress).

- Need for coordination and communication: no need to change the scale factors, but some minor modification of the explanation of the scales included in the NPSAG.53-002 might be needed for the PSF. Kcoordination =2 might be justified as 1 in PROSAFE scenario as information need to be exchanged between different groups inside and outside the control room. As long as good conditions for communication are in place, it is suggested to consider this as a relatively easy to coordinate activity (Kcoordination =1).

In the Forsmark/Ringhals HRA method, recovery of failed diagnosis can be considered if there is a long time window and there is additional personnel who can be assumed to be rather independent from the original decision makers. This criterion is usually met for the 'normal' category C HFEs in PROSAFE. On the other hand, we shall also realize the possible challenges in the recovery, for example fatigue, several parallel actions, decisions outside the main control room (MCR), etc. Finally there should be some reasonable limiting (lowest) HEPs in place for individual HFE as we cannot repeat the use of recovery factors for too many times. As the base diagnosis is already quite low for the PROSAFE HFEs, it is not the dominant part of total HEP and is not necessary to consider the recovery further.

5.1.2.2 Execution HEP

The quantification of the execution is rather simple in the Forsmark/Ringhals HRA method. Criteria are provided and the probabilities can be chosen from six probability grades (values). The interpretation of conditions of six grades is provided and it is closely related to the quality of instruction, training, ergonomics, stress and human resources/communication. The normal Grade has probability of 0.01 and this is a somewhat conservative screening value.

In the Forsmark/Ringhals HRA method, recovery is also possible for the four of six probability scales, with the recovery probability of 0.1. If the condition is judged to be medium difficult Grade (HEP=0.1) and very difficult Grade (HEP = 0.5-1.0), recovery is not credited.

As the normal Grade has quite conservative HEP, the following recovery is thus proposed for execution HEP in PROSAFE long time windows scenarios:

- In general, one recovery (e.g. failure probability 0.1) is suggested if normal Grade is chosen for the extensive situation (more than 8 hours)

- Additional recovery (e.g. failure probability 0.5) can be credited for the extremely extensive situation (more than 24 hours). 0.5 is simply very conservative as it is a rough estimation assuming there is high dependency between the two recoveries.

Note: When the available time is a few days or even weeks, additional recovery can be considered with medium or low dependency. On the other hand, the HEP would be low enough and it is not necessary to consider more recoveries. It is thus suggested not to further lower the execution HEP if two recoveries have already been credited and the HEP is already lower than 1E-4. One can add a new HFE for function recovery for the significant scenarios, instead of multiple recoveries.

5.1.3 HRA method for FLEX actions

5.1.3.1 HRA Literature review on FLEX

FLEX actions can be considered as a special type of Category C human actions, in which diverse and flexible coping strategies are implemented in response to a beyond-design basis accident. Some FLEX actions, such as snow removal, could also be considered partly as pre-initiator actions (Category A) as preparations and arrangements will take place after snowing but before any initiators happen at the plant.

Many FLEX actions can be modelled with current HRA methods and data (EPRI, 2018; Presley, 2017). However, certain types of actions and some PSFs associated with the use of portable equipment might substantially differ from similar but non-FLEX actions. Hence the HEP for a human task in THERP can be very different from the HEP of the corresponding task in the FLEX scenario. The NRC considers that there are still "significant uncertainties in human error probabilities and lack of operating experience associated with deployment and operation of offsite portable equipment" as well as lack of "comprehensive human reliability analysis methodologies and guidance" (NRC, 2017).

NEI 16-06 (NEI, 2016) pointed out that there are actions that may be required when implementing mitigating strategies that do not match the data that was used to assess the failure probabilities in current HRA methodologies. Until good basis HRA data and method are

provided, engineering judgement is required to assess the probability of a human error that prevents the successful implementation of the strategy. These actions that are not explicitly covered may include *debris removal*, *transportation of portable equipment*, *installation of equipment at a staging location* and *routing of cables and hoses*.

Table 2 lists the peculiarities of FLEX actions (compared with most post-initiator actions) and shows the communalities with actions in external flooding and main control room abandonment (MCRA) scenarios.

Table 2 FLEX Action Characteristic

FLEX Action Characteristic	**FLEX**	**Ext. Flood**	**MCRA**
Tasks outside the main control room -Transportation & Installation of equipment -Hardware limitations (Once DC Load Shed occurs, how easy is it to "undo", especially large complex Offsite Power supply breakers) -Sandbag wall construction -Debris removal -Routing of cables and hoses	X	X	
Uncertainty in Timing/Staffing -Prioritization not specified -Alternative strategies available (If ELAP is declared, then do other strategies such as EDG restoration and Offsite Power recovery continue? Under what guidance?) -Soft Cues (judgment required or large uncertainty on timing/clarity of cue, e.g. "If power is not expected to be restored within 4 hours, declare an ELAP") -Additional crew availability questionable -Demands on the available manpower may require personnel to perform tasks that are not part of their normal duties	X	X	X
Decision Making -Making decisions to enter a procedure using judgement based on a belief in a future event (e.g., the expectation that offsite power will not be restored in a certain time frame) -Cue based on judgment or requires prioritization that is not pre-defined -Prioritization when order is not specified but order is important to success -Crediting actions when there is no explicit procedural link -Reliance on assessments for time available for response -Reliance on grid operators for return-to-service estimates -Reliance on weather forecast for future weather conditions	X	X	X
Environmental Effects on Execution -Collapsed structures/debris -Components accessibility (High temperatures, steam) -Water and high winds -Timing of actions	X	X	
Complex Execution Actions -Many steps or manipulations involved in single "actions" -Long time windows, extended period of action (refuelling) -Multiple people/locations working in coordination to complete a single task	X	X	X
Organizational Prioritization -Multi-unit/Multi-site coordination -Large scope resource management tasks -Soft Cues/Cues from outside organizations	X	X	
Complex Control Actions	X	X	X
Changes in command/control	?	X	X

5.1.3.1.1 Qualitative HRA for FLEX

The typical actions in FLEX-type scenarios relate to the use of portable equipment. It is possible to decompose use of portable equipment by considering the applicable following sub-actions:

1. Transportation
2. Placement
3. Connection
4. Local control of portable pumps and generators
5. Refilling water storage tanks using alternate water sources
6. DC load shedding
7. Restoring equipment from DC load shedding
8. Refuelling
9. Use of pre-staged equipment
10. Dam break and sandbag wall (external flooding).

The following timing information might be relevant for the timeline analysis for FLEX actions:

1) Receive enough indications (cue)
2) Enter and evaluate the written instructions
3) Take any necessary preparatory actions to begin the deployment actions (including potential for debris removal for external events that make the travel path more difficult)
4) Transportation and staging
5) Installation of hoses or cables
6) Pre-operational checks, electrical rotation checks, and/or alignments
7) Complete the steps to start equipment
8) Begin restoration or continuation of the function provided by the equipment
9) Ancillary actions required by the portable equipment (e.g., opening doors or establishing alternate ventilation systems for long term room cooling, refuelling).

Figure 10 is an example of timeline analysis for a FLEX action to start the portable water injection system (Kirimoto et al., 2020).

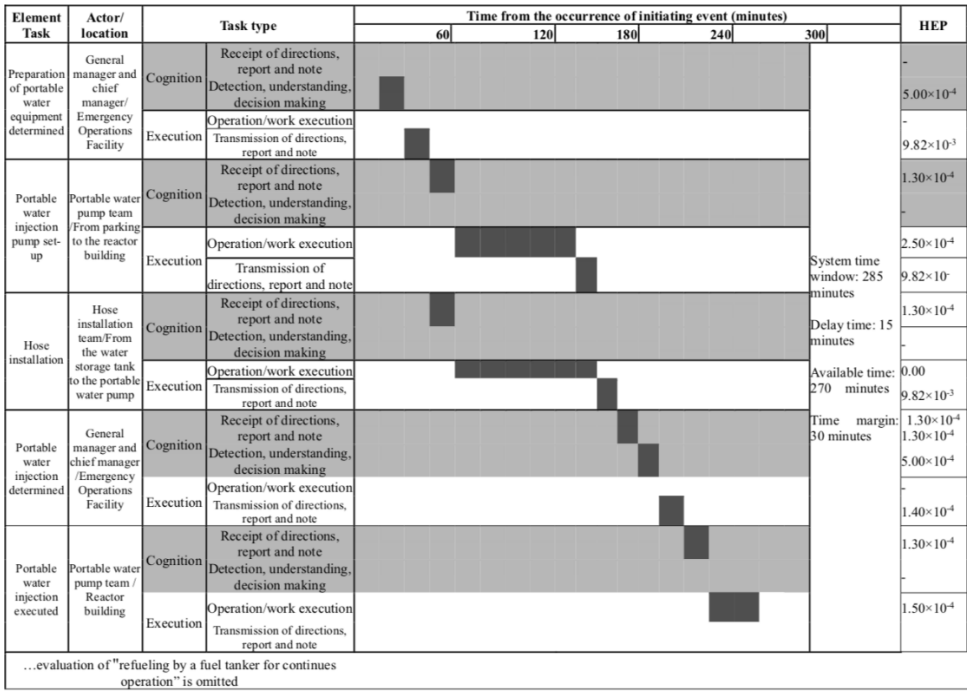

Figure 10. Example of timeline analysis from Kirimoto et al. 2020

5.1.3.1.2 Important PSFs

Procedures
It is necessary to understand how procedures fit together, e.g. the linkage between Flex Support Guidelines (FSG) and the Emergency Operating Procedure (EOP) network.

FLEX Support Guidelines (FSG) provide pre-planned strategies for establishing an indefinite coping capability to prevent core damage, ensure containment function and spent fuel pool cooling in beyond-design-basis external events (extended loss of AC power (ELAP) and simultaneous loss of normal access to the ultimate heat sink (LUHS)). FLEX guidelines support Emergency Operating Procedures (EOP) and Abnormal Operating Procedures (AOP). In general, the EOPs direct implementation of the FSGs based on specific conditions that necessitated entry into the FSGs, but the FSGs are not necessarily formally incorporated into the plant's EOPs. There could be different procedures for different types of scenarios for the same equipment. For portable equipment not all instructions will be contained within plant procedures: other written instructions may be implemented.

Evaluate:
- if the operators would be directed to implement FLEX equipment after diagnosing the scenario
- if the operators would know how to use the portable equipment for the given scenario
- whether there are written instructions that would drive the use of the portable equipment in the given scenario.

Cues and indications
The HRA process includes identifying clear cues to enter the procedure and clear direction within the procedure on the steps required to be performed. For FLEX, cues may be complicated by the need to make decisions to enter a procedure using judgement based on a belief in a future event (e.g., the expectation that offsite power will not be restored in a certain time frame).

If the procedure and cues are ambiguous, e.g. there is some leeway in the decision (e.g., "If power is not expected to be restored within 4 hours, declare an ELAP"), engineering judgement is suggested in NEI 16-06 to provide a basis for the probability of failure given the subjective nature of the decision point. This could be a standalone basic event and may not necessarily be developed within any specific HRA tool.

Training
Training for FLEX actions might not be as good as for EOPs. For instance, NRC rule allows training to be infrequent (>5 years periodicity), but some actions might be trained on more frequently (Julius, 2019). The process of deploying and installing the portable equipment should have been demonstrated and/or validated and the timings available.

The quality, effectiveness, and frequency of training programs and operator exercises should be evaluated to understand if the personnel required to perform the necessary actions to implement FLEX strategies.

Evaluate:
- if the operators are aware of equipment capabilities
- if the operators are aware of the location of the equipment and ancillary equipment (self-contained breathing apparatus, portable lighting)

- if the operators are aware of the actions necessary to deploy, align and operate the equipment.

Staffing and communications
For each scenario where mitigating strategies are to be credited, it should be confirmed that personnel are qualified to perform required duties and will not be diverted to other tasks such that they would not be available to support the strategy.

Evaluate:
1) availability of the staffing
2) additional staffing
3) reduced staffing (seismic)
4) multi-unit considerations
5) availability of necessary communications equipment
6) absence of competing tasks.

Environmental conditions
Each hazard presents different impacts on the plant and may require the performance of different activities by the available staff depending on the actual environmental conditions. It should be confirmed that staff is capable of operating in the scenario and the impact of the conditions on timings and the complexity of the actions.

Evaluate:
- Challenges to equipment deployment and operation due to accessibility and habitability (failure of buildings, debris, snow or ice, fire, flood). No credit should be taken for deployment in persisting conditions that exceed any personnel protection safety limits.
- Challenges to instrumentation and controls needed to ensure the functionality of the equipment (e.g., communication equipment antenna failed in seismic event).

5.1.3.1.3 Latent errors

FLEX actions might include preparation and arrangement to take place before initiators. Their failure modes would be comparable to latent error modes observed in operational events.

The latent error can cause equipment to be not operational when it is required. This is typically included in the failure data of the equipment and thus included in the PSA model. Only if the latent errors identified are specifically related to FLEX mitigations and have much higher probability than other failures of the equipment, they should be modelled by HRA.

5.1.3.1.4 Example HEPs from Don E. MacLeod 2014

MacLeod et al. (2014) commented that the current HRA methods commonly used are not designed to accommodate the evaluation of some of the tasks associated with the use of portable equipment, such as retrieving equipment and making temporary power and pipe connection. A decision tree method was thus proposed for estimating HEPs associated with the deployment of portable equipment. It suggested that the HEPs of failure to identify the need to initiate portable equipment deployment can be addressed with existing HRA method.

The method is a simplified process that applies adjustment factors to represent the impact of PSFs on a hazard-specific basis on a base HEP. A failure probability of 0.1 is assigned as the base HEP, which is consistent with a screening HEP from NUREG-1792.

An example decision tree for high winds is presented in Figure 11. The method is of necessity bounding in nature and therefore tends to be somewhat conservative. The HEP result should be combined with other components of the human failure event (i.e., decision to initiate deployment, and the use of the equipment once deployed). The other components of HFE are evaluated with 'normal' HRA method.

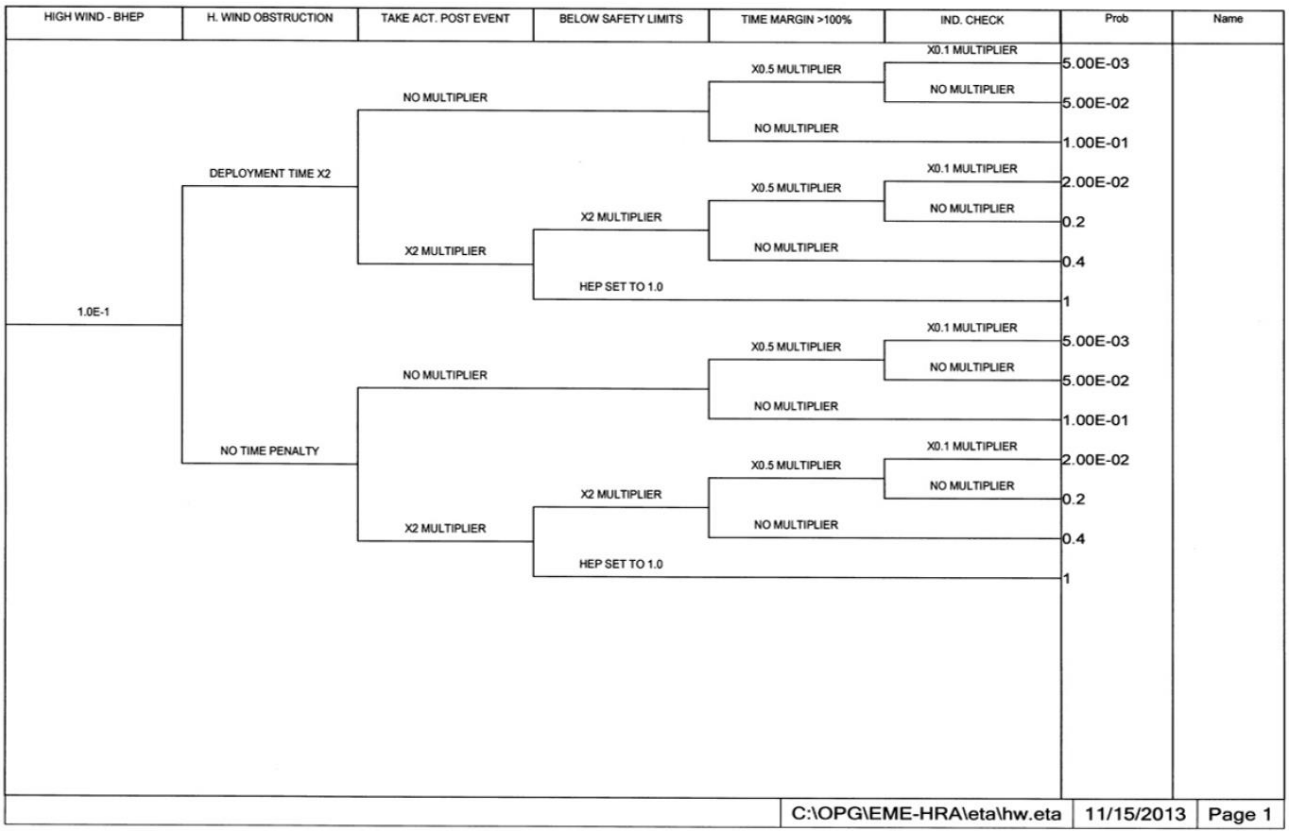

Figure 11. An example decision tree for high winds

5.1.3.1.5 Example HEPs from NEI 16-06

NEI 16-06 (NEI, 2016) outlines a three-tiered approach for evaluating the potential safety benefits of plant mitigation strategies: (Tier 1) qualitative assessment, (Tier 2) semi-quantitative streamlined assessment, and (Tier 3) full probabilistic risk assessment. The Tier 3 approach of NEI 16-06 provides guidance for fully quantifying the impact of mitigating strategies in PSA models that intends to meet the guidance of Regulatory Guide (RG) 1.200.

NEI 16-06 Section 7.5 describes that the current HRA methods are largely based on observed behaviour that does not necessarily translate directly to some human actions required when implementing mitigating strategies with portable equipment. In some cases, engineering judgement will be required to estimate human error probabilities until new guidance on these issues is developed. In these cases, a sensitivity study should be performed to evaluate the impact of these estimates on the PSA results.

It is also highlighted that an additional requirement is to assess the probability that multiple human actions are dependent on each other, so a dependency analysis will be required using existing guidance.

Mitigating strategies may include actions that require many steps over an extended period of time, multiple personnel and locations, evolving command and control, and extended time delays. These types of actions pose several challenges when using existing HRA tools that sum probabilities of failure for each step in a procedure.

Before the HRA method is improved for FLEX, NEI 16-06 proposed that the best approach is to determine either equivalent failure probabilities that are currently addressed by the HRA methodology that can be used as surrogates for specific actions or use engineering judgement to estimate the failure probability. Some of the actions that may not be explicitly addressed in existing guidance or provided in HRA tools include:

- Making decisions to enter a procedure using judgement based on a belief in a future event (e.g., the expectation that offsite power will not be restored in a certain time frame).
- Actions to transport and install portable equipment.
- Actions that require many people working in coordination to complete a single task.

NEI 16-06 proposed the below decision tree for semi-quantitative feasibility assessment, see Figure 12. An initial estimated probability of 0.1 is used for nominal failure of a mitigating strategy where a successful outcome of the initial feasibility assessment has been demonstrated. The actual failure probability used in the assessment can range from 0.1 (likely to succeed) to 1.0 (will not provide additional mitigation capability) for the scenarios of interest.

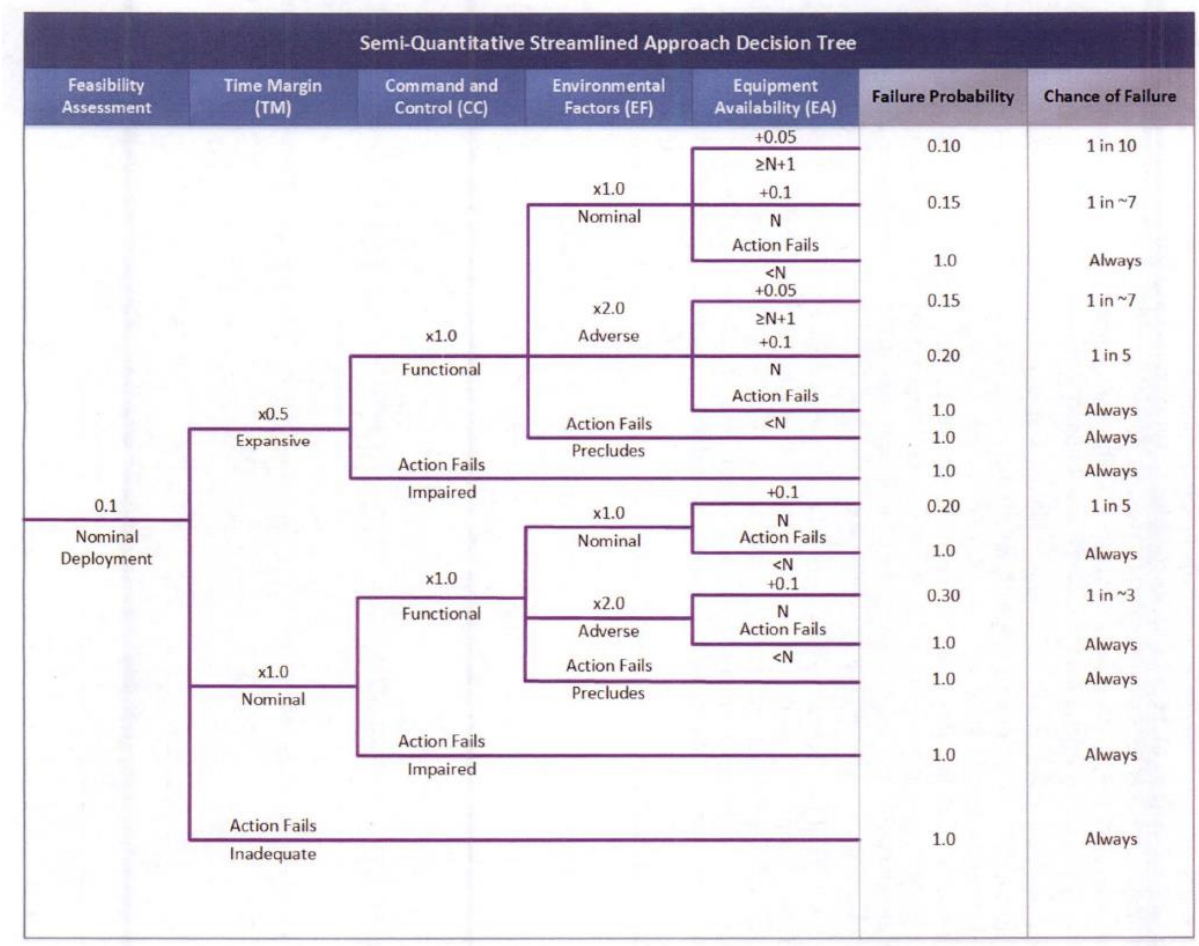

Figure 12. Decision tree for semi-quantitative feasibility assessment

NEI 16-06 Appendix C provides example FLEX actions credited in LOOP. The example focuses on adding the FLEX mitigating strategies to the Internal Events PSA, so it does not include any adverse environmental conditions. Other hazard groups may add additional environmental impacts that affect the probability that a function will succeed.

Table 3. Example 1 from NEI 16-06: Operators fail to load Shed DC Buses (internal events/no debris)

HEP Summary				
	P_{cog}	P_{exe}	Total HEP	Error Factor
Method	CBDTM	THERP	CBDTM + THERP	
Without Recovery	2.0e-03	3.2e-02		
With Recovery	5.0e-04	1.9e-02	1.9e-02	5

For the modelling of failure to deploy and install the FLEX generator, engineering judgement was used in the development of the applicable HEPs. In the absence of an external event that could require additional steps such as debris removal, for this example, the probability of failure to transport and stage the portable generator is judged to be about lE-3; therefore, in the EPRI HRA Calculator, the THERP Table (Reference 19) 20-13, Locally Operated Valves, is chosen and Item 1 is picked to give a probability of failure of 1.3E-3. The remaining execution steps are represented in the THERP Tables and are selected appropriately.

Table 4. Example 2 from NEI 16-06: Operators fail to deploy and install FLEX generator (internal events/no debris)

HEP Summary				
	Pcog	Pexe	Total HEP	Error Factor
Method	CBDTM	THERP	CBDTM+THERP	
Without Recovery	2.00E-03	1.18E-01		
With Recovery	2.90E-04	5.06E-03	5.35E-03	5

Note that the NRC in 2017 published a memorandum assessing NEI 16-06 (Reisi-Fard, 2017). It commented that no basis is provided to justify the estimated value of 1E-3 or to show that the HEP of deploying and installing a generator is similar to the HEP of operating a valve locally.

5.1.3.1.6 Example HEPs from EPRI studies

EPRI in its report on HRA for FLEX (EPRI, 2018) quantifies selected HFEs. The report is not public but a few example results are available in the open presentation slides by Julius (2019). The selected HFEs are quantified using EPRI methods.

Table 5. Example HEPs from EPRI studies

Event Description	Probability of Failure	
	Internal Events	Seismic
Operators Fail DC Load Shed (SBO, Div I Only)	2.5E-02	6.2E-02
Operators Fail DC Load Shed (ELAP)	3.8E-02	9.8E-02
Operators Fail to Align Flex Generator to Div I	3.6E-02	3.7E-02
Operator Fails to Partially Depressurize RPV and Vent Cont. to Prolong RCIC	(<7.2E-02)	7.2E-02
Operators Fail to Align Flex Flow Path to RPV	2.5E-02	2.5E-02

5.1.3.1.7 Example HEPs from US NRC using Expert elicitation method

The NRC staff performed a formal expert elicitation with the purpose of supporting quantification of HEPs associated with the use of portable FLEX equipment (Xing, 2019). The expert elicitation employed a structured process following established NRC guidance. The expert panel consisted of six experts with expertise in HRA, implementation of FLEX strategies, and typical maintenance practices in nuclear power plants. The FLEX HRA expert elicitation project used an expert panel to estimate HEPs for a representative set of FLEX actions under given scenarios and to identify PSFs that are pertinent to FLEX strategies.

Overall, the HEPs for FLEX actions are about an order of magnitude higher than most HEPs for well trained, proceduralized EOP actions in main control rooms (see Table 6). Moreover, the likelihood of failure for the overall FLEX strategy is high. Implementation of the FLEX strategies can fail due to the failure of any of the four key actions: Declaration of ELAP, Load Shed, Use of Portable Generator, and Use of Portable Pump. The experts estimated the overall HEP for failing the four actions is in the range of 0.3~0.6. Yet, the experts were able to justify and defend their judgment. In the experts' justification, the main drivers to the HEPs of the FLEX actions are training and scenario familiarity.

Table 6 Summary of the HEPs (Xing, 2019)

Action	Task	Non-FLEX HEP (1th, 50th, and 99th)			FLEX-scenario HEP (1th, 50th, and 99th)		
Action 1: Use of Generator	Decide	0.016	**0.052**	0.101			
	Transport	0.023	**0.057**	0.27	0.038	**0.14**	0.52
	Connect and start	0.027	**0.088**	0.31	0.043	**0.16**	0.41
	Operate	0.024	**0.052**	0.22	0.036	**0.12**	0.44
Action 2: Use of Pump	Decide	0.034	**0.055**	0.1			
	Transport	0.016	**0.058**	0.23	0.023	**0.12**	0.47
	Connect and start	0.019	**0.078**	0.27	0.036	**0.13**	0.45
	Operate	0.017	**0.05**	0.21	0.043	**0.14**	0.44
Action 3: Refill CST	Decide	0.034	**0.057**	0.11			
	Refilling	0.01	**0.046**	0.28	0.072	**0.14**	0.36
ELAP Declaration	Decide	0.046	**0.31**	0.66	0.089	**0.19**	0.35
Load Shed	Open 18 breakers	0.011	**0.057**	0.22	0.025	**0.08**	0.31

5.1.3.1.8 Example HEPs from KAERI

Jaewhan Kim and his colleagues at KAERI performed a preliminary FLEX HRA (Kim, 2018). The HFE is**: Deploy the 4.16kV AC/480V AC portable generator and connect it to a required AC bus.** It was calculated with EPRI's external event HRA method with surrogate values for actions related to portable equipment not included in the method (Table 7).

Table 7 Example FLEX HFE quantification (Kim, 2018)

Action	**Failure modes**	**HEPs**
Order local emergency response team (via communication system or direct oral communication)	-Omission of Task Initiation -Wrong communication	Initial HEP * recovery error prob. = 6.0E-3 (CBDT Pce) * 5.0E-2 (assuming LD between SS and TSC) = **3.0E-4**
Preparation of essential equipment/tools/ components	EOO	Initial HEP * 'High' stress level * recovery error prob. = 4.2E-3 (Mean) x 5 x (1+19*2.1E-2)/20 = **1.47E-3**
Selection and Loading of the equipment	Selection/loading of wrong equipment from the storage facility	1.3E-3 x 5 x 3.2E-1 = **2.08E-3**
Transportation and Unloading of the equipment	-Damage to the equipment during transportation /unloading -Debris/Obstruction may be intervened on the road in external events	HEP = E_{trans}
Installation/Connection of the portable equipment (i.e., cables and buses)	-Inadequate/loose connection -Connection to wrong object (bus)	-EOM omission of connection: 4.2E-3 (Mean) x 5 x 1.3E-2 = 2.73E-4 -EOC Inadequate/loose connection: 1.3E-2 x 5 x 1.3E-2 = 8.45E-4 -EOC connection to wrong object (bus): 3.8E-3 x 5 x 1.3E-2 = 2.47E-4 • **Sum of HEPs** = 2.73E-4 + 8.45E-4 + 2.47E-4 = **1.37E- 3**
Report to the MCR on the completion of installation /connection and Startup (i.e., generator started and circuit breaker put in)	-Omission of reporting on completion of connection -Omission of reporting generator startup -Section of wrong circuit breaker -Failure of coordination with MCR	-EOM Omission of reporting connection: 2.60E-3 x 5 = 1.3E-2 -EOM Omission of reporting generator startup: 4.2E-3 x 5 x 1.30E-2 = 2.73E-4 -EOC: commission of the generator startup - 3.8E-3 x 5 x 1.30E-2 = 2.47E-4 -EOM: Omission of putting circuit breaker in: 1.25E-3 x 5 x 1.30E-2 = 8.13E-5 -EOC: Commission of putting circuit breaker in: 6.3E-3 x 5 x 1.30E-2 = 4.10E-4 -**Sum of HEPs** = 2.73E-4 + 2.47E-4 + 8.13E-5 + 4.10E- 4 = **1.01E-3**
Refueling task is required for long-term operation, but it is not included in this study		
		Final HEP = 6.23E-3

5.1.3.2 HRA method for FLEX action (Category C): SFP make-up system 2

SFP make-up system 2 is to use portable water pump to inject the salt sea water into SFP. The applied approach is the Forsmark/Ringhals HRA method, as described in section 5.1.2.

As the available time window is very long (72 hours from boiling to fuel uncover), the base diagnosis HEP is expected to be quite low (close to 1E-4) from the time reliability curve.

The scale factors (ki) for the five PSFs are still applicable and are used to adjust the base diagnosis HEP. The discussions in section 5.1.2 is applicable for the category C FLEX action.

When the final diagnosis HEP is already very low, we do not consider recovery of the diagnosis failure.

For this particular FLEX action, only the mental load PSF Kstress =2 as a serious decision needs to be made. The decision to start the make-up system 2 is challenging as this system will provide salt water to the SFP, which has major financial consequences. The other four Ki is still 1.

Note for PSF coordination and communication, Kcoordination is considered as 1. It is justified that in PROSAFE the information would be naturally needed to be communicated between different groups inside and outside of control room. As long as the good condition for communication is in place, it is suggested to consider this as relatively easy to coordinate activities.

As this FLEX action can be considered as Category C human action, the quantification of the post-diagnosis is heavily relied on expert judgement. The quantification itself is quite simplified as described in the Forsmark/Ringhals HRA method.

5.1.3.3 HRA method for FLEX action (Category A/C): Snow removal

Snow removal is a very important action for the plant, since if it is not performed successfully, a few important safety buildings might be damaged by heavy load and safety systems might be impacted.

Snow removal is a special FLEX action which also includes pre-initiator action as preparations and arrangements should take place before initiators. The action also needs to be performed continuously and repeatedly after heavy snow if operators are pre-warned.

The applied quantification method is the Forsmark/Ringhals HRA method. Two options are considered: (1) operators are pre-warned, (2) operators are not pre-warned. The difference between two options is the time window for diagnosis and decision making.

- Diagnosis probability: basis HEP from F/R TRC curve, with 5 PSFs adjustment
- Execution probability: the execution of the actions is to protect critical equipment located in different buildings of the plant. Four conditions are identified to evaluate the execution HEP (see Table 8). For each condition, a probability (selected from: very easy 1E-4, easy 2E-3, normal 1E-2, somewhat difficult 5E-2 and medium difficult 0.1 and very difficult 1) is estimated using expert judgement and the execution HEP = $1 - (1 - P1)(1 - P2)(1 - P3)(1 - P4)$:
    - P1: human resources for the action
    - P2: interface, instructions and training
    - P3: availability of equipment needed for the action and their transport to the required place
    - P4: manoeuvre

Table 8. Probability scale for conditions for post-diagnosis actions related to extreme weather conditions (NPSAG 53-002)

Grade *p*	Condition			
	Human resources	**Interface, instructions, training**	**Equipment**	**Manoeuvre**
Very easy 1E-4	Optimal, practically impossible to fail	Optimal	Optimal, practically impossible to fail	Practically impossible to fail
Easy 2E-3	Resources always exist, no problem with coordination	Very good interface, very clear instructions, very well trained	All equipment exist and can be easily transported	Low complexity, routine manoeuvre
Normal 1E-2	May be concurring activities	Good interface, clear instructions, well trained	Somewhat difficult to get the equipment or to transport them	Some complexity, small confusion risk, routine manoeuvre
Somewhat difficult 5E-2	Likely concurring activities, maybe problems with coordination	Some deficiencies in interface, instructions, or training	Difficult to get the equipment or to transport them	Complex manoeuvre, clear confusion risk
Medium difficult 0,1	Very likely concurring activities, problems with coordination	Evident deficiencies in interface, instructions, or training	Very difficult to get the equipment or to transport them	Very complex manoeuvre due to circumstances, evident risk for failure,
Very difficult 1	Failure is very likely	Failure is very likely	Failure is very likely	Failure is very likely

In PROSAFE, a recovery factor (0.1) is credited for the execution failure in case the operators are pre-warned. With pre-warning, operators and plant personnel have around 12 hours to 24 hours to prepare for the heavy snow weather and thus make the four conditions easier. This is particularly relevant for P1 and P3, as extra human and equipment resources could be deployed for to the plant to prepare for the snow weather condition.

Without pre-warning, the operators will have shortened available time for diagnosis, and also the eventual recovery of the execution failure in terms of human resources and extra equipment will be questioned. Recovery without pre-warning might still be possible but is not credited by default. A detailed analysis will be needed to justify the recovery, e.g., review the resources and perform plant personnel interviews.

5.1.4 HRA method for repair actions

Repair actions involve the elimination or mitigation of the faults that caused a component or system to fail and bringing it to operable state. Examples of repair actions include repairing weather-related losses of offsite power, repair of a pump that failed to start, or replacement of a failed circuit breaker.

In general, before modelling the repair action in PSA, it is suggested to determine the feasibility of repairs for the significant scenarios:

- Is the equipment repairable?
- Can the crew diagnose the need for repair?
- Will the repair be conducted (prioritized)?
- Can it be accomplished in the time available?
- Can the crew gain access to the equipment?
- Are the required staff (with the right skills) available?
- Are there spare parts, materials, tools available for repair?

Estimation of repair failure probabilities requires input from HRA when considering diagnosis, decision, and dependencies to other HFEs. The execution part should be analysed with failure and repair data and will require a distribution for repair time and will also depend on the specific available time.

It is suggested to consider the following time information to evaluate the required repair time:

- Time for communication of the decisions
- Time for transit of plant personnel to equipment location
- Time for access (if required)
- Time to put personal protection equipment (if required)
- Time for obtaining special equipment (if required)
- Time for diagnosis and assessment of equipment status (if required)
- Time for arrival of other plant personnel (if required)
- Time for performing repair action tasks

MTTR from component reliability database, e.g. T-book, provides good data basis of the required repair time. However, it is suggested to investigate what is included in the MTTR in the database and also add the necessary time slots if needed.

Repair probability estimation should consider the following elements (the total of the following probabilities):

- Diagnosis: Detect the failed component and diagnose the need for repair
    - PSFs: available time, cues, instructions, experiences
    - Method: Forsmark/Ringhals HRA method (SPAR-H is used for comparison). Note the dependencies with the preceding HFEs should be considered at the specific MCS.
- Execution: Repair of the failed component
    - Available time, required time (history mean time to repair)
    - Method: Probability distribution can be used considering the available time and mean time to repair. If we assume exponential distribution, Pexe=Exp(-Ta/MTTR), see Figure 13. In the pilot study the available MTTRs from T-book are used. The values should be further evaluated to cover all the required time in the repair execution.
- Availability of the needed materials and personnel
    - Method: expert judgement, using the information from the plant. Note in the current pilot study, this part of the probability is not estimated.

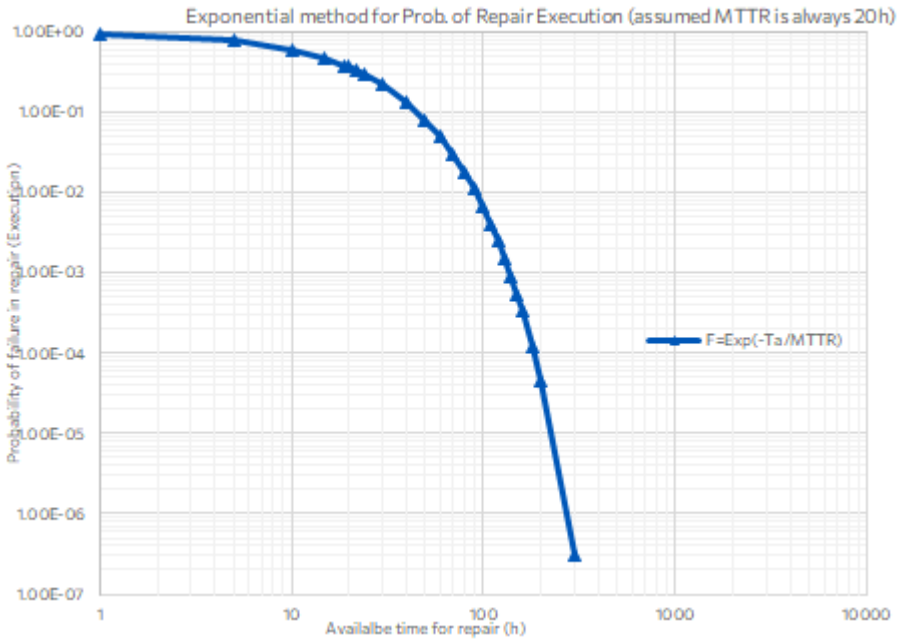

Figure 13. Exponential model for Repair Execution HEP considering available time and MTTR

The main feature of repairs that distinguishes them from tasks that are usually analysed in nuclear HRA is that they involve, besides the operators, another worker group. These are called "field men", and they are mechanics that are responsible of carrying out maintenance and repair work at the plant. They utilize different kinds of instruments, equipment, spare parts and implements that are available at the plant.

The repair may consist of different kinds of activities. Here we assume that it consists of the following main phases:

1. Operators notice that something is wrong. Possibly they try to conduct a tentative diagnosis based on measurements and observations.
2. Operators alert a field man - a mechanic whose duty is to conduct different kinds of repair, maintenance and monitoring work - explain him the deviations observed (and possibly their theory on what is wrong) and ask him to check the situation.
3. The field man walks to the location of the equipment that he assumes to be the culprit of the symptoms observed by the operators.
4. The field man diagnoses the root cause of the observed symptoms, possibly reading or conducting some measurements.
5. The field man decides on the repair actions needed.
6. The field man conducts the actions that vary by repair task. They may consist of fetching equipment, spare parts and means of protection, doing measurements, uninstalling pieces of equipment, doing measurements, adjusting and aligning some parts, replacing broken components with new ones, re-assembly etc.
7. The field man and/or operators test the repaired component or sub-system.
8. The operators recommission the repaired subsystem.

This generic repair procedure is used as a basis of the repair analyses that are described in section 0.

5.1.5 HRA dependencies

Dependency treatment is another element for the multiple HFEs in one MCS. When the recovery actions and repairs are considered in the dominant MCSs, the possible dependencies should be checked and considered on the result.

The rules or decision trees used in the existing PSA study can be used for the prolonged time window. An example model is the decision tree proposed in SPAR-H method (see Figure 14).

Dependency Condition Table

Condition Number	Crew (same or different)	Time (close in time or not close in time)	Location (same or different)	Cues (additional or no additional)	Dependency	Number of Human Action Failures Rule ☐ - Not Applicable. Why?_____
1	s	c	s	na	complete	When considering recovery in a series e.g., 2nd, 3rd, or 4th checker If this error is the **3rd error in the sequence**, then the dependency is at least **moderate**. If this error is the **4th error in the sequence**, then the dependency is at least **high.**
2				a	complete	
3			d	na	high	
4				a	high	
5		nc	s	na	high	
6				a	moderate	
7			d	na	moderate	
8				a	low	
9	d	c	s	na	moderate	
10				a	moderate	
11			d	na	moderate	
12				a	moderate	
13		nc	s	na	low	
14				a	low	
15			d	na	low	
16				a	low	
17					zero	

Figure 14. SPAR-H HRA dependency condition table

Another model is the EPRI HRA dependency decision tree and its latest decision tree model was developed in NUREG-1921 Fire HRA guideline document in 2012 (see Figure 15).

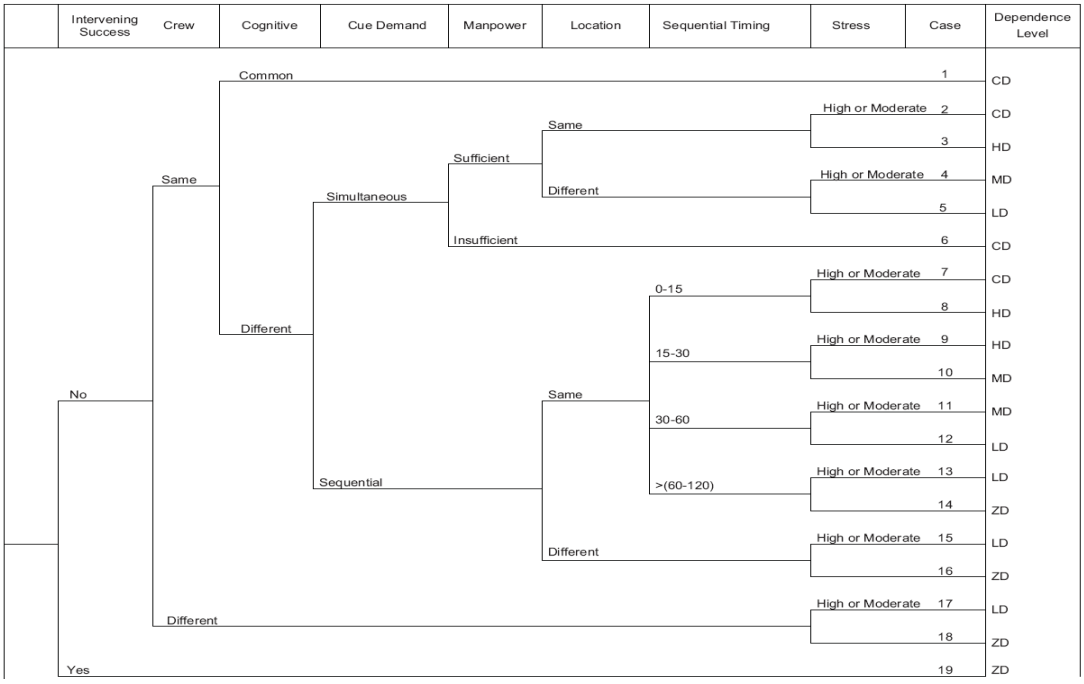

Figure 15. HRA dependency decision tree (NUREG-1921).

For a prolonged time window, the recommendations proposed in the NPSAG HRA dependency projects (He, 2015, 2017) are still applicable. It is suggested to consider the context surrounding the events in question, determine whether dependencies exist between two human actions and then use decision trees to assess the dependency level.

The following rules can be used as justification for zero dependence or independence between HFEs:

Rule 1: separated by a successful action

Cognitive connection between human actions is a crucial criterion for existence of dependencies between human actions. The presence of success may be able to indicate a break in the mind-set of the operators. Therefore, if two HFEs are identified in a cut set and a successful action can be identified between the two HFEs, the two HFEs in that cut set might be considered independent. Please be aware that in the PSA MCSs, the success might not be evident in the cut set (if no negated event is included in the MCSs), but will be seen by following the sequence in the event tree.

Rule 2: separated by a long-time interval (more than 2 hours)

The required actions are separated sufficiently in the development of the accident sequence and stress level is low.

In many cases it is hard to say the exact separation time between two actions since action 2 might be taken right after action 1. However when we know the total available time for action 1 and 2 is more than 8 or 12 hours, it can be assumed that a new shift should arrive within the available time window and provide 'independent' check and recovery to the actions. See Rule 4.

Rule 3: distinct cues

The cues for subsequent actions are independent of those for prior actions.

Rule 4: different crew (when the available time is more than 8 hours, different crews can be assumed for the crews working with 8-hour shift or 12 hour shift)

Zero dependence can be assigned if two actions are performed by different crews and under low stress level.

5.1.6 Limiting HEPs for individual HFEs and multiple HFEs in one MCS

5.1.6.1 Minimum individual HEPs

The majority of the HEPs of nuclear level 1 PSA HFEs are within the range [1E-4, 1E-1], as derived using the existing HRA methods and practices.

Considering the extended time window condition, the following limiting HEPs for individual HFE are recommended:

- < 24 hours, limiting individual HEP is 1E-5 for optimal conditions

- >= 24 hours but < 3 days, limiting individual HEP is 1E-6 for optimal conditions
- > =3 days, limiting individual HEP is 1E-7 for optimal conditions

Please note that most HRA methods will not produce an individual HEP lower than 1E-5 for a category C HFE. When recovery needs to be considered from different personnel/crew for sufficiently long time windows, the HEP might be lower. In principle, we can consider recovery for each new shift. However, it is difficult to justify that each new shift will be independent from the previous shifts. The limiting individual HEP is thus proposed.

The reasonableness of the above limiting values should be checked, and the following typical optimal conditions can be referenced:

- Straightforward, trained and well-understood task led by symptom-based procedures
- Required equipment and instrumentation available
- Need for action signalled strongly/repetitively via diverse and sustained high-level alarms/events
- Sufficiently qualified and experienced personnel available
- Excessive time available (more than triple the time required to complete the action)
- No credible human failure mechanism identified (including via operational experience review and critical incident interviews) other than perverse or extreme ones
- No improvement measures identifiable
- New staff will arrive via shift change and/or new emergency technical advisor(s)

5.1.6.2 Minimum joint HEPs

When there are multiple HFEs included in a cut set, the joint HEP probabilities will be derived considering the individual HEPs and their dependencies.

In addition to the dependency adjustment, it is also recognized by many HRA experts that there should be some limiting values for the joint probability of multiple HFEs within the same cut set. These limiting values are in place to make sure the risk is not underestimated since there are many assumptions and uncertainties in the HEP estimation. 1E-5 is typically suggested as a general limiting value for the joint HEP from a HFE combination in NRC HRA Good Practice (Kolaczkowski et al., 2005). In optimal situations, lower values, e.g. 1E-6 or 1E-7, can be justified.

However up to now, there has been no consensus practice in setting or using such minimum values in the nuclear industry worldwide. Experience has also shown that indiscriminate use of a lower bound joint human error probability can result in technical and process issues, such as potentially inappropriate risk ranking of resulting MCSs and very long quantification times. Furthermore, application of an imposed minimum value as a means to assess unknown or

unquantifiable sources of dependency does not provide information on how to improve plant operational practices to enable operators to cope with accidents.

In NPSAG HRA dependencies project reports (He, 2015, 2017), it is recommended to look at only important HFE combinations (CDF and LERF contributions) and check if their joint probabilities go much lower than 1E-5 or 1E-6 after dependencies have been incorporated.

In PROSAFE extended timescale situations, the following is recommended:

- If HFEs in the important combinations are already judged to be independent, it is recommended not to apply the limiting value.

- If HFEs in the important combination are judged as dependent, it is recommended to apply limiting values, which shall not be a fixed value. It is recommended to start with the limiting value 1E-5. For the long time window situations, a few lower limiting values (e.g. 1E-6 or 1E-7) can also be applied for optimal conditions with extended timescale (e.g. > 12 hours or > 24 hours).

- If the timescale is more than 24 hours, it is recommended not to apply the limiting value.

5.1.7 ASEP

VTT's HRA pilot is based on ASEP (Swain, 1987), which is a shortened and simplified version of THERP (NUREG/CR-1278, U.S. NRC, 1983), and likewise places emphasis on nuclear power plant applications. It is intended to enable systems analysts and other non-HRA specialists to make estimates of HEPs and other human performance characteristics in a manner that is easy to learn and use, and also sufficiently accurate for many PSAs. These objectives, together with the scope of handling both pre-accident and post-accident HRAs, have led to the methodological choice that the ASEP procedure resembles a cookbook: the user follows a list of instructions, and looks up HEPs from tables and figures. When the cookbook instructions do not handle the HRA modelling task well, the analyst is referred to the respective parts in THERP; on the other hand, ASEP contains some complements to THERP as described in NUREG/CR-1278, such as the estimation of effects of using symptom-oriented emergency operating procedures. ASEP's handling of timings is simplistic: the procedure of calculating the execution time of post-accident actions is very crude, and no procedure for calculating the execution time of post-accident diagnosis is given.

The ASEP procedure consists of four sub-procedures: pre-accident screening HRA, pre-accident nominal HRA, post-accident screening HRA, and post-accident nominal HRA. As the objective of screening HRA is to assess what human actions to analyse in nominal HRA, and the human actions to be considered have been chosen by other means in PROSAFE, ASEP screening HRAs will not be considered here. As pre-accident human actions play no role in the Finnish PROSAFE PSA pilot, pre-accident nominal HRA will also not be considered. Thus, we will consider only post-accident nominal HRA here.

Post-accident tasks are divided into diagnosis and action. Time needed for action is estimated first, and based on that, the time available for diagnosis is calculated by subtracting action time from total available time.

The nominal diagnosis model of THERP is used. The diagnosis HEP is looked up from a time-reliability curve (or table) where the time used is the time available for diagnosis. The diagnosis

model of ASEP does not include performance shaping factors (PSF). Instead, the steps of the diagnosis contain rules to adjust the nominal diagnosis HEP upwards or downwards in the time-reliability curve - from nominal to maximal or nominal to minimal, for example.

The HEPs of post-diagnosis actions are chosen from a table, with a main distinction being made between dynamic (non-routine, interactive, involving several functions etc.) and step-by-step (routine, procedurally guided) tasks. Also a distinction is made between moderately high stress and extremely high stress tasks (it is assumed that post-accident tasks involve hight stress). If a task analysis exists and contains enough information, HEPs are obtained from THERP tables, and its performance shaping factors and recovery factor scheme are used. Otherwise, the HEPs are chosen from three alternatives, classified according to stress level and action complexity. The HEPs of error recoveries are chosen from four alternatives, each of which has certain conditions; if the conditions are not met, the advice is given to conduct a separate analysis.

It is of some interest to see how applicable ASEP in the HRA of repairs and FLEX actions. Repair actions, and likely also FLEX actions, are mostly such that are not conducted normally by operators, and thus it is unclear how valid the HEPs provided by ASEP are. Thus, comparisons of ASEP results with those obtained by applying the Ringhals-Forsmark method and SPAR-H may shed some light on whether the HEPs of activities provided by ASEP are sufficiently accurate from a practical point of view, or whether perhaps new and more accurate HEPs would be needed for the HRA involving repair and FLEX activities. The preliminary findings presented in section 5.2.3.1 shed some light on this question from one point of view.

To conduct the analysis, we need to have an understanding of how repair work is carried out. As a proper task analysis is impracticable in the present context, we proceed on the following grounds.

5.2. Pilot studies

5.2.1 HRA results in Swedish pilot studies

5.2.1.1 HRA Scenario and HFEs in PROSAFE

The initiating event (transient, LOOP or external event) is assumed to cause loss of residual heat removal due to stop of operational cooling train. The crew will then try to initiate/recover cooling with train 2, 3 or 4 (start of a stand-by train). In LOOP situation the cooling train 1 is also available and we assume the train 1 will be started automatically when the power is recovered. If train 1 fails, the crew needs to switch to other trains. The available time to initiate or start a stand-by SFP cooling train is assumed to be 24 hours before boiling.

It is assumed that make-up is initiated after boiling has occurred (although the level in the SFP can decrease somewhat before the cooling function is lost due to loss of suction). After start boiling it is assumed that the crew (in main control room) will initiate/start make-up system 1 (available time 72 hours assumed after boiling, before uncovered fuel in SFP) to maintain water level in the SFP and compensate for water losses due to boil off effects. Failure of make-up system 1 will lead to the activating of make-up system 2. Note that make-up system 2 will not be initiated unless absolutely necessary as this system will provide sea water to the SFP.

In extreme weather conditions (snow), snow removal is considered for two conditions: with pre-warning and without pre-warning. This HFE will be modelled in both the SFP model and reactor model as it will impact safety systems used in both models.

Based on the scenario above, the following post-initiator human actions are considered:

- Start (standby) SFP cooling train when the operating train stops before boiling
- Start make-up system 1 before uncovered fuel
- Start make-up system 2 before uncovered fuel (FLEX)
- Snow removal with pre-warning (FLEX)
- Snow removal without pre-warning (FLEX)

The following repair actions are evaluated in the pilot study:

- Repair SFP cooling before boiling
- Repair Make-up 1 before uncovered fuel
- Repair the SFP cooling system while the water make-up is working
- Repair the DG before SFP boiling
- Repair the DG from IE to fuel uncover

5.2.1.2 Start (standby) SFP cooling before boiling

To start the standby SFP cooling trains when the operating train stops is the first HFE in the sequence. Total available time is 24 hours. Operators in the main control room may notice the alarm right after the operating pump is stopped. It will take longer time to notice if the heat exchanger is leaking. It will take a few hours for the temperature and water level alarms. It is also assumed that every shift (every 8 hours) should check the SFP parameters and thus notice the problem.

The required time for execution (to switch to one of the standby systems) is assumed as 1 hour as the action might be taken locally.

Diagnosis part
Method: F/R HRA method

The available time for diagnosis is assumed as 24 -8 -1 =15 hours. It is assumed with 8 hours to notice the alarms/parameters related to the loss of SFP cooling.

The basic HEP is thus 4.5E-4.
The Ki multipliers from 5 PSFs are 1.

The final diagnosis HEP is 4.5E-4.
As the HEP is already very low, we do not consider further recovery of the diagnosis failure.

Execution part
Method: F/R HRA method
The probability scale for the post-diagnosis execution is considered as normal 0.01. As there is plenty of time, the recovery of the execution is very likely and thus we choose recovery failure probability 0.1 to the execution HEP. The final execution HEP is 1E-3.

5.2.1.3 Start make-up system 1 before uncovered fuel

If cooling fails for 24 hours, the spent fuel pool will start boiling. It is assumed that make-up is initiated after boiling has occurred (although the level in the SFP can decrease somewhat before the cooling function is lost due to loss of suction). After the start of boiling it is assumed that the crew (in the main control room) will initiate/start make-up system 1 (available time 72 hours assumed after boiling, before uncovered fuel in the SFP) to maintain water level in the SPF and compensate for water losses due to boil off effects. Failure of make-up system 1 will lead to the activating of make-up system 2 (FLEX action using portable equipment to take the sea water). If no actions are taken this will eventually lead to fuel damage (available time 72 hours assumed, from the start of boiling to uncovered fuel). Since the level in the fuel pool decreases during boiling, it will not be possible to go directly from this state to restart of cooling since the water intake to the pumps are placed near the top of the fuel pool.

The required time to start make-up system 1 is assumed as 1 hour.
The required time to start make-up system 2 is assumed as 2 hours.

Diagnosis part
Method: F/R HRA method

The indications (alarms) are obvious in this case as the SFP is boiling.
The available time for diagnosis is assumed as 72- 1 -2 =69 hours.
It is assumed when the SFP is boiling, the plant emergency manager will be in place and make the decision.

The basic diagnosis HEP is 1.7E-4.
The Ki multipliers from 5 PSFs are 1.
The final diagnosis HEP is 1.7E-4.

As the HEP is already very low, we do not consider recovery of the diagnosis failure.

Execution part
Method: F/R HRA method

The probability scale for the post-diagnosis execution is considered as normal 0.01. As there is plenty of time, the recovery of the execution is very likely. Considering there are plenty of times for multiple shifts to perform multiple tries within every shift, the recovery is at least 0.1*0.5=0.05.
The final execution HEP is 5E-4.

5.2.1.4 Start make-up system 2 before uncovered fuel (FLEX)

Failure of make-up system 1 will lead to the activating of make-up system 2 (FLEX action using portable equipment to take the sea water). If no actions are taken this will eventually lead to fuel damage (available time 72 hours assumed, from the start of boiling to uncovered fuel).

The required time to start make-up system 2 is assumed as 2 hours.

Diagnosis part to start make-up system 2 (FLEX)
Method: F/R HRA method

The indications (alarms) are obvious in this case as the SFP is boiling. The make-up system 2 will be started by the operators when make-up 1 is failed. Make-up 1 can be failed by human errors (as quantified above) or hardware failure. The available time for make-up 2 could be different for different failures in make-up 1.

In our analysis, the available time for make-up 2 diagnosis is assumed as 72- 1 -2 =69 hours. It is assumed when the SFP is boiling, the plant emergency manager will be in place and make the decision.

This assumption might not be conservative, especially if make-up 1 is failed by human error, the available time for make-up 2 might be less as the operator might still try to work on make-up 1 for a while. One option would be that we assume operators will wait for some hours to start make-up 2. However, this does not mean operator will not think/diagnosis make-up 2 as a barrier, they just want to wait for some hours to perform make-up 2. In addition, as the available time window is so long, the basis HEP is not sensitive and there is no strong need to provide exact estimation of the available time (see Figure 7).

Anyway we will consider the dependencies in the MCSs where two human actions (on make-up 1 and make-up 2) are together. The dependency level will be evaluated, and post-process will be used in RiskSpectrum to consider the conditional HEP.

The basic diagnosis HEP is 1.7E-4.
The mental load PSF Kstress =2 as a serious decision needs to be made. The decision to start the make-up system 2 is challenging as this system will provide sea water to the SFP. The other four Ki multipliers are still 1.

The final diagnosis HEP is 3.4E-4.
As the HEP is already very low, we do not consider recovery of the diagnosis failure.

Execution part to start make-up system 2 (FLEX)
Method: F/R HRA method

The probability scale for the post-diagnosis execution is considered as somewhat difficult 0.05. This is FLEX action and the execution consists of deployment and start of the pump.
As there is plenty of time, the recovery of the execution is very likely. The final execution HEP is 0.05*0.1 = 5E-3.

5.2.1.5 Snow removal with and without pre-warning (FLEX)

Diagnosis part of snow removal with pre-warning
A pre-warning will be given to plant personnel 24 hours before the heavy snow (over 90mm) or 12 hours before heavy snow (over 20mm) occurs. Thus in PROSAFE, if pre-warning is given, the total available time is assumed as 12 hours. The T_0 is assumed as 0 hour (required for indication). The execution time is 1 hour. Available for diagnosis is 11 hours.

The basic diagnosis HEP is 5.4E-4.
Ki multipliers are assumed as 1.

The final diagnosis HEP for snow removal with pre-warning is 5.4E-4. We do not consider recovery as the HEP is quite low.

Diagnosis part of snow removal without pre-warning
Method: F/R HRA method

If pre-warning is not given, the total available time is assumed as 2 hours. T_0 is assumed to be 0 hour (required for indication). The execution time is 1 hour.

The basic diagnosis HEP is 3.0E-3.
Ki multipliers are assumed as 1.

The final diagnosis HEP for snow removal without pre-warning is 3E-3. We do not consider recovery as the HEP is quite low.

Execution part of snow removal without pre-warning
Method: F/R HRA method for local actions

The probability scale for the post-diagnosis execution regarding snow removal is evaluated according to four conditions which must be satisfied for a successful outcome. For each condition, a probability scale is applied (see Table 8). For assumed snow removal during extreme weather conditions the following probability scale (Grade p) is assumed:

- Human resources (p=0.1)
- Interface, instruction and training (p=0.01)
- Equipment (p=0.05)
- Maneuver (p=0.01;)

Failure probability of the post-diagnosis action is: 1-(1-0.1)(1-0.01)(1-0.05)(1-0.01)=1.62E-1.

Execution part of snow removal with pre-warning
Method: F/R HRA method for local actions

With pre-warning on snow, the plant will have 12 hours before the snow to prepare the required human resources and extra equipment, if needed. So it is suggested to credit additional recovery 0.1 on the above execution HEP for snow removal without pre-warning.

Recovery is credited for execution considering when pre-warning is given, the plant has a long time to call for people that are required for coping with extra-snow and other required resources. This will increase the success probability to ensure sufficient human resources and other resources at site within the time window.

Failure probability of the snow removal execution with pre-warning is thus considered with recovery: 1.62E-1 * 0.1 =1.62E-2.

5.2.1.6 Repair SFP cooling before boiling

Repair of SFP cooling is to repair the failed cooling train. As there are redundant trains in the cooling system, the operators are expected to try to start the standby cooling trains. As there is long time available, it is also expected that the operators will start to diagnosis why the cooling train is failed and try to repair the malfunctional trains.

To meet the need of the PSA modelling, the repair of the SFP cooling is considered for two situations: repair the cooling before SFP boiling (24 hours) and repair the cooling while the water make-up is working (2 weeks). Note if any of the standby trains are working, in such case the repair of the train 1 will be performed with extensive available time and thus it will be very likely. The second situation is discussed in a later section.

Diagnosis part of the repair of cooling before boiling
Method: Forsmark/Ringhal HRA method
The available time for repair is assumed as less than 24 hours. It might be performed for:

- Train 1 (repair the initiating event). As the pump is in operation, the possible failure mode for the pump is fail in operation. The MTTR for a pump failure in operation is 24 hours according to T book. The MTTR for the heat exchanger leak is 11 hours. To be conservative, we use the maximum MTTR as the time required for repair execution. The time available for repair diagnosis = total available time - MTTR (max) <0. This means train 1 has a low probability to be repaired before boiling. A conservative screening HEP=1 could be assigned. Note this does not mean the plant personnel will not start to prepare the repair before boiling. The repair work can be started before boiling and it will be continued until it is repaired successfully (see 5.2.1.8).
- Train 2/3/4. Same as train 1, the repair of the cooling is not considered before boiling.

5.2.1.7 Repair Make-up 1 before uncovered fuel

Diagnosis part of Repair of Make-up 1 before fuel uncovered in SFP
Method: Forsmark/Ringhal HRA method
Total available time to repair make-up system 1 is 69 hours. It is assumed that the operators will start the repair of make-up 1 as soon as they fail to start make-up 1. We have assumed that

the execution of the make-up 1 takes about 1 hours. It is thus assumed that the operators will have about 72-3 = 69 hours available for repair.

The MTTR for make-up system 1 pump is 12 hours for failure mode fail to start and 24 hours for failure mode fail in operation. It is thus assumed that 24 hours are needed to perform the repair task for the pump.

The available time for repair diagnosis is 69-24 = 45 hours.
The basic diagnosis HEP is 2.2E-4.

K procedure =2, procedure is imperfect. The repair is not specifically mentioned or instructed.
K training =2, some training has been given but is not fully applicable for the situation.
K coordination =2, coordination of many activities with good condition for communication.

The final diagnosis HEP is 2.2E-4*8 = 1.76E-3.

Execution of Repair of Make-up 1 before uncovered fuel in the SFP
Total available time for repairing the make-up system 1 is 69 hours.
The required time for diagnosis is assumed as 2 hours.
The available time to perform repair action (execution) is thus 67 hours.
MTTR is 24hours.

The execution HEP is thus: Exp(-Ta/MTTR) = 6.13E-2

5.2.1.8 Repair the SFP cooling system while the water make-up is working

When a make-up system is operating (or repaired), the water level in the pool will be restored and the cooling system should be re-activated. The cooling system needs to be repaired and the available time for this action is determined by the reliability of the make-up system. That is, as long as one of the make-up systems works, there will be sufficient time to repair the cooling system (available time for repair is minimum of the pump's mean time between failures and possible other limitations, e.g., the water sources for the make-up systems).

Diagnosis part of Repair of the cooling system while the water make-up is working

The failure rate for the make-up pump 1 is 5E-6/hour. The mean time to failure (MTTF) is 2E5 hours.
The possible other limitation is assumed as 2 weeks (336 hours).

The MTTR is 24 hours.

The diagnosis HEP is 1E-4 (the cut off value).
K procedure =2, procedure is assumed as imperfect. It is assumed that the repair is not specifically mentioned or instructed.
K training =2, some training has been given but is not fully applicable for the situation.
K coordination =2, coordination of many activities with good condition for communication.
Recovery: 0.1 as the time window is extremely long (weeks)

The final diagnosis HEP is 1E-4*8*0.1 = 8E-5 (recovery is credited)

Execution part of Repair of the cooling system while the water make-up is working

Total available time for repair is 336 hours.
The required time for diagnosis is assumed as 2 hours.
The available time to perform repair action (execution) is thus 334 hours.
MTTR is 24 hours.
The execution HEP is Exp(-Ta/MTTR) = 9E-7, can be considered as 0.

5.2.1.9 Repair the DG before SFP boiling

In LOOP situation if the DG is failed, the crew will try to repair the DG. The available time for DG repair is 24 hours before boiling, and 72 hours before fuel uncovery (after boiling has started).

MTTR for DG is 6 hours for fail to start and 10 hours for fail in operation. So in HRA, we assume nominal repair execution time is 10 hours.

The indication time is assumed as a few minutes.

Diagnosis of Repair of the DG before boiling
Total available time is 24 hours. The MTTR is 10 hours for failure mode DG fail in operation.
The available time for diagnosis is 24-10 =14 hours.
The basic diagnosis HEP is 4.7E-4.

K procedure =2, procedure is imperfect. The repair is not specifically mentioned or instructed. At the same time, when LOOP and loss of DG occur, it is quite urgent situation and there might be several mitigation measures that need to be taken. It is expected that operators will ask field engineers to check DG as this is obviously high priority to recover power supply.
K stress =5, loss of DG is critical in LOOP situation and the mental load and stress is high.
K coordination =2, coordination of many activities with good condition for communication.
The final diagnosis HEP is 4.7E-4*20 =9.4E-2.

Execution of Repair of the DG before boiling
Total available time for repair is 24 hours.
The required time for diagnosis is assumed as 2 hours.
The available time to perform repair action (execution) is thus 22 hours.
MTTR is 10 hours for failure mode DG fail in operation.

The execution HEP is Exp(-Ta/MTTR) = 1.1E-1.

5.2.1.10 Repair the DG from IE to fuel uncovery

Diagnosis of Repair of the DG before fuel uncovery
Total available time from IE LOOP until fuel uncovery is 96 hours. The MTTR is 10 hours for failure mode fail in operation.
The available time for diagnosis is 96-10 =86 hours.
The basic diagnosis HEP is 1.5E-4.

K procedure =2, procedure is imperfect. The repair is not specifically mentioned or instructed.

K stress =5, loss of DG will impact both the reactor and SFP, and the mental load and stress are high.
K coordination =2, coordination of many activities with good condition for communication.

The final diagnosis HEP is 1.5E-4*20 = 3.0E-3.

Execution of Repair of the DG before fuel uncovery
Total available time for repair is 96 hours.
The required time for diagnosis is assumed as 2 hours.
The available time to perform repair action (execution) is thus 94 hours.
MTTR is 10 hours for failure mode fail in operation.
The execution HEP is Exp(-Ta/MTTR) = 8.27E-5.

5.2.1.11 Summary of HEPs and HRA dependency adjustment

Table 9 and Table 10 list the summary results from the above quantification.

Table 9. Summary of category C and FLEX HFE results

HFE Description	TW (h)	T_{delay} (h)	T_{exe} (h)	HEP Diagnosis	Diagnosis Recovery	HEP Execution	Execution Recovery	Total
start (standby) SFP cooling before boiling	24	8	1	4.50E-04	No	1.00E-03	Yes, 0.1	1.45E-03
start make-up system 1 before uncovered fuel	72	0	1	1.70E-04	No	5.00E-04	Yes, 0.1*0.5	6.70E-04
FLEX, start make-up system 2 before uncovered fuel	72	1	2	3.40E-04	No	5.00E-03	Yes, 0.1	5.34E-03
snow removal with pre-warning	12	0	1	5.40E-04	No	1.62E-02	Yes, 0.1	1.67E-02
snow removal without pre-warning	2	0	1	3.00E-03	No	1.62E-01	No	1.65E-01

Table 10. Summary of repair HFE results (Note a few repair HEPs can be considered as optimal as MTTR is directly from T-book for a boundary failure mode without adjustment for the plant situation in the specific scenarios; the required human resources and spare parts are assumed as available)

Repair actions	T_{avail}	T_{cog}	MTTR	HEP Diagnosis	Diagnosis Recovery	HEP Execution	Execution Recovery	Total
Repair SFP cooling before boiling	15	2	24	1	No	5.82E-01		1
Repair Make-up 1 before uncovered fuel	69	2	24	1.76E-03	No	6.13E-02	No	6.30E-02
Repair SFP cooling system while the water make-up is working	336	2	24	8.00E-05	Yes, 0.1	9.04E-07	No	8.09E-05
Repair the DG before boiling	24	2	10	9.40E-02	No	1.11E-01	No	1.94E-01
Repair the DG from IE to fuel uncover	96	2	10	3.00E-03	No	8.27E-05	No	3.08E-03

In order to evaluate the dependencies among the diagnosis HFEs, the top MCSs are checked and the multiple diagnosis HFEs identified.

The diagnosis HFE to start make-up 1 appears in the same MCS with the diagnosis HFE to start make-up 2.

Dependency level is judged as Low Dependency, considering the following factors:

- Same crew or not: same crew will diagnosis the two make-up systems, however as the available time window is 72 hours, there will be several crew shifts.
- Close in time or not: No (72h time window)
- Procedure: unclear. It is assumed that different procedures are used as the start of make-up system 2 is a FLEX action. The condition to use make-up 2 is stricter as it will use sea water.
- Same location or not: Diagnosis is performed in the MCR, but execution places are different.
- Additional cues: No. Both HFEs rely on same types of alarms. However there might be additional alarms when the water level is decreased continuously.
- Stress level: Low-moderate stress level.

Note: if the diagnosis is judged as same for make-up 1 and make-up 2, and make-up 2 is never used if make-up 1 system is feasible, it is more appropriate to assume complete dependency among them. In such case, a common diagnosis HFE can be used. The extended available time can then be as a recovery factor to justify a lower diagnosis HEP.

Table 11. Dependency adjustment for the second diagnosis HFE2.

	HFE1: Diagnosis of make-up 1	**HFE2: Diagnosis of make-up 2**
HEPs	1.70E-04	3.40E-04
HEPs after adjustment	1.70E-04	5.03E-02

5.2.2 HRA results of VTT pilot studies

5.2.2.1 HRA scenarios and HFEs in the Finnish pilot

The following post-initiator human actions are based on the PROSAFE SFP model. However, in some cases, much longer time windows are assumed than in other analyses described in this report.
The following post-initiator human actions are considered:

- Deployment of the second redundancy of the main SFP cooling system
- Deployment of make-up system 1 before uncovered fuel
- Deployment of make-up system 2 before uncovered fuel (including deployment of FLEX diesel generator)

The following repair actions are evaluated in the pilot study:

- Repair of the main SFP cooling system before boiling. The repair items considered for the first redundancy are pump stopping and failure of heat exchanger. For the other redundancies, also failure to start pump is considered.
- Repair of make-up system 1 before uncovered fuel. The only repair item is pump failure.

- Repair of make-up system 2 before uncovered fuel. The repair items considered are FLEX DG failure and pump failure.

All of these are modelled and analysed with ASEP.

5.2.2.2 Deployment of the second redundancy of the main SFP cooling system

This is the analysis of the human action "deployment of the second redundancy of the main cooling system" for the PROSAFE spent fuel pool PSA model. Because the human action "deployment of make-up system 1" seems identical to the "deployment of the second redundancy…" human action, this analysis serves also as the analysis of that human action. The only difference is that as make-up system 1 will be deployed only after the deployment of the 2nd redundancy has failed, there will be less time available for the deployment of make-up system 1; however, as there is ample time for the actions even after the attempt to deploy 2nd redundancy (see Step 3 below), this does not affect the analysis. The ASEP procedure for nominal (post-initiator) HRA (Swain, 1987, Chapter 8) is followed. The steps below are the steps in table 8-1 of the ASEP manual (Swain, 1987), and also all of the references to tables and figures in the following are references to (Swain, 1987), unless otherwise indicated.

The steps are as follows:

1. Preparatory.
2. It is assumed that a symptom-oriented emergency operating procedure is available for the action. It is assumed that the instrumentation works (otherwise, set HEP=1.0).
3. Available time: in an unpublished VTT report where a deterministic physical model of SFP was developed and accidents analysed, the time to boiling was estimated as 6 days (144 hours) from the loss of cooling, and the time to rod uncovering 36 days (864 hours). However, to facilitate better comparability with the Swedish model, the former is denoted as T_m, the time available for diagnosis and the human action combined.
4. The main operator actions are assumed to be
   - Start-up of pumps (2 pieces)
   - Open the valves of the water pools (2 pieces) to be used by the 2nd redundancy
   - Open the valve of the coolant circulation for the 2nd redundancy

   It is assumed that all of these actions are critical, that is, all of them must be performed correctly in order for the task to be successful.
5. It is assumed that the manipulation needed in conducting the activities listed in step 4 take place outside the main control room. Otherwise:
   a. After a correct diagnosis, the operators spend 5 minutes to read EOP.
   b. It is assumed that the SFP controls are not in the primary operating panels.
   c. They spend 2 minutes of travel and manipulation time for each control action, for a total of 6 minutes. Both times a and c are negligible in comparison with the available time.
6. It is assumed that the time to walk to the places where the actions listed in step 4 can be performed takes 5 minutes, and the time it takes to carry out the actions takes 10 minutes for the start-ups and 1 minute for opening each of the valves. We assume two operators will take the action.
7. The time needed for actions $T_a = 5 + 10 + 1 + 1 = 17$ minutes (assumption: the operators work in parallel).
8. The time allowable for diagnosis $T_d = T_m - T_a$ = 144 hours - 17 minutes.

9. From Table 8-2, item 6, it is estimated that the nominal diagnosis HEP is 1E-5.
    a. This diagnosis HEP is considered to be the probability of misdiagnosis which will eventually result in a fuel damage accident. Thus it is appropriate to adjust the HEP upwards to its upper bound 1E-4.
    b. For the accident sequence to be evaluated, only one diagnosis is required (since redundancy 1 has been lost, water flow measurement is probably close to 0).
    c. The event is covered in training. However, it is unclear whether the event is practiced regularly. Thus it is appropriate to keep the HEP in the upper bound.
    d. Symptom-oriented EOP is available. The event is most probably covered in the EOP. The control room operators have most likely been trained in the use of symptom-oriented EOPs. However, it is not known how many of them will use the EOP instead of trusting their memory, so a 0.5 probability is assessed that the appropriate operator will use the EOPs in a step-by-step manner instead of depending on their memory. Thus, conservatively, the HEP is not adjusted. The EOPs are probably well-designed.
    e. The action does not deal with reactor vessel/containment critical parameters.
    f. All control room operators have probably been trained to quickly initiate action, so the probability of diagnosis error is negligible. However, it seems that the situation described in 9f is not applicable in the present context. Therefore no adjustment of HEP is done.
    g. The diagnosis task in this case is simple, and diagnosis errors are not credible. Therefore it could be concluded that diagnosis HEP is negligible. However, because there is not much information on the (imaginary) plant available, and to keep the analysis conservative, we assume that the HEP arrived at above, 1E-4, holds.
10. Since sufficient information cannot be obtained from task analysis, Table 8-5 is used to obtain the HEPs of the post-diagnostic human actions listed in Step 4. Since the time available for the actions is abundant, it is concluded that the lower of the applicable risk levels, moderately high stress, can be assumed. Furthermore, all the actions (starting of pumps, opening of valves) are parts of a step-by-step task and not a dynamic task. Therefore, the HEP of each action is 0.02. Then, the probability of the action failing is $1-(1-0.02)^5=0.096$. Alternatively, one may assume that the actions are well-trained and easy; then the HEP of each of them is 0.001 (table 8-5, item 10), and the HEP of the whole action failing is $1-(1-0.001)^5=0.005$.
11. Due to the ample time available, recoveries are also possible for each action. ASEP does not specify how this should be done. An event tree model, described in section 5.2.2.2.1 below, was constructed and implemented as a Microsoft Excel worksheet. Taking into account recoveries, the HEP of this task is 0.002.
12. This step - using the obtained HEP values in the PSA model - takes place outside of HRA.

5.2.2.2.1 Recovery model

Here recovery means recovery from error, that is, the human error is noticed and a corrective action is taken before the error leads to irreversible consequences; this is the way recovery is understood in Table 8-5 of (Swain, 1987). We consider both recovery from diagnosis error and recoveries from errors in the post-diagnosis actions. The following assumptions are made:

- diagnosis, possible recovery from diagnosis error, actions, and possible recoveries from failed actions are conducted in this order; that is, first the diagnosis, then recovery from diagnosis error (if any), then the actions etc.

- wrong diagnosis without successful recovery (that is, the correct diagnosis will not be made before action) will lead to failure of the task
- diagnosis and action are independent in the sense that initial failure of diagnosis, if recovered, does not affect the success probabilities of actions
- all actions must be performed correctly, either directly or by recovery from failed execution
- each of the recoveries consist of 1) another crew member verifying the correctness of the diagnosis/action, and 2) the diagnosis/action redone.

Under these assumptions, the calculation of the HEP is organized into an event tree. The sections of the tree are as follows:

- diagnosis success/failure
- failed diagnosis recovery success/failure
- actions success/failure
- failed actions recoveries success/failure

Each sequence of the tree has one of two possible labels attached to it: OK or FAIL. OK means that the task was carried out successfully and FAIL means that the task failed.

The failure probabilities in each section are calculated as follows:

- Diagnosis failure probability is 0.0001 (see Step 9, part g in the previous section)
- Diagnosis recovery failure probability is assessed as follows. As an error in the diagnosis has been found, it is likely that the correct action will be taken. However, as there is less time available for the re-diagnosis, it is conservatively assumed that the HEP of diagnosis recovery is 0.001 (Table 8-2, item (4)).
- The HEP of each action is 0.02, as explained in the section above. This allows us to condense the event tree somewhat. As all action failure probabilities are equal and action failures are assumed to be independent, all cases having the same number of action failures can be lumped together to form a single branch in the event tree, and the binomial distribution can be used to calculate the probability of n failures (n=0, 1, …, 5). That is, the probability of the branch is Bin(n, HEP_{action}, 5).
- The HEP of action recovery may be calculated as follows. Since all actions need to be performed correctly for the task to be executed successfully, in recoveries all the actions that failed in the first round need to be performed correctly in the recovery. We assume that each recovery of an action is more or less re-doing that action, but correctly this time. Furthermore, we assume that the HEP of action recovery includes also the possible error made in the verification of the action. Thus, we may attach the same human error probability $HEP_{actionrecovery}$ for each action recovery, that is, 0.02. Since each failed action needs to be recovered, the probability of successful recovery from n action failures is $(1- HEP_{actionrecovery})^n$.

The event tree was implemented in Microsoft Excel (Figure 16).

diagnosis OK	diagnosis recovery OK	actions OK	actions recovery OK	probability	status
0,9999		0,903830405		0,90383	OK
		0,092227592	0,09038304	0,090383	OK
			0,001844552	0,001845	FAIL
		0,003764392	0,003615322	0,003615	OK
			0,00014907	0,000149	FAIL
		7,68243E-05	7,23064E-05	7,23E-05	OK
			4,51788E-06	4,52E-06	FAIL
		7,83922E-07	7,23064E-07	7,23E-07	OK
			6,08573E-08	6,09E-08	FAIL
		3,19968E-09	2,89226E-09	2,89E-09	OK
			3,07423E-10	3,07E-10	FAIL
0,0001	9,99E-05	9,03017E-05		9,03E-05	OK
		9,21446E-06	9,03017E-06	9,03E-06	OK
			1,84289E-07	1,84E-07	FAIL

Figure 16. A part of the recovery event tree Excel implementation. The first line presents the sequence that both diagnosis and actions succeed; the second that diagnosis is successful, and one of the actions fails but its recovery is successful; and so on.

5.2.2.3 Deployment of make-up system 1 before uncovered fuel

This is a start-up of a cooling system. Since no differences with the deployment of the second redundancy have been identified (task analysis does not exist), we may assume that the ASEP model developed for that task (section 5.2.2.2) can be utilized. Therefore, the results of that section apply.

5.2.2.4 Deployment of make-up system 2 before uncovered fuel (including FLEX)

This scenario is identical to deployment of make-up system 1, except that the FLEX diesel generator must be started before starting the pumps. Thus the ASEP model developed for the deployment of the 2nd redundancy of the spent fuel pool cooling system (section 5.2.2.2) may be used in this case also, with one modification.

The modification is that we must take into account the deployment of the FLEX diesel generator. Thus, we have six human actions in the model instead of five.

The HEP of the deployment of the FLEX equipment may be estimated using ASEP as follows. First, concerning diagnosis, it might be the case that make-up system 2 is deployed only after attempts to deploy the main SFP cooling systems and make-up system 1 have failed. This raises the question whether the time available for diagnosis is substantially shorter than what could be inferred from just subtracting time needed for actions from the nominal available time. This would require a separate analysis. However, since the nominal available time is quite long, it is reasonable to assume that the time spent in previous deployment attempts of other safety systems does not significantly affect diagnosis HEP in the present task. Indeed, if there had been previous attempts to deploy the second redundancy and make-up system 1, this would imply that a correct diagnosis has already been made, and therefore it could be argued that there would be no need to incorporate diagnosis error in the model of the present task at all. Therefore it is reasonable and arguably even conservative that we use the diagnosis HEP value of section

Deployment of the second redundancy of the main SFP cooling system, 0.0001. Since no task analysis for FLEX actions is available, we again use Table 8-5 of the ASEP manual. Since the time available for the actions is abundant even with six actions, it is concluded that the lower of the applicable risk levels, moderately high stress, can be assumed. Furthermore, the action is probably well-trained and thus a step-by-step task and not a dynamic task. Therefore, the HEP of each action is 0.02.

Since there is ample time for recovery, we can utilize the recovery event tree model described in section 5.2.2.2.1, with some modifications:

- the number of actions is 6, so the binomial distribution utilized becomes Bin(n, HEP_{action}, 6) for n= 0, 1, …, 6.
- we must add four sequences to the tree: two for the case that diagnosis succeeds (all 6 actions fail but are recovered, and all 6 actions fail and at least one of them is not recovered), and the same two for the case that diagnosis fails but its recovery succeeds.

The HEP of this task is 0.0024. This is somewhat larger than the HEP of the deployment of the second redundancy task (section 5.2.2.2).

5.2.2.5 Repair of main SFP cooling system before boiling

The repair items considered for the first redundancy are pump stopping and failure of heat exchanger. For the other redundancies, also failure to start a pump is considered.

The generic procedure of conducting repair, described at the end of section 5.1.7, is used as the basis of ASEP analysis. The analysis itself proceeds as the one presented in section 5.2.2.2.

We assume that a single field man conducts the repair work. Further, we assume that repair of a failed pump is a step-by-step task for field men, and it has been well covered in their training.

The time available for repair is the same as with the Swedish pilot (section 5.2.1), that is 24 hours when there is no cooling circulation and the objective is to prevent cooling water boiling, and 2 weeks when there is cooling circulation.

We consider first the pump repair. The main repair actions of pump repair are assumed to be the following:

- fetching the appropriate instruments, equipment, spare parts and protective gear
- uninstalling a part of the pump
- install spare part to replace the broken part
- reassemble the pump
- restart the pump

Error in any of these steps is assumed to lead to a failure of the task. However, the possibility of recovery is credited in the way described in section 5.2.2.2.1.

We assume the following durations for the steps 6–8 of the repair procedure listed at the end of section 5.1.7: 120+15+5 = 140 minutes. The communication and travel times (steps 1-3) are assumed to be 5+5+5 = 15 minutes. Thus, the time left for diagnosis is 1440-(140+15) = 1285 minutes. We assume that non-recovered misdiagnosis will lead to boiling, symptom-oriented repair instructions are available to the field man, are well-designed, cover also the present failure, and the field man has been trained to use them. However, it is not known whether the

field man will actually use the repair instructions instead of relying on memory. From ASEP Figure 8-1, the diagnosis HEP is 2.5E-4.

As stated above, all of the tasks are assumed to be critical, but they are step-by-step tasks. Stress level is assumed to be only moderately high because there is ample time to do the repair. Therefore, the HEP of each action is 0.02.

For recovery, we assume that the stress level is extremely high - when the error is detected, there might be shortage of time. Therefore, recovery verification HEP is 0.001, and the HEP of each recovery action is 0.05.

Utilizing the recovery model, the HEP of the pump repair task is 0.005.

The calculation of the HEP of the heat exchanger recovery task goes similarly. The only change is that in the repair actions list, the object of repair is the heat exchanger. Thus, the HEP of the pump repair task applies also here.

As no information about the complexity or other factors of failure of a pump to start is available, it is assumed that it corresponds to the repair of a pump that has stopped working, and therefore the HEP of the pump repair task is also valid in this task.

5.2.2.6 Repair of make-up system 1 before uncovered fuel

This case, with only pump failure and repair considered, is identical to the pump repair task considered in section 5.2.2.5, except that the available time is 69 hours (see section 5.2.1.7). This long available time changes the diagnosis error probability to 0.0001 (much longer time available for diagnosis), and the HEPs of the recovery actions to 0.02 (only moderately high stress due to ample available time). Using these values, the HEP of the task is calculated to be 0.002.

5.2.2.7 Repair of make-up system 2 before uncovered fuel

The repair items considered are FLEX diesel generator failure and pump failure. The pump failure case has been considered in section 5.2.2.6. Therefore, here we consider only the FLEX diesel generator failure.

As in section 5.2.2.6, the available time is 69 hours.

We assume that the repair of the FLEX diesel generator consists of the following parts:

- fetching the appropriate instruments, equipment, spare parts and protective gear
- uninstalling a part of the generator
- install spare part to replace the broken part
- reassemble the generator
- restart the generator

However, we also assume, as was assumed in section 5.2.1.10, that written repair procedures have not been constructed and that the repair procedure has been covered in training but not much practiced. This changes the nature of the repair task somewhat.

First of all, the HEP of diagnosis is taken from the upper bound of the time-reliability curve in Figure 8-1 (Swain, 1987), even though there is ample time available. That means that the diagnosis HEP of diagnosis is 0.0001.

Second, we must assess the HEPs of actions. All the actions are assumed to be critical. They are also dynamic in the sense of (Swain, 1987), due to lack of written repair procedures and shortcomings of training (item 10 c in Table 8-1 of Swain, 1987). On the other hand, there is ample time available, and therefore moderately high stress level can be assumed. Thus, from item (4) of Table 8-5 (Swain, 1987), the HEP of each action is 0.05.

Third, we must adjust the recovery probabilities of errors in actions. The recovery verification (corresponds to diagnosis, because it means that the result of actual action is verified which may lead to the discovery of the error) HEP is 0.5 (item (7), Table 8-5 of Swain, 1987). For the same reasons as for the post-diagnosis actions, also the HEPs of recovery actions are 0.05.

Once these HEPs are used in the recovery model, the HEP of the task is 0.012.

5.2.3 HRA Benchmark and comparisons

5.2.3.1 HRA results from Swedish study and VTT study

Two HFE results from the studies are listed in Table 12.

Table 12. Example HFE results comparison

HFE Description	**Basis HRA methods**	**TW (h)**	**T_{delay} (h)**	**T_{exe} (h)**	**HEP Diagnosis**	**Diagnosis Recovery considered**	**HEP Execution**	**Execution Recovery considered**	**Total**
Start (standby) SFP cooling before boiling	F/R method for both diagnosis and execution	24	8	1	4.50E-04	No	1.00E-03	Yes, 0.1	1.45E-03
Deployment of the second redundance of the main cooling system	ASEP	144			1E-7	yes	1.0E-2	yes	2.0E-3
FLEX, start make-up system 2 before uncovered fuel	F/R method for both diagnosis and execution	72	1	2	3.40E-04	No	5.00E-03	Yes, 0.1	5.34E-03
Deployment of make-up system 2 (with startup of FLEX diesel generator)	ASEP	72	1	2	5E-5	yes	2.3E-1	yes	1.2E-2

One topic of interest, pointed out in section 5.1.7, is whether the HEPs of different activities provided by ASEP are applicable to repairs and FLEX actions. The HRA results between the results of Finnish and Swedish models concerning the task involving FLEX activities are not radically different from each other, which gives some support to the notion that ASEP HEPs could be sufficiently accurate for practical purposes also concerning tasks involving repair and FLEX actions. Furthermore, the HEP estimate given by ASEP is clearly larger than that provided by F/R method, and thus is acceptable as a conservative estimate. However, more research would be needed to corroborate these preliminary findings.

5.2.3.2 Comparison of diagnosis HEPs from F/R method and SPAR-H

In Swedish studies, F/R method is used as the main method for diagnosis HEP estimation, see section 5.1.1.

SPAR-H method is used to quantify the diagnosis HEP of a selected HFE, with the result from the F/R method. In the SPAR-H method, 8 PSFs are to be evaluated to get multipliers to multiply with the nominal diagnosis HEP which is 1E-2.

The available time is one of the eight PSFs and the typical multipliers are 0.01, 0.1, 1, 10 or HEP =1, as showed in Figure 17.

Available Time	Inadequate time	P(failure) = 1.0	☐
	Barely adequate time (≈ 2/3 x nominal)	10	☐
	Nominal time	1	☒
	Extra time (between 1and 2 x nominal and > 30 min)	0.1	☐
	Expansive time > 2 x nominal & > 30 min	0.1 to 0.01	☐
	Insufficient Information	1	☐

Figure 17. Multiplier of PSF Available Time in SPAR-H for low-power shutdown condition

In SPAR-H, the time PSF is 0.01 at lowest and if we consider all other PSFs are nominal, the diagnosis HEP would be 1E-4. This is similar to Ringhals/Formark method whose basis HEP is based on the available time and TRC. When the available time is 4.5h, the basis diagnosis HEP from F/R method is 1E-3. The lowest basis HEP from F/R method is 1E-4.

Note the available time PSF in SPAR-H method considers both the available time and the nominal (required) time.

Besides the available time PSF, both methods consider other PSFs as multipliers. Table 13 lists the PSFs considered in each method and their possible largest multiplier in the worst situation and the lowest multiplier in the best optimal situation. Note in SPAR-H method, the maximum products from the 8 multipliers will be adjusted if there are more than 3 PSFs have negative multipliers. The main reason is to ensure the final diagnosis HEP is less than 1. Thus in SPAR-H the maximum products of 7 PSFs will not reach 6250000 as listed in Table 13.

Table 13. PSFs in F/R and SPAR-H

PSFs in F/R method for diagnosis	Ki worst	Ki best	PSFs in SPAR-H	PSF worst	PSF best
Procedure	5	0.5	Procedure	50	0.5
Training	5	0.2	Training	10	0.5
MMI	5	0.2	HMI	50	0.5
Mental load	5	1	Stress	5	1

PSFs in F/R method for diagnosis	Ki worst	Ki best	PSFs in SPAR-H	PSF worst	PSF best
Communication/coordination	5	0.5	Complexity	5	0.1
			Fitness for duty	5	1
			Work process	2	0.8
The product of the multipliers	3125	0.01		6250000	0.01

To illustrate the differences of these two methods, Figure 18 shows the possible diagnosis HEPs from these two methods. It is based on the assumption that the nominal (required) diagnosis time is 2 hours as this is needed in SPAR-H quantification.

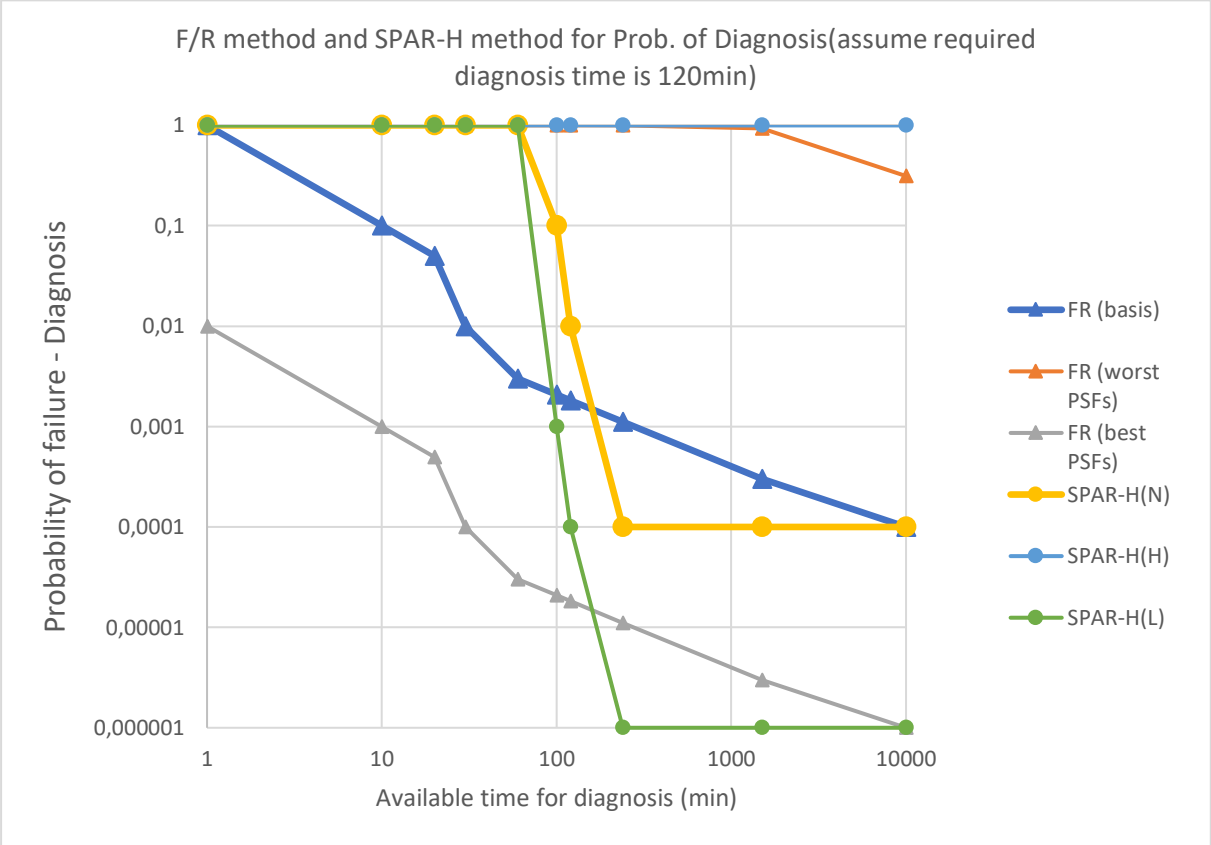

Figure 18. Diagnosis HEPs from F/R method and SPAR-H method (nominal diagnosis time is 120 minutes)

As we can see from the Figure 18, the diagnosis HEP from SPAR-H method will be 1 when the available is shorter than 2/3 of the required diagnosis time. This is not reflected in the basis curve of F/R method. It is however still possible to get diagnosis HEP as 1 from F/R method, through the multipliers from the 5 PSFs. This requires that F/R method analysts select negative multipliers from the corresponding PSFs (need to reflect the fact that the operator has not enough time for diagnosis) to adjust the basis HEP. This is a main difference between these two methods.

If we assume the nominal diagnosis time is 15 minutes, the nominal SPAR-H curve will be different from the above figure and thus its curve for the worst situation (H) and curve for the best optimal situation (L) are also adjusted. Figure 19 shows the new comparisons of the diagnosis HEPs. In such situation, the F/R method basis curve and SPAR-H method nominal curve match quite well in the short-time window.

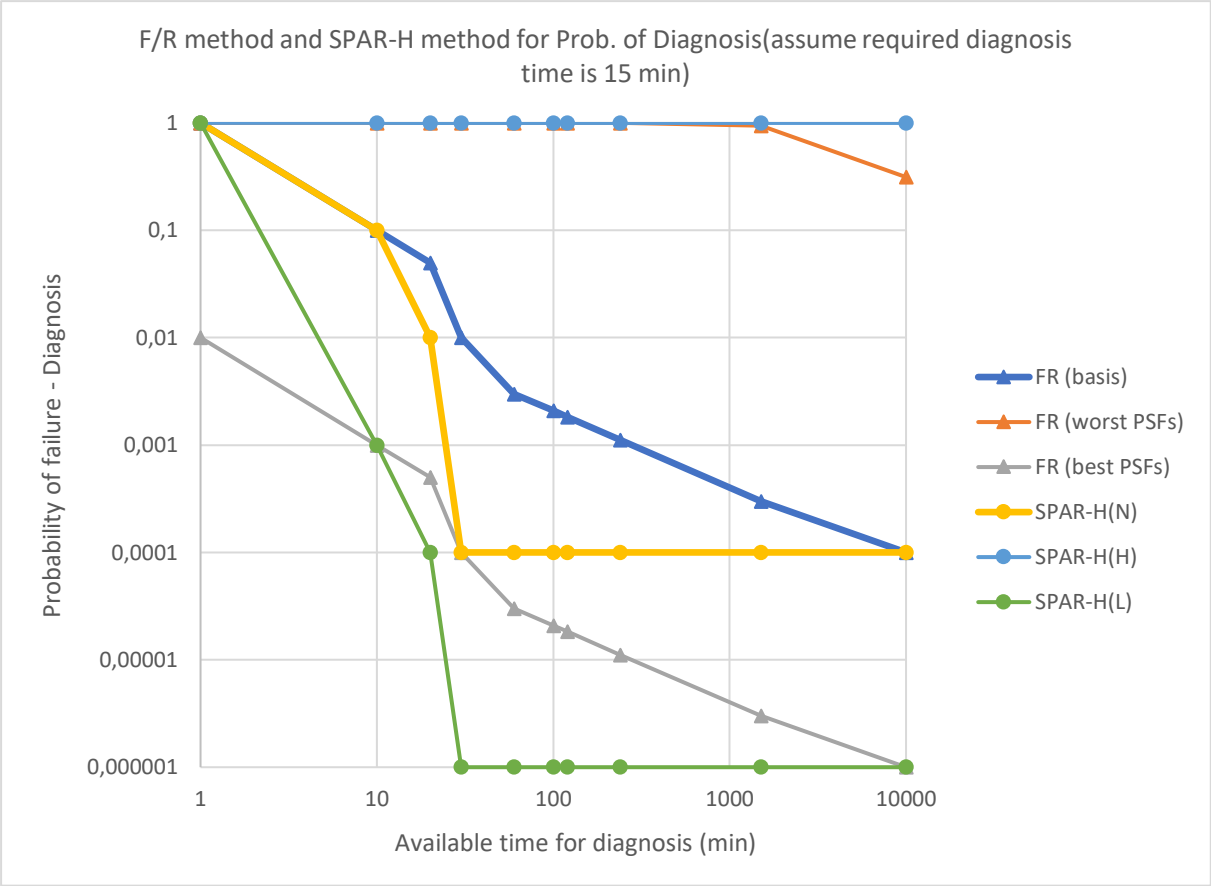

Figure 19. Diagnosis HEPs from F/R method and SPAR-H method (nominal diagnosis time is 15 minutes)

For HFE to repair make-up 1 before uncovered fuel, SPAR-H is used for diagnosis HEP estimation. This is to compare the diagnosis quantification from F/R method, as described in section 5.2.1.7.

PSF: Available Time
The available time for repair diagnosis is 69-24 = 45 hours
The nominal required time for repair diagnosis is 2 hours

Thus it is judged as Expansive Time with multiplier 0.01 — the time margin exceeds the time required; the time available is much greater than the time required.

PSF: Stress/Stressors
Stress is high with multiplier 2. It is higher than the nominal level (e.g., instruments with anomalous readings or unexpected alarms; loud, continuous noise impacts ability to focus attention on the task; the consequences of the task represent a threat to plant safety).

PSF: Complexity
Complexity is Nominal with multiplier 1
Diagnosis is not difficult as it is obvious that the system is failed and need to be repaired. However there might be ambiguity in such situation and it is a matter of priority for the situation when there are other tasks that should be performed. If we assume complexity is moderately complex, the multiplier should be 2. If it is highly complex, the multiplier is 5.

PSF: Experience/Training
Experience/Training is Low with multiplier 10.
Some training has been given but is not fully applicable for the situation. Low Experience/Training means it does not provide adequate practice in those tasks, or does not expose individuals to various abnormal conditions.

PSF: Procedures
Procedures are Available but Poor. A procedure is available but is difficult to use because of factors such as formatting problems, ambiguity, or such a lack in consistency that it impedes performance. The repair is not specifically mentioned or instructed. The multiplier is 5.
Note: If we assume Procedure is Incomplete (lacking), the multiplier is 20. The multiplier of this PSF should be further checked with the plant real situation.

PSF: Ergonomics/HMI
Nominal with multiplier 1.
Operators are provided useful labels; the computer interface is adequate and learnable.

PSF: Fitness for Duty
Nominal with multiplier 1
The individual operator is able to carry out tasks; no known performance degradation is observed.

PSF: Work Processes
Nominal with multiplier 1
Performance is not significantly affected by work processes at the plant, or work processes do not appear to play an important role (e.g., crew performance is adequate; information is available, but not necessarily proactively communicated).
Work Processes refer to aspects of doing work, including inter-organizational, safety culture, work planning, communication, and management support and policies.

The final diagnosis HEP from SPAR-H is approximately as:1E-2* 0.01*2*10*5=1E-2.
As in section 5.2.1.7, the final diagnosis HEP from F/R method is 2.2E-4*8 =1.76E-3.

Discussions: In the above example HFE, without considering of recovery in both approaches, the F/R method provides lower HEP than SPAR-H. This is mainly because the PSF (e.g. Experience/training and procedure) multipliers in SPAR-H are typically higher than those in F/R method when they are judged to negatively impact the diagnosis.

5.2.3.3 Comparison of repair execution HEP from SPAR-H and MTTR exponential distribution

As described in section 5.1.4, exponential distribution model is used as the main method for repair execution HEP quantification. For comparison purpose, SPAR-H method is used to compared with the result as described in section 5.2.1.7 for HFE to repair make-up 1 before uncovered fuel.

In SPAR-H, the nominal execution HEP is 0.001. The following 8 PSFs are evaluated for the selected HFE.

PSF: Available Time
The available time for repair execution is 67 hours. The nominal required time for repair diagnosis is assumed 24 hours.
Thus it is judged as Nominal Time for execution with multiplier 1. Note for SPAR-H execution, Extra time (multiplier 0.1) means time available ≥ 5x the time required.

PSF: Stress/Stressors
Stress is high with multiplier 2. It is higher than the nominal level (e.g., instruments with anomalous readings or unexpected alarms; loud, continuous noise impacts ability to focus attention on the task; the consequences of the task represent a threat to plant safety).

PSF: Complexity
Complexity is Moderately complex with multiplier 2.
There is some ambiguity in what needs to be executed. Several variables are involved, perhaps with some concurrent actions. It is a matter of priority sometimes if there are other tasks/repairs that should be performed.

PSF: Experience/Training
Experience/Training is Nominal multiplier 1.
Repair execution is performed by maintenance team with necessary knowledge on the failed system and component.

PSF: Procedures
Procedure is as Nominal with multiplier 1.
Necessary system manuals are assumed available for repair purpose.

PSF: Ergonomics/HMI
Nominal with multiplier 1.
It is assumed that ergonomics is ok, not a performance driver.

PSF: Fitness for Duty
Nominal with multiplier 1
The individual operator is able to carry out tasks; no known performance degradation is observed.

PSF: Work Processes
Nominal with multiplier 1.
Performance is not significantly affected by work processes at the plant, or work processes do not appear to play an important role (e.g., crew performance is adequate; information is available, but not necessarily proactively communicated). Work Processes refer to aspects of doing work, including inter-organizational, safety culture, work planning, communication, and management support and policies.

The final execution HEP from SPAR-H is approximately as:1E-3*1*2*2=4E-3.
Note: The execution HEP from the exponential model is Exp(-Ta/MTTR)= 6.13E-2.

Discussions:
In comparison, SPAR-H provides lower execution HEP. Its nominal execution HEP is quite low which is 0.001. The time PSF is 1, even though there is good time margin as it is not easy to get lower multiplier in time PSF. On the other hand, the other PSFs are not very high as they

are not significantly negative in the repair execution. If we consider that all other PSFs are nominal, the execution HEP is 1E-3.

The exponential approach is very sensitive to the ratio of the available time and MTTR, which makes it a natural engineering choice to consider the time factor. The obvious drawback is that it does not consider other PSFs at all. Also it is noted from the curve that the repair execution HEP can be extremely small when Ta is much longer.

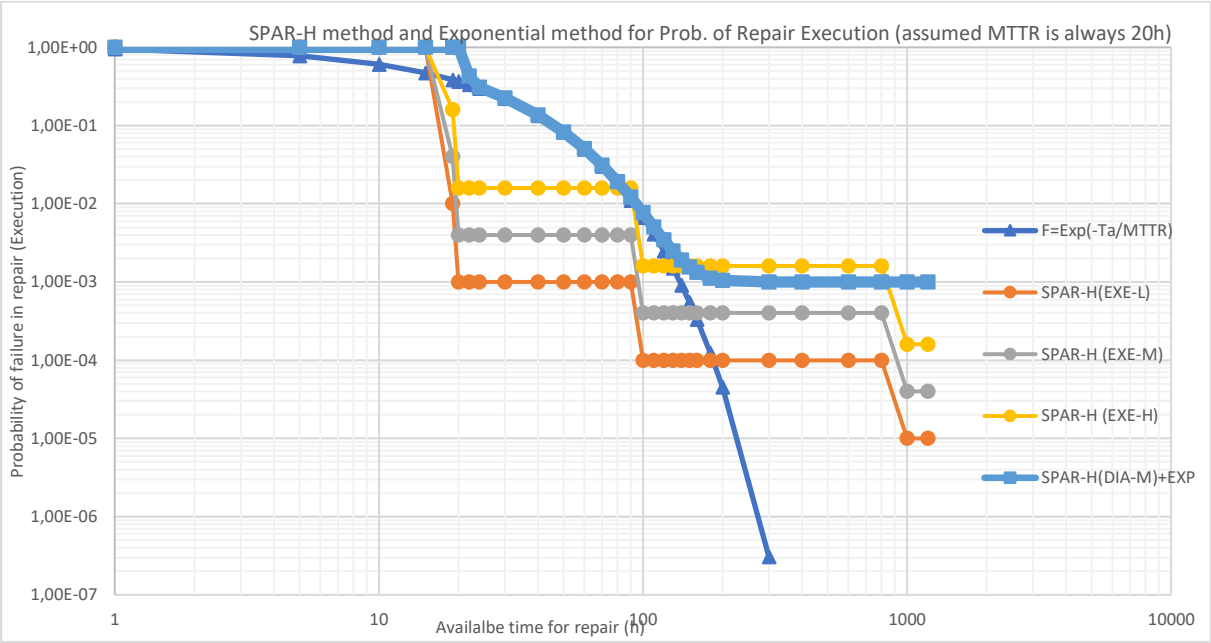

Figure 20. Repair execution HEPs from SPAR-H method and Exponential distribution

Figure 20 shows three SPAR-H execution HEP curves as it can consider other PSFs in the execution HEP (e.g. EXE-H curve represents a case where a few other PSFs are negative and thus HEPs are higher). Also the execution HEP from SPAR-H has the lowest limits (unlike the exponential approach, the execution HEP can be extremely small when Ta is much longer).

In order to use the exponential model for repair execution HEP, the following suggestions are provided:

- For each required action, diagnosis HEP must be quantified. The repair execution HEP must be added with the diagnosis HEP. Example curve 'SPAR-H (DIA-M)+EXP' in Figure 20 represents the total HEP and it will have limit values.

The exponential approach is rather very sensitive to the ratio of the available time and MTTR. The MTTR for a particular component (failure mode) could be available from some database e.g. T-book. The MTTR should be evaluated to ensure it represents the total required execution time in different situation to include all the time needed for repair execution including spare parts transportation, etc. Since the MTTR might be different for different failure modes of a component, it could be a good idea to use a or a few boundary MTTRs so that the time is not underestimated (the operator might have difficulties to know the exact failure mode when a component is failed). On the other hand, it is not suggested to use MTTR which are overestimated.

6. PSA

In this chapter, three PSA methods, I&AB, Enhanced fault/event tree and simulation-based event tree, are presented. Pilot study models and results are also presented for each method. Finally, the methods and results are compared.

6.1. I&AB

6.1.1 Method

The I&AB (Initiator and All Barriers) method is developed by EdF and are described in more detail in (Bouissou & Hernu, 2017) and (Bouissou, 2018).

In a traditional static PSA approach the exact timings of failures leading to the analysed consequence is not taken into account. A fully dynamic approach would model these time dependencies in a realistic representation. However, the complexity and size of a standard nuclear PSA would lead to unacceptable calculation times with a fully dynamic approach. The I&AB method is an intermediate model that combines some properties of a dynamic model with the static PSA approximation. It captures some dynamic features as:

- A component could fail and be repaired several times during a long time window
- A component may run for some time before it fails.
- The “mission time” for the barrier of safety functions is the time to restore the initiating event

The method is based upon two approximations:

1. When an initiating event occurs, all standby components are supposed to start functioning (or maybe fail to start) immediately after the initiating event; then, they may fail and be repaired independently from each other until the initiating event is repaired.
2. Once an initiating event is repaired, the system cannot fail anymore, whatever happens.

To understand the key features of the I&AB, a comparison is made with the fully dynamic representation on one hand, and with the static representation on the other. Figure 21, Figure 22 and Figure 23 compare the graphical representation of a fully dynamic Markov chain, a static PSA and the I&AB method for a system with three components. In the normal state of the system component 1 is running (represented by a bold figure) and component 2 is the primary redundant standby component and component 3 is the secondary redundant standby component. A failed component is indicated with a grey figure. The component failure rate is denoted with λ and the component repair rate is denoted with μ. The failure rates and repair rates describe the changes between the states of the system.

The Markov chain in Figure 21 takes into account repairs of all components and the fact that the system can return to the normal state repeatedly during the analysed time.

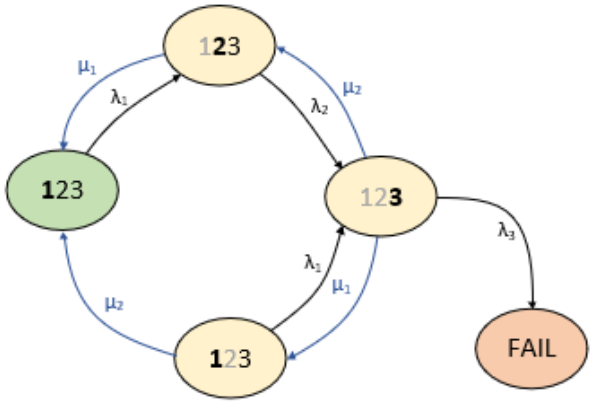

Figure 21. State graph for the fully dynamic representation of a three component system.

In the traditional static PSA approach in Figure 22 no repairs are considered. Once an initiating event occurs, the failures of all other components in the sequence are assumed to occur instantly and independently. Another limitation of this approach is that the failed state can only be reached within the fixed mission time used in the analysis, which usually is 24 hours.

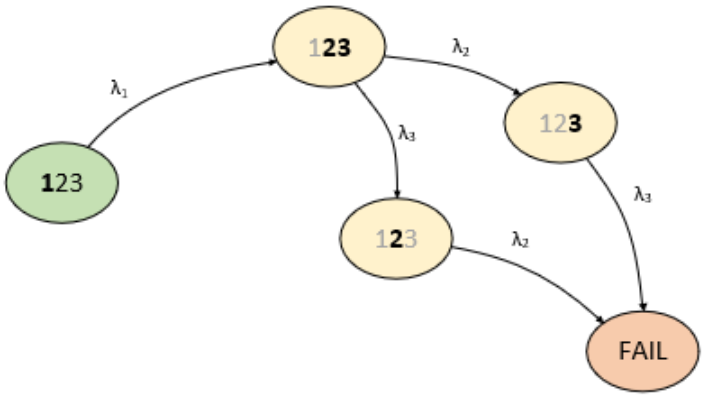

Figure 22. State graph for the PSA approximation

The state graph in Figure 23 illustrates the intermediate model of I&AB that combines some properties of both the previous models. It also contains an additional state, which is called an absorbing state. This state is not necessarily always the same as the normal state, but it is a state in which the initiating event has been repaired. The absorbing state can be interpreted as the safe state or success to recover from the initiating event. In this approach the analysis is performed until either the absorbing state or the failed state is reached.

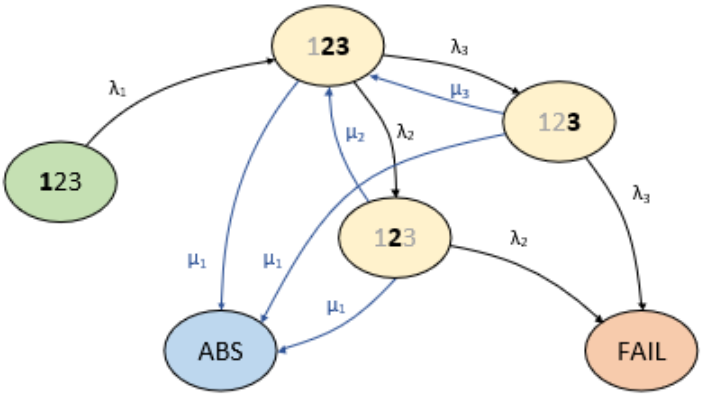

Figure 23. State graph for the intermediate model using the I&AB method.

In addition to simulate the dynamics of failure and repair processes, the extension of the I&AB method does also take into account deterministic delays that allows extra time before the undesired consequence occurs. Two different types of deterministic delays are defined:

- **Grace time -** the undesired consequence is delayed by some physical process. The spent fuel pool is a good example of such a time window. If the cooling of the spent fuel pool is lost, boiling or fuel damage does not occur instantly. Instead the water will heat until it reaches boiling after a certain time. The water will then start to evaporate and after some additional time fuel uncovery and fuel damage occurs. These extra available time windows are represented as grace time.
- **Deterministic failure -** the capacity of a function is limited in time and not repairable. An example of this is if the cooling is lost for the spent fuel pool, it may be possible to add water from water tanks. However, the amount of water in the tanks is limited and after a certain time the water tanks will be empty which can be seen as a deterministic failure. It is also not possible to fill up the water tanks in a short amount of time, i.e. it is a non-repairable failure. Also, batteries would be an example of a function that is well described by a deterministic failure as they last for a limited amount of time before they fail.

6.1.2 Application

I&AB is implemented as an add-on tool in the RiskSpectrum PSA software tool. The calculation method contains five types of events with input parameters within brackets:

- Initiating events (failure frequency λ_{ie} and repair rate μ_{ie})
- Failure in Function events (failure rate λ and repair rate μ)
- Failure on Demand events (failure probability q and repair rate μ)
- Grace time event (grace time parameter t_{gt})
- Deterministic failure event (deterministic failure time parameter t_{df})

The MCS list is extracted in the same way as for the static PSA calculations. The MCSs are then calculated individually with an approximation of the unreliability of all barriers in the MCS, i.e. the probability that a moment where all barriers are failed comes before the initiating event is repaired. Additionally, a MCS might specify a grace delay between the failure of all barriers and the system failure and a deterministic failure occurring exactly after a given time.

The repair rate μ is a new parameter introduced with the I&AB method. This represents the rate with which a failure is repaired in an accident sequence. The user can define a "Sequence Mean Time To Repair" (Sequence MTTR) for each basic event. The repair rate is then calculated by μ=1/(Sequence MTTR). If the sequence MTTR is set to zero it is handled as repair rate zero in the calculations. Also, the grace time parameter t_{gt} and the deterministic failure time parameter t_{df} are new parameters. All three additional input parameters are defined in the I&AB Editor, see Figure 24.

For CCF event repair rates there are two different strategies that can be chosen. The first is concurrent repair strategy which means that all components in the CCF group can be repaired (remedy their CCF) in the same time as repairing a single component. The second alternative is consecutive repair strategy where the total repair time for the CCF is the sum of the repair times for all events in the group.

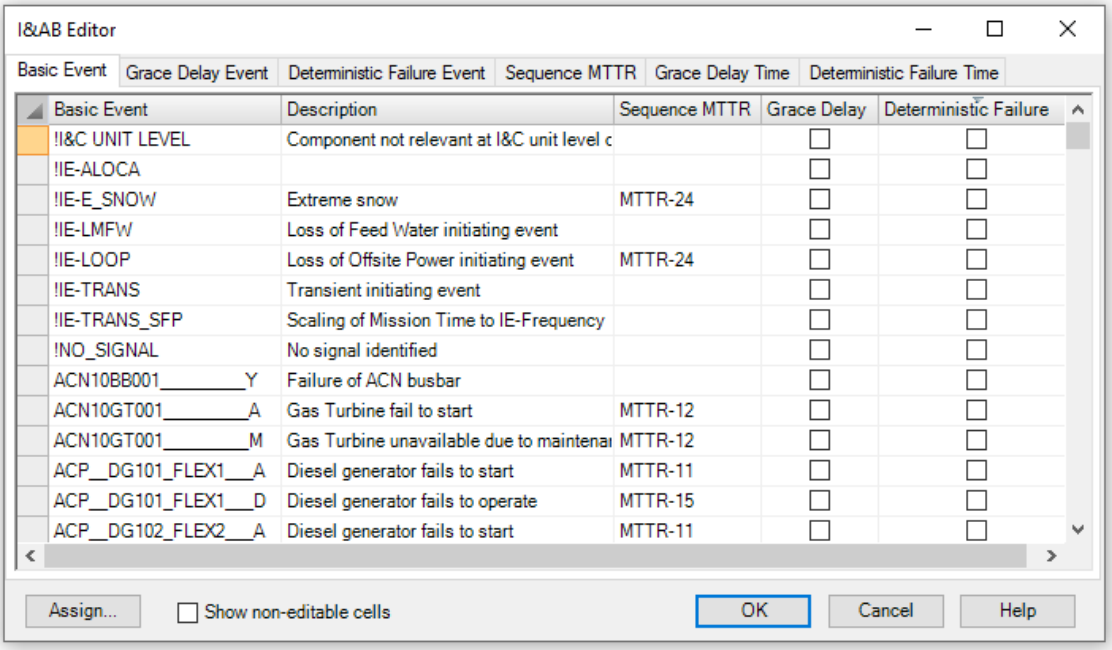

Figure 24. I&AB editor in RiskSpectrum PSA.

6.1.3 Pilot studies

Pilot studies are performed where I&AB are applied to two different models. The following pilot studies are presented in the following sections:

- PROSAFE SFP model, section 6.1.3.1
  - Transient
  - Loss of Offsite Power (LOOP)
  - Extreme Snow
- PROSAFE Reactor model, section 6.1.3.2
  - Extreme Snow
- Full scale PSA SFP model, section 6.1.3.3
  - Loss of Offsite Power (LOOP)

6.1.3.1 Pilot study - PROSAFE SFP model

The scope of the pilot study is to analyse the consequences feed and boil (FAB) and fuel damage (FD) for the spent fuel pool for the following initiating events:

- Transient
- Loss of Offsite Power (LOOP)
- Extreme Snow

The description of the pilot study is divided into the following chapters:

- Implementation, section 6.1.3.1.1
- Results and Interpretation, section 6.1.3.1.2
- Sensitivity Analysis, section 0
- Conclusions, section 6.1.3.1.4

6.1.3.1.1 Implementation in the PROSAFE model

The I&AB method is implemented in RiskSpectrum with an addon that was used to perform the pilot study on the PROSAFE model. RiskSpectrum version 1.4 together with RSAT version 3.4.5.18 was used.

All the additional parameters required for the I&AB calculation are defined and assigned to basic events in the I&AB Editor, see Figure 25.

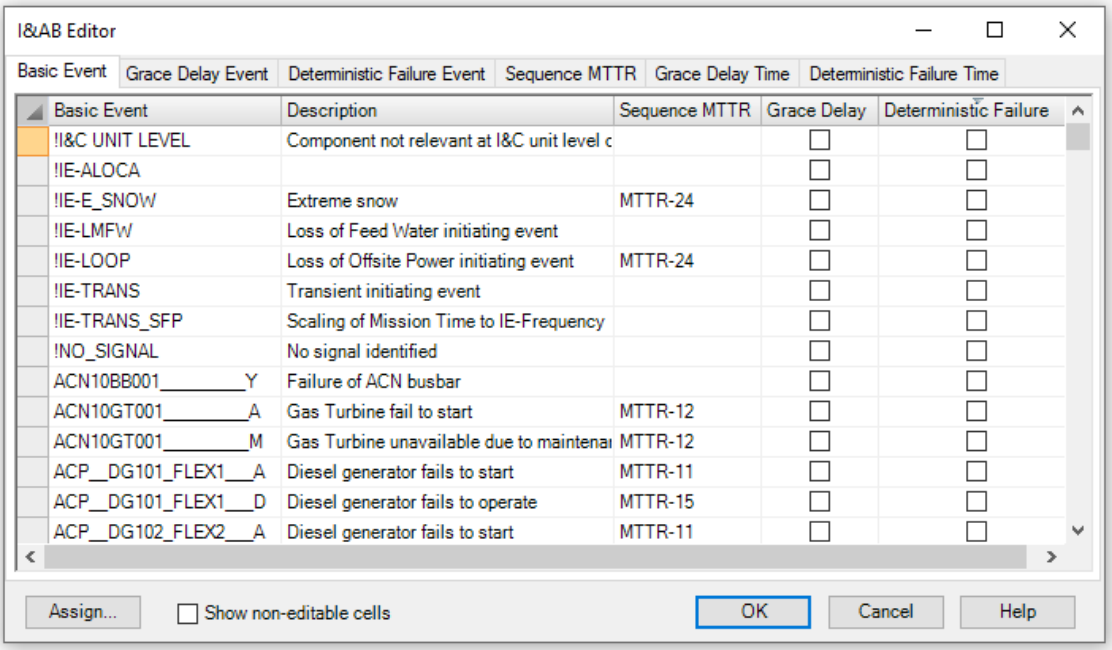

Figure 25. The I&AB editor in RiskSpectrum PSA.

The following sections will describe

- Modelling of repair
- Modelling of repair of the initiating event
- Modelling time windows

Modelling of repair

In this chapter it is described how the MTTR for the repairable components in the pilot study were assigned.

Components that were modelled as repairable components were identified based on the importance analysis. Among the events with FC > 0.5% or risk increase factor (RIF) >2 the events that can be considered to be repairable within a reasonable time frame were selected. For these events, a MTTR will be assigned as an additional input parameter. This parameter is called the Sequence MTTR in RiskSpectrum, not to be confused with the MTTR parameter used for the basic event type Repairable Component, which is used to calculate the unavailability for a basic event. The Sequence MTTR represents the rate with which a failure is repaired in an accident sequence. The Sequence MTTR parameters are defined in the I&AB Editor, see Figure 26.

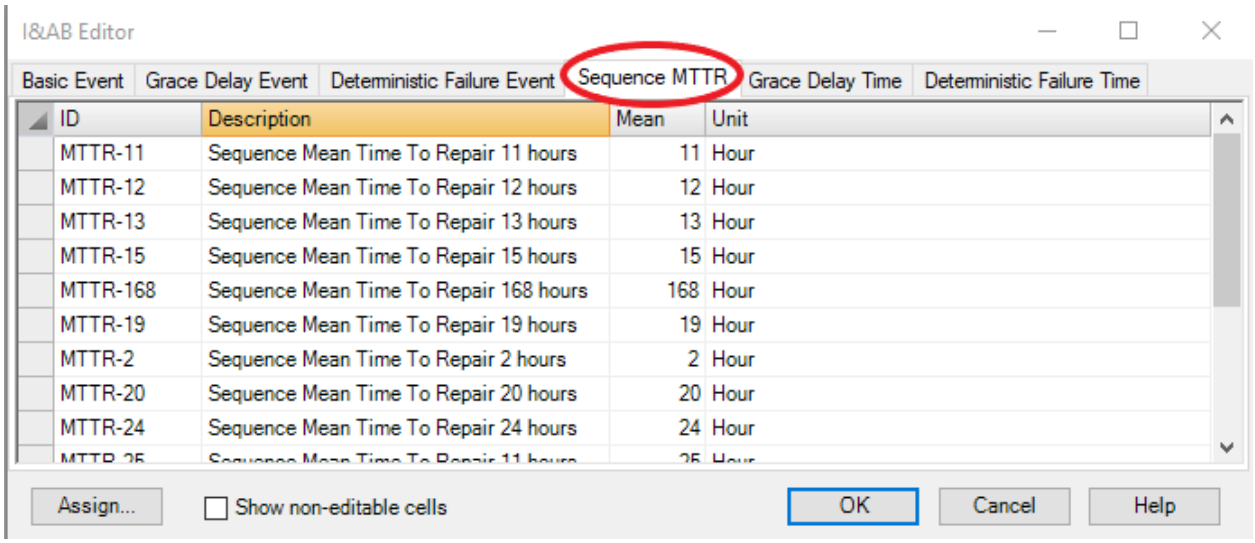

Figure 26. Defining Sequence MTTR parameters in the I&AB editor.

Table 14 summarizes which basic events have been assigned with a sequence MTTR parameter in the pilot study. The total MTTR is the sum of the MTTR for the diagnosis part and the MTTR for the execution part. The execution part for the MTTR is obtained from the appropriate component table in the T-book 8. The diagnosis part is obtained based on the HEP calculated in chapter 5.2.1. Note that this HEP is calculated based on the failure mode with the most conservative MTTR from the T-book. The total repair time is assumed to be exponentially distributed. The total MTTR is estimated so that the probability to exceed the available time is the total HEP. The total HEP can then be transformed into a corresponding total MTTR with the exponential distribution relation. The diagnosis MTTR for a component is then obtained by subtracting the most conservative MTTR from the T-book for that component from the total MTTR. The same diagnosis MTTR is used for all failure modes for a component type.

Repair of the gas turbine has not been studied within the scope of the HRA. Repair of the gas turbine has been modelled with the assumption that there is a dependency to the failure to repair the diesel. The total MTTR to repair the gas turbine is calculated based on a middle dependence (definition according to SPAR-H) to the total MTTR for repair of the diesel. A few busbars were identified in the importance analysis. These have in this pilot study been assumed to not be repairable, even though this is a conservative assumption.

Table 14. The basic events in the Prosafe model that are assigned a sequence MTTR parameter. The last column, Total MTTR, is the parameter value.

Basic event	Description	Basic Event Type	MTTR Diagnosis [h]	MTTR Execution [h]	Total MTTR [h]
SFPC_P1_____D	Spent Fuel Pool Cooling Pump 1 - Fails to Run	Mission Time	8	24	32
SFPC_P2_____D	Spent Fuel Pool Cooling Pump 2 - Fails to Run	Mission Time	8	24	32
SFPC_P3_____D	Spent Fuel Pool Cooling Pump 3 - Fails to Run	Mission Time	8	24	32
SFPC_P4_____D	Spent Fuel Pool Cooling Pump 4 - Fails to Run	Mission Time	8	24	32
SFPMU:1_P1_____D[1)]	Spent Fuel Pool Make Up:1 Pump 1 - Fails to Run	Mission Time	8	24	32
SFPMU:1_P2_____D[1)]	Spent Fuel Pool Make Up:1 Pump 2 - Fails to Run	Mission Time	8	24	32
SFPMU:2_P1_____D	Spent Fuel Pool Make Up:2 Pump 1 - Fails to Run	Mission Time	8	24	32

Basic event	Description	Basic Event Type	MTTR Diagnosis [h]	MTTR Execution [h]	Total MTTR [h]
SFPC_P2_____A	Spent Fuel Pool Cooling Pump 2 - Fails to Start	Tested	8	12	20
SFPC_P3_____A	Spent Fuel Pool Cooling Pump 3 - Fails to Start	Tested	8	12	20
SFPC_P4_____A	Spent Fuel Pool Cooling Pump 4 - Fails to Start	Tested	8	12	20
SFPMU:1_P1_____A	Spent Fuel Pool Make Up:1 Pump 1 - Fails to Start	Tested	8	12	20
SFPMU:1_P2_____A	Spent Fuel Pool Make Up:1 Pump 2 - Fails to Start	Tested	8	12	20
SFPMU:2_P1_____A	Spent Fuel Pool Make Up:2 Pump 1 - Fails to Start	Tested	8	12	20
SFPC_H1_____X	Spent Fuel Pool Heat Exchanger 1 - Failure/Leakage	Mission Time	8	11	19
SFPC_H2_____X	Spent Fuel Pool Heat Exchanger 2 - Failure/Leakage	Mission Time	8	11	19
SFPC_H3_____X	Spent Fuel Pool Heat Exchanger 3 - Failure/Leakage	Mission Time	8	11	19
SFPC_H4_____X	Spent Fuel Pool Heat Exchanger 4 - Failure/Leakage	Mission Time	8	11	19
ACP__DG101_FLEX1___D	Diesel generator fails to operate	Mission Time	5	10	15
ACP__DG102_FLEX2___D	Diesel generator fails to operate	Mission Time	5	10	15
ACP10DG001_____D	Diesel generator fails to operate	Mission Time	5	10	15
ACP20DG001_____D	Diesel generator fails to operate	Mission Time	5	10	15
ACP30DG001_____D	Diesel generator fails to operate	Mission Time	5	10	15
ACP40DG001_____D	Diesel generator fails to operate	Mission Time	5	10	15
ACN10GT001_____A	Gas Turbine fail to start	Tested	-	4	12[2)]
ACN10GT001_____M	Gas Turbine unavailable due to maintenance	Probability	-	4	12[2)]
ACP__DG101_FLEX1___A	Diesel generator fails to start	Tested	5	6	11
ACP__DG102_FLEX2___A	Diesel generator fails to start	Tested	5	6	11
ACP10DG001_____A	Diesel generator fails to start	Tested	5	6	11
ACP20DG001_____A	Diesel generator fails to start	Tested	5	6	11
ACP30DG001_____A	Diesel generator fails to start	Tested	5	6	11
ACP40DG001_____A	Diesel generator fails to start	Tested	5	6	11
ACN10BB001_____Y	Failure of ACN busbar	Mission Time	-	-	0
ACP10BB001_____Y	Failure of ACP busbar	Mission Time	-	-	0
ACP20BB001_____Y	Failure of ACP busbar	Mission Time	-	-	0
ACP30BB001_____Y	Failure of ACP busbar	Mission Time	-	-	0
ACP40BB001_____Y	Failure of ACP busbar	Mission Time	-	-	0

1) This basic event was not identified from the importance list. However it was modelled with a sequence MTTR parameter since other failure modes of this component had been identified to be of importance.

2) The total sequence MTTR for the gas turbine was calculated based on a HEP value with a middle dependence with regards to the repair HEP for the diesel. The HEP for the gas turbine is then transformed into a sequence MTTR using the exponential distribution formula with the available time 24 hours.

Modelling repair of the initiating event

One key feature of the I&AB method is the requirement to assign a MTTR for the repair or recovery of the initiating event. This MTTR can in some sense be compared to the mission time used for components and systems in the static PSA approach as it is the time that we need our barriers to function in order to be able to bring the system into a safe state. This MTTR is set for each initiating event and can thus be different for each initiating event in the analysis. The

initiating events and the assigned MTTR parameters used in the pilot study are presented in Table 15.

For the basic events representing initiating events for the transient sequences, the total MTTR is calculated in the same manner as for the MTTR of component basic events. For the LOOP and Extreme Snow Events the same time that is used as a mission time in the static PSA model was assumed.

Table 15. The basic events in the PROSAFE model representing initiating events that are assigned a sequence MTTR parameter. The last column, Total MTTR, is the parameter value.

Initiating Event	Basic event	Description	Basic Event Type	MTTR Execution [h]	MTTR Diagnosis [h]	Total MTTR [h]
Transient	SFPC_P1_____I____D	Spent Fuel Pool Cooling Pump 1 - Fails to Run - Initiating Event	Frequency	24	8	32
Transient	SFPC_H1_____I____X	Spent Fuel Pool Heat Exchanger 1 - Failure/Leakage - Initiating Event	Frequency	11	8	19
LOOP	!IE-LOOP	Loss of Offsite Power initiating event	Frequency			24
Extreme snow	!IE-E_SNOW	Loss of Offsite Power initiating event	Frequency			24

Modelling time windows

The time windows that is modelled in the pilot study are:

- 24 hours from the initiating event until boiling of the spent fuel pool
- 72 hours from boiling until fuel damage (not credited in this pilot study)
- 336 hours (2 weeks) of extra time available if operation of any of the make-up (MU) systems can be established.

If the cooling of the spent fuel pool is lost as a consequence of an initiating event the available time to take action to start the cooling before the pool starts to boil is 24 hours. This will be denoted a grace time in I&AB. A new basic event (GRACE-TIME) is created and the type of event is chosen to be “grace delay event”. This basic event takes one parameter as input, the grace delay time, which in this case is assigned the value 24 hours.

When the boiling state is reached after 24 hours, it is assumed that the cooling of the spent fuel pool cannot be restarted due to the water level being too low in the SFP. However, if operation of any of the two MU systems can be established, the water level in the pool is recovered which makes it possible to restart the cooling system again. Running the MU system then in practice means that we buy extra additional time for the repair of the cooling system. This is represented in the I&AB method as a deterministic time. A new basic event (DET-TIME) is created and the type of event “Deterministic Failure Event” is assigned. This type of basic event takes the parameter Deterministic Failure Time” as input. In the pilot study this value is 336 hours.

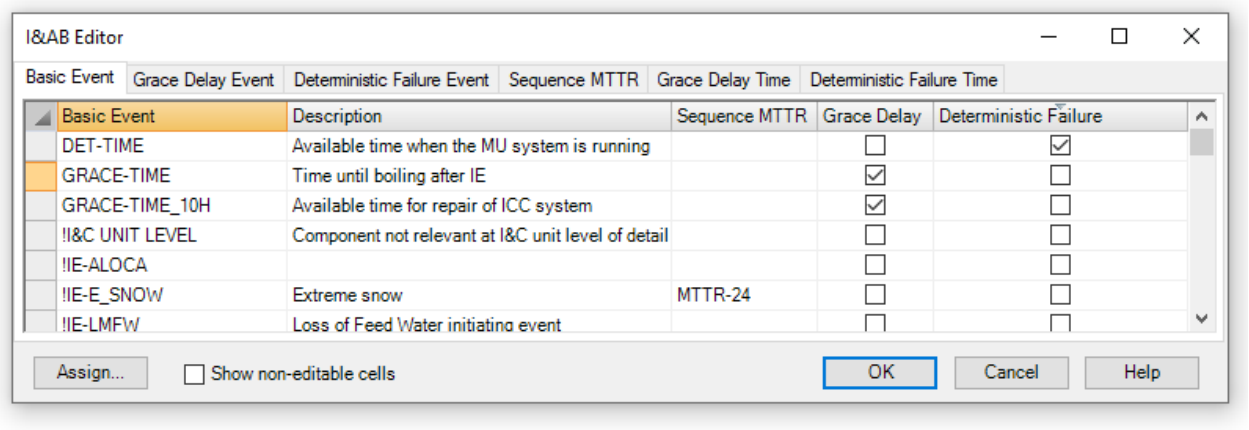

Figure 27. Defining basic events as Grace Delay events or Deterministic Failure events in the I&AB editor.

Now the new basic events used to represent time windows can be defined in the I&AB editor, see Figure 27. In the "basic event" tab it can be selected for each basic event if it is a grace time or deterministic time event. The input parameters are then defined in the other tabs in the I&AB editor.

Next, the second step is to define in which sequences in the model these time windows can be credited.

The grace time of 24 hours can be credited in every sequence where the SFPC system is lost. Practically this means that the grace time can be credited in sequence 2, 3 and 4 in the example event tree for the transient in Figure 28. This is modelled with an AND-gate where the basic event GRACE-TIME is added as input in the fault tree in second function event (SFPC-R), see Figure 29. With this modelling the event GRACE-TIME will exist in all MCS for sequence 2, 3 and 4. It can be noted also that in order to be able to also run a frequency analysis, the probability of the basic event GRACE-TIME is set to 1.0. If I&AB is chosen as a calculation method, the basic event will be treated as a grace time event. If any other calculation methods are chosen, the basic event will be treated as defined in the basic events list (in this case as a probability event with Q=1.0).

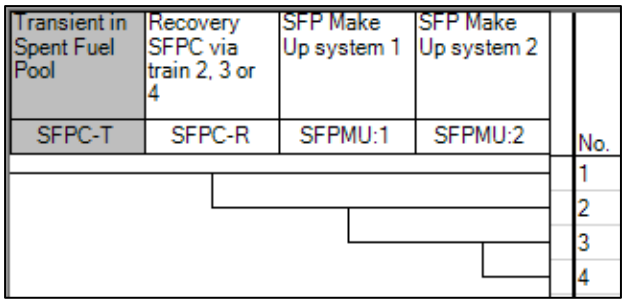

Figure 28. Event Tree representing a transient.

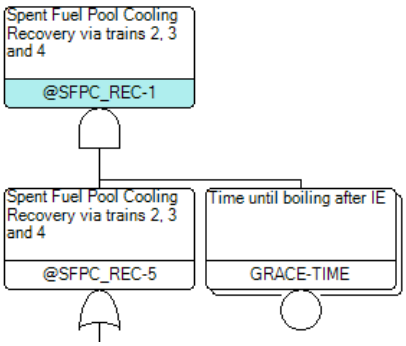

Figure 29. Modelling of the grace time in the fault tree logics.

The deterministic time of 336 hours can be credited in sequences where any of the MU systems functions, which means sequence 2 and 3 in Figure 28. This is modelled with the basic event DET-TIME as an input to an OR top gate in the function events SFPMU:1 and SFPMU:2, see Figure 30. This can be interpreted as either the MU system fails OR extra time is bought (which equals to MU system functions).

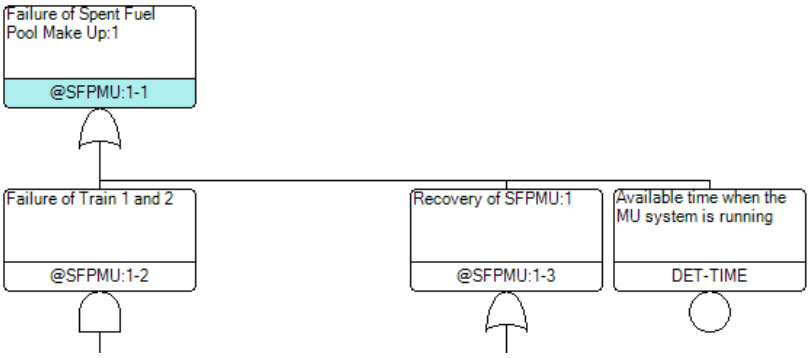

Figure 30. Modelling of the deterministic time in the fault tree logics.

With the above described modelling, the events GRACE-TIME and DET-TIME will appear in the MCS lists in sequences where the corresponding extra time can be credited.

6.1.3.1.2 Results and Interpretation

Table 16 presents the results from the base model where no repair is modelled (column FREQ) and compares it with the I&AB calculation (column I&AB) where repair and time windows are credited. The main conclusion from the comparison of the results is that the static PSA approach where no repair is credited is largely conservative.

Table 16. Results from the PROSAFE SFP model pilot study using the I&AB method.

Consequence Analysis Case	Description	FREQ [year^{-1}]	I&AB [year^{-1}]	Diff
SFP-FAB-EX_SNOW	Feed and boil - External, extreme snow	3.1E-06	1.2E-06	-63%
SFP-FAB-LOOP	Feed and boil - LOOP	2.7E-06	1.8E-08	-99%
SFP-FAB-TRANS	Feed and boil - Transients	1.1E-04	3.5E-05	-67%
SFP--FD-EX_SNOW	Fuel Damage - External, extreme snow	4.2E-07	8.8E-08	-79%
SFP--FD-LOOP	Fuel Damage - LOOP	2.2E-07	2.6E-10	-100%
SFP--FD-TRANS	Fuel Damage - Transients	6.0E-08	4.5E-09	-93%
CORE-CD-EX_SNOW	Core Damage - External, extreme snow	2.0E-07	8.8E-08	-56%

By studying the MCS list we also learn that the order of the MCSs are not the same when we compare the quantifications. To get an understanding of this implication, the 30 first MCSs for LOOP events that lead to the consequence feed and boil are presented in more detail (consequence analysis case SFP-FAB-LOOP). The 30 first MCSs for the frequency calculation with no repair credited are presented in Table 17. Note that in this calculation the basic event GRACE-TIME is treated as a probability event with Q=1.0. The 30 first MCSs for the I&AB calculation with repair and grace time credited are presented in Table 18.

In Table 17 MCS #7 represents a sequence with LOOP followed by fail to run of the diesel for SFPC system train 1 (ACP10DG001_____D), the gas turbine fails to start (ACN10GT001_____A) combined with a failure to run CCF for the SFPC system pumps in train 2, 3 and 4 (CCF-SFPC-PM--A-3AD). This MCS contributes with almost 2 % to the total frequency. In Table 18 we find the same MCS on #30 contributing with 0.2 % to the total frequency. This MCS has two failure in function events (FIFs). This implicates that the dynamic aspects of this MCS could be of great importance. When there is two or more FIFs in the MCS it is possible to have one component running while another component is being repaired. In this example this dynamic aspect clearly is significant as this MCS is not contributing as much to the total risk when the analysis case is quantified with I&AB.

The most contributing MCS in Table 18 with 44 % is LOOP followed by a failure to run CCF for all four pumps in the SFPC system (CCF-SFPC-PM--D-ALL). In Table 17 this sequence contributes with less than 2 % to the total risk, see #15. While MCSs with several repairable events (including both FIF and failure on demand (FOD) events) in general are supressed in Table 18 compared to Table 17, MCSs including only one FIF or FOD are not supressed as much and thus become more important contributors to the total risk. Another example of this is MCS #3 in Table 18, which represents the sequence with LOOP followed by failure to run for the SFPC system pump in train 1 (SFPC_P1_____D) and failure of the manual action to start the standby trains in the SFPC system (SFPC_MANSTART_____H). In this MCS only the pump in train 1 is a repairable event.

These observations are of course also dependent of the input parameters (sequence MTTR, grace time and deterministic time) used in this particular example. However, the main finding here is that taking the dynamic aspects with repair and available time into account, the most contributing sequences could be different from the results in the static PSA approach with no repair taken into account.

New reflections may of course naturally arise while studying the MCS list from a dynamic analysis and the “new” dominating sequences. In this pilot study for example the most contributing MCS in Table 18 is LOOP followed by CCF failure to run for all four SFPC system pumps. One could reflect upon if this MCS is well represented in a dynamic model. Right before the initiating event one pump is in operation (functioning) and the other three in standby. A question that arises is, is it then reasonable to model all of them in one CCF group for this sequence? Does the modelling of this sequence contain some significant conservatisms? These questions are not answered within the scope of this project, however these are some reflections that was found of interest while studying the results in the pilot study.

Table 17. The top 30 MCS from analysis case SFP-FAB-LOOP with frequency calculation with no repair credited.

#	Q	%	Event 1	Event 2	Event 3	Event 4	Event 5
1	5.97E-07	22.01	!IE-LOOP	ACN10GT001_____A	ACP-DG--------D-ALL	GRACE-TIME	
2	2.75E-07	10.14	!IE-LOOP	ACN10GT001_____M	ACP-DG--------D-ALL	GRACE-TIME	
3	1.40E-07	05.17	!IE-LOOP	ACN10GT001_____A	ACP10DG001_____D	GRACE-TIME	SFPC_MANSTART_____H
4	6.95E-08	02.56	!IE-LOOP	ACN10GT001_____A	ACP-DG--------A-ALL	GRACE-TIME	
5	6.46E-08	02.38	!IE-LOOP	ACN10GT001_____M	ACP10DG001_____D	GRACE-TIME	SFPC_MANSTART_____H
6	6.31E-08	02.32	!IE-LOOP	ACN10GT001_____A	ACP10DG001_____D	GRACE-TIME	SFPC_DIAG_____H
7	**5.16E-08**	**01.90**	**!IE-LOOP**	**ACN10GT001_____A**	**ACP10DG001_____D**	**CCF-SFPC-PM--A-3AD**	**GRACE-TIME**
8	5.16E-08	01.90	!IE-LOOP	ACN10GT001_____A	ACP-DG--------D-3AA	GRACE-TIME	SFPC_P4_____A
9	5.16E-08	01.90	!IE-LOOP	ACN10GT001_____A	ACP-DG--------D-3AB	GRACE-TIME	SFPC_P3_____A
10	5.16E-08	01.90	!IE-LOOP	ACN10GT001_____A	ACP-DG--------D-3AC	GRACE-TIME	SFPC_P2_____A
11	5.07E-08	01.87	!IE-LOOP	ACN10GT001_____A	ACP-DG--------D-3AD	ACP10DG001_____D	GRACE-TIME
12	5.07E-08	01.87	!IE-LOOP	ACN10GT001_____A	ACP-DG--------D-3AC	ACP20DG001_____D	GRACE-TIME
13	5.07E-08	01.87	!IE-LOOP	ACN10GT001_____A	ACP-DG--------D-3AA	ACP40DG001_____D	GRACE-TIME
14	5.07E-08	01.87	!IE-LOOP	ACN10GT001_____A	ACP-DG--------D-3AB	ACP30DG001_____D	GRACE-TIME
15	**4.47E-08**	**01.65**	**!IE-LOOP**	**CCF-SFPC-PM--D-ALL**	**GRACE-TIME**		
16	3.20E-08	01.18	!IE-LOOP	ACN10GT001_____M	ACP-DG--------A-ALL	GRACE-TIME	
17	2.91E-08	01.07	!IE-LOOP	ACN10GT001_____M	ACP10DG001_____D	GRACE-TIME	SFPC_DIAG_____H
18	2.37E-08	00.88	!IE-LOOP	ACN10GT001_____M	ACP10DG001_____D	CCF-SFPC-PM--A-3AD	GRACE-TIME
19	2.37E-08	00.88	!IE-LOOP	ACN10GT001_____M	ACP-DG--------D-3AB	GRACE-TIME	SFPC_P3_____A
20	2.37E-08	00.88	!IE-LOOP	ACN10GT001_____M	ACP-DG--------D-3AA	GRACE-TIME	SFPC_P4_____A
21	2.37E-08	00.88	!IE-LOOP	ACN10GT001_____M	ACP-DG--------D-3AC	GRACE-TIME	SFPC_P2_____A
22	2.34E-08	00.86	!IE-LOOP	ACN10GT001_____M	ACP-DG--------D-3AD	ACP10DG001_____D	GRACE-TIME
23	2.34E-08	00.86	!IE-LOOP	ACN10GT001_____M	ACP-DG--------D-3AA	ACP40DG001_____D	GRACE-TIME
24	2.34E-08	00.86	!IE-LOOP	ACN10GT001_____M	ACP-DG--------D-3AC	ACP20DG001_____D	GRACE-TIME
25	2.34E-08	00.86	!IE-LOOP	ACN10GT001_____M	ACP-DG--------D-3AB	ACP30DG001_____D	GRACE-TIME
26	2.06E-08	00.76	!IE-LOOP	ACN10GT001_____A	ACP10DG001_____D	CCF-SFPC-PM--A-ALL	GRACE-TIME
27	1.63E-08	00.60	!IE-LOOP	ACN10GT001_____A	ACP10DG001_____A	GRACE-TIME	SFPC_MANSTART_____H
28	**1.05E-08**	**00.39**	**!IE-LOOP**	**GRACE-TIME**	**SFPC_MANSTART_____H**	**SFPC_P1_____D**	
29	9.50E-09	00.35	!IE-LOOP	ACN10GT001_____M	ACP10DG001_____D	CCF-SFPC-PM--A-ALL	GRACE-TIME
30	7.52E-09	00.28	!IE-LOOP	ACN10GT001_____M	ACP10DG001_____A	GRACE-TIME	SFPC_MANSTART_____H

Table 18. The top 30 MCS from analysis case SFP-FAB-LOOP with I&AB calculation with repair and grace time credited.

#	Q	%	Event 1	Event 2	Event 3	Event 4	Event 5
1	**7.77E-09**	**43.50**	**!IE-LOOP**	**CCF-SFPC-PM--D-ALL**	**GRACE-TIME**		
2	2.04E-09	11.42	!IE-LOOP	ACN10GT001_____A	ACP-DG--------D-ALL	GRACE-TIME	
3	**1.82E-09**	**10.21**	**!IE-LOOP**	**GRACE-TIME**	**SFPC_MANSTART_____H**	**SFPC_P1_____D**	
4	9.40E-10	05.26	!IE-LOOP	ACN10GT001_____M	ACP-DG--------D-ALL	GRACE-TIME	
5	8.21E-10	04.59	!IE-LOOP	GRACE-TIME	SFPC_DIAG_____H	SFPC_P1_____D	
6	4.73E-10	02.65	!IE-LOOP	ACN10GT001_____A	ACP10DG001_____D	GRACE-TIME	SFPC_MANSTART_____H
7	4.15E-10	02.32	!IE-LOOP	ACP10BB001_____Y	GRACE-TIME	SFPC_MANSTART_____H	
8	3.91E-10	02.19	!IE-LOOP	ACN10GT001_____A	ACP-DG--------A-ALL	GRACE-TIME	
9	2.50E-10	01.40	!IE-LOOP	GRACE-TIME	SFPC_H1_____X	SFPC_MANSTART_____H	

#	Q	%	Event 1	Event 2	Event 3	Event 4	Event 5
10	2.18E-10	01.22	!IE-LOOP	ACN10GT001_____M	ACP10DG001_____D	GRACE-TIME	SFPC_MANSTART_____H
11	2.13E-10	01.19	!IE-LOOP	ACN10GT001_____A	ACP10DG001_____D	GRACE-TIME	SFPC_DIAG_____H
12	1.87E-10	01.04	!IE-LOOP	ACP10BB001_____Y	GRACE-TIME	SFPC_DIAG_____H	
13	1.80E-10	01.01	!IE-LOOP	ACN10GT001_____M	ACP-DG--------A-ALL	GRACE-TIME	
14	1.12E-10	00.63	!IE-LOOP	GRACE-TIME	SFPC_DIAG_____H	SFPC_H1_____X	
15	9.81E-11	00.55	!IE-LOOP	ACN10GT001_____M	ACP10DG001_____D	GRACE-TIME	SFPC_DIAG_____H
16	9.19E-11	00.51	!IE-LOOP	CCF-SFPC-PM--D-3AB	GRACE-TIME	SFPC_P3_____A	
17	9.19E-11	00.51	!IE-LOOP	CCF-SFPC-PM--D-3AC	GRACE-TIME	SFPC_P2_____A	
18	9.19E-11	00.51	!IE-LOOP	CCF-SFPC-PM--D-3AA	GRACE-TIME	SFPC_P4_____A	
19	9.19E-11	00.51	!IE-LOOP	CCF-SFPC-PM--A-3AD	GRACE-TIME	SFPC_P1_____D	
20	9.17E-11	00.51	!IE-LOOP	ACN10GT001_____A	ACP10DG001_____A	GRACE-TIME	SFPC_MANSTART_____H
21	6.48E-11	00.36	!IE-LOOP	CCF-SFPC-PM--D-2AB	GRACE-TIME	SFPC_MANSTART_____H	
22	6.48E-11	00.36	!IE-LOOP	CCF-SFPC-PM--D-2AA	GRACE-TIME	SFPC_MANSTART_____H	
23	6.48E-11	00.36	!IE-LOOP	CCF-SFPC-PM--D-2AC	GRACE-TIME	SFPC_MANSTART_____H	
24	4.60E-11	00.26	!IE-LOOP	ACP10BB001_____Y	CCF-SFPC-PM--A-3AD	GRACE-TIME	
25	4.22E-11	00.24	!IE-LOOP	ACN10GT001_____M	ACP10DG001_____A	GRACE-TIME	SFPC_MANSTART_____H
26	4.13E-11	00.23	!IE-LOOP	ACN10GT001_____A	ACP10DG001_____A	GRACE-TIME	SFPC_DIAG_____H
27	3.79E-11	00.21	!IE-LOOP	ACN10GT001_____A	ACP-DG--------D-3AB	GRACE-TIME	SFPC_P3_____A
28	3.79E-11	00.21	!IE-LOOP	ACN10GT001_____A	ACP-DG--------D-3AC	GRACE-TIME	SFPC_P2_____A
29	3.79E-11	00.21	!IE-LOOP	ACN10GT001_____A	ACP-DG--------D-3AA	GRACE-TIME	SFPC_P4_____A
30	**3.76E-11**	**00.21**	**!IE-LOOP**	**ACN10GT001_____A**	**ACP10DG001_____D**	**CCF-SFPC-PM--A-3AD**	**GRACE-TIME**

We can also study the dominating MCS for LOOP events that lead to the consequence fuel damage. The results for these sequences are dominated by failure of the gas turbine and diesels combined with various failures on the MU:2 system and the grace time. Failure of the gas turbine and the diesels will lead to failure of both the SFPC system and the MU:1 system. The grace time in all sequences is 24 hours, which in other words means that repair is only credited within the first 24 hours. This is conservative since repair is thus not credited for any of the MU systems after boiling and before fuel damage. Repair of the MU system within 72 hours between boiling and fuel damage has not been considered in this simplified pilot study. There are several alternatives how this could be credited in the model. One can for example modify the modelling in a way so that different grace times are considered for different sequences. It would also be possible to simply model the repair of the MU system as a probability basic event.

6.1.3.1.3 Sensitivity analysis

Some sensitivity studies are performed for the different input parameters used in the pilot study. The sensitivity analysis is performed for the LOOP analysis cases. The sensitivity of following parameters is studied:

- Deterministic time, 336 hours (extra time bought from running MU system)
- Repair time (MTTR) for the initiating event, 24 hours (time to restore the external grid)
- Grace time, 24 hours (time before boiling)
- Sequence MTTR for components, various values (Total repair time for specific components)

Deterministic Time

The extra time that can be acquired from running any of the MU systems is assumed to be 2 weeks (336 hours). In these sequences the consequence feed and boil is assumed to occur, but it is still possible to avoid fuel damage. During the extra time bought with the MU systems it is possible to restore the initiating event in order to avoid fuel damage. This time is modelled as a deterministic time in I&AB. The graph in Figure 31 shows the results from the sensitivity analysis where various values have been assigned to the deterministic time. If the deterministic time is set to zero, which means no extra time is credited if the MU system functions, the fuel damage frequency is 1.8E-8 per year. With longer deterministic times (~200 hours) the fuel damage frequency converges towards 2.6E-10 per year. For shorter deterministic times, the MCS results will be dominated by events where the MU system functions but the repair of the initiating event within the available time window (in this case including both the grace time and the deterministic time) fails. For the longer deterministic times, the MCS results will be dominated by events where the MU system fails and repair of the initiating event within the available time (grace time) fails.

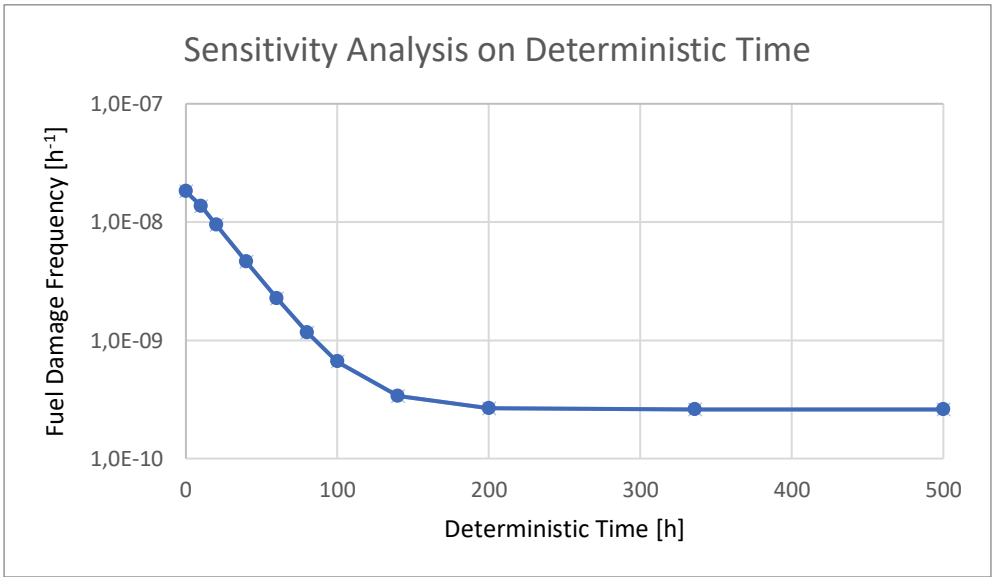

Figure 31. Dependency of the Fuel Damage frequency with different deterministic time values. The base value used in the pilot study is 336 hours.

Time to Repair the Initiating Event

The mean time to restore the external grid is assumed to be 24 hours. This assumption is based on the mission time used in the static PSA approach. The graph in Figure 32 shows the results from the sensitivity analysis where various repair time values have been assigned to the sequence MTTR for the initiating event LOOP.

The slight "bump" in the curve for the FD case that can be noted in the graph is due to the change of the type of dominating MCS. If the repair times for the initiating events is longer (~50 hours), MCS with the MU system functioning but failure to repair the initiating event within the available time window are the dominant contributors to the total fuel damage frequency. For shorter repair times of the initiating event the MCS results will be dominated by events where the MU system fails and repair of the initiating event within the available time (grace time) fails.

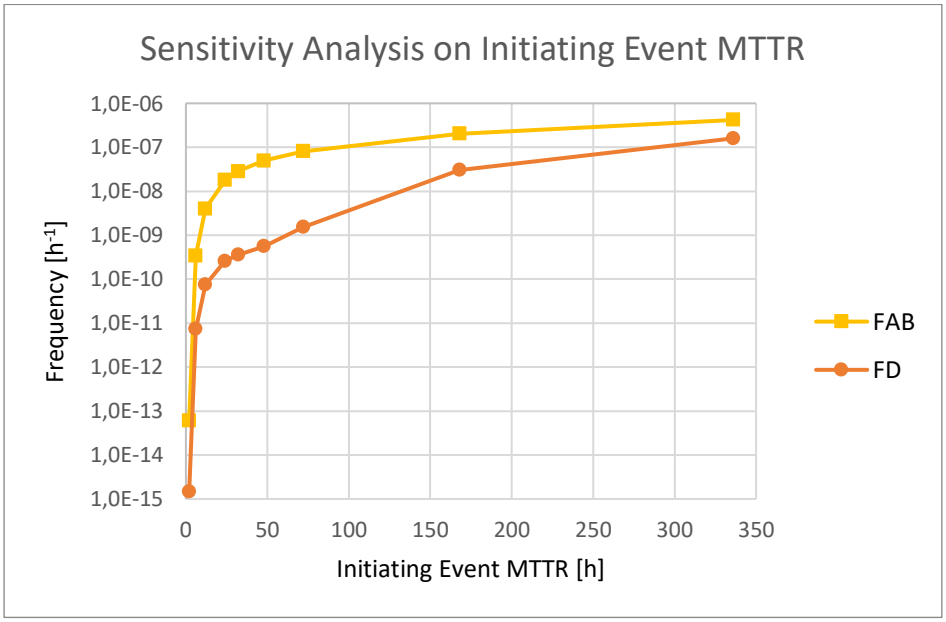

Figure 32. Looking at the dependency of the Fuel Damage frequency and Feed and Boil frequency respectively with different initiating event MTTR values. The base value used in the pilot study is 24 hours.

Grace Time

The grace time used in the pilot study represents the time from the initiating event until boiling of the SFP. This time is set to 24 hours. The graph in Figure 33 shows the results from the sensitivity analysis where various grace time values have been assumed.

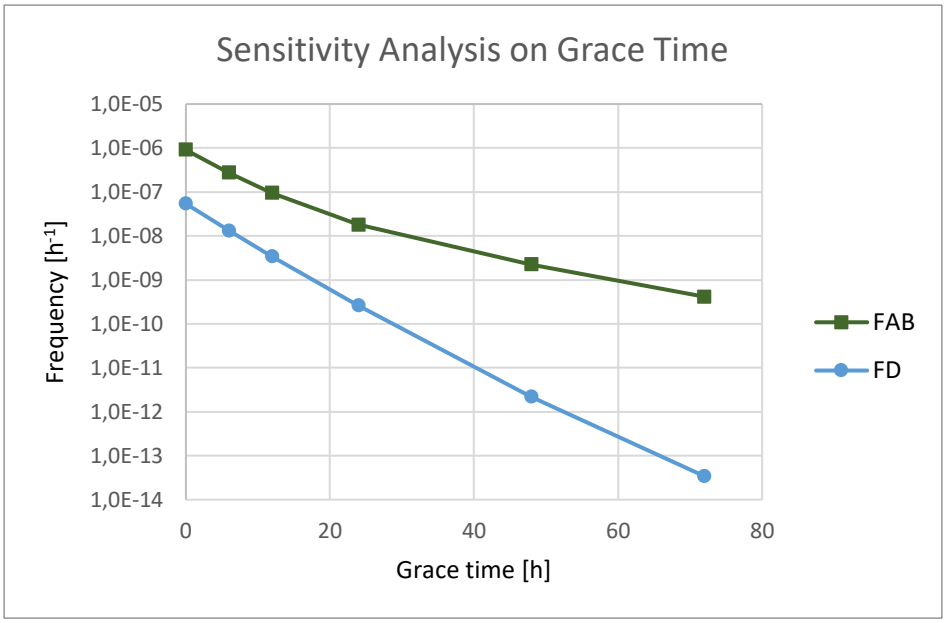

Figure 33. Dependency of the Fuel Damage frequency and Feed and Boil frequency respectively with different grace time values. The base value used in the pilot study is 24 hours.

If the grace time is set to zero it means that we assume that the boiling occurs immediately when the SFPC system fails. In Table 19 we see that with this assumption and still crediting the repairs and extra available time bought from a functioning MU system, the result is significantly lower than in the base model with no repairs.

Table 19. Comparison of results between the frequency calculation and the I&AB calculation crediting repairs but not the extra grace time for the LOOP analysis cases.

Conseq Analysis Case	Description	FREQ	I&AB (grace time = 0h)	Difference
SFP-FAB-LOOP	Feed and boil - LOOP	2.71E-06	9.03E-07	-67%
SFP-FD-LOOP	Fuel Damage - LOOP	2.19E-07	5.39E-08	-75%

Sequence MTTR for components

The sequence MTTR for selected components are assigned with values as described in section 6.1.3.1.1. The graph in Figure 34 shows the results from the sensitivity analysis where all sequence MTTR parameter values have been multiplied with a factor 0.5 versus a factor 2.

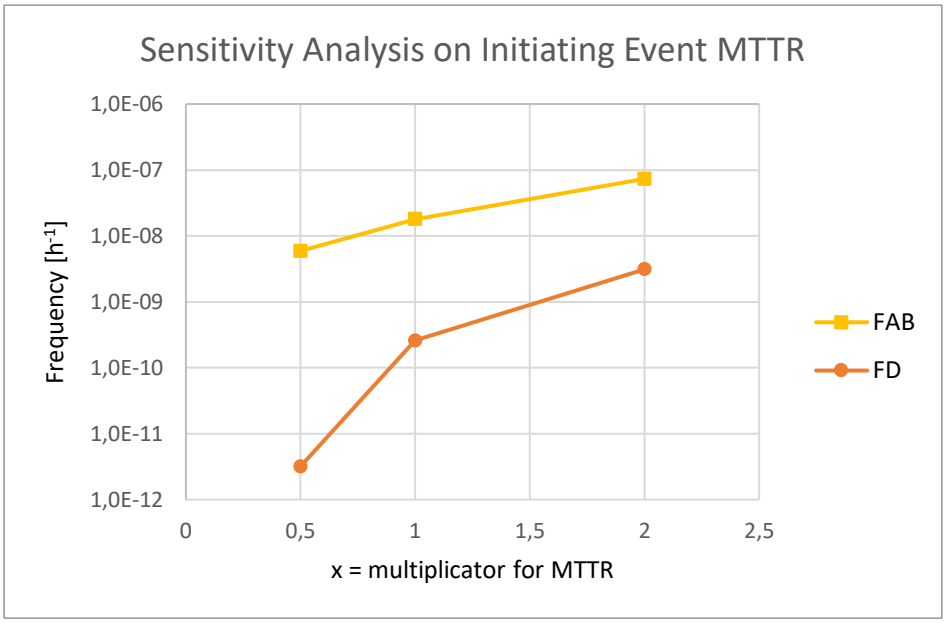

Figure 34. Dependency of the Fuel Damage frequency with different component sequence MTTR values.

It can from Table 20 be concluded that even with assuming double as long repair times, the differences in results from the base model are still large.

Table 20. Comparison of results between the frequency calculation and the I&AB calculation crediting repairs with double as long repair times as in the base study.

Conseq Analysis Case	Description	FREQ	I&AB (double component MTTR)	Diff
SFP-FAB-LOOP	Feed and boil - LOOP	2,71E-06	7,34E-08	-97%
SFP-FD-LOOP	Fuel Damage - LOOP	2,19E-07	3,11E-09	-99%

6.1.3.1.4 Conclusions

From the pilot study on the PROSAFE SFP model the following conclusions can be made:

- Modelling of repair is of great significance of the resulting frequencies for the analysed consequences FAB and FD.
- Time windows in different sequences are also a significant factor for the resulting frequencies.
- Dynamic aspects of failures and repairs in sequences can be of great importance. It is especially significant for sequences containing several failure in function (FIF) events. When there is two or more FIFs in the MCS it is possible to have one component running while another component is being repaired, which was shown to be of importance in this pilot study.
- Taking the dynamic aspects, repair and time windows into consideration may change the overall risk picture of the system. In the pilot study it was shown that the most dominating MCS changed significantly when applying I&AB.
- From the sensitivity analysis on the repair time for the initiating event it can be concluded that it is of importance to assign an accurate value for this parameter, as it has great impact on the result. This parameter can be compared to the mission time used in a static PSA approach. For level 1 PSA it is often assumed to be 24 hours for all

initiating events. The sensitivity analysis suggests that the value of this parameter is of great importance for the analysis results.

- Benefits of using the I&AB method is that the repair and time window modelling are integrated parts in the model. This means that when updates are performed on other parts of the model, no separate updates of the repair or time window modelling is needed. Also, it is possible to model repair and time windows for any selected parts in the model, and still run the common analysis results for the whole model at once.

6.1.3.2 Pilot Study – PROSAFE CORE model

For the PROSAFE reactor model one initiating event was selected to test the I&AB method in a small scale. The studied initiating event is external extreme snow. This will cause loss of offsite power and blocking of the ventilation for the diesel generators and blocking of the sea water intake for cooling. The selected sequence where repair is modelled in this pilot study is the initiating event followed by failure of initial manual actions to remove the snow in combination with failure of the independent core cooling system (ICCS). This is sequence 18 in the event tree in Figure 35.

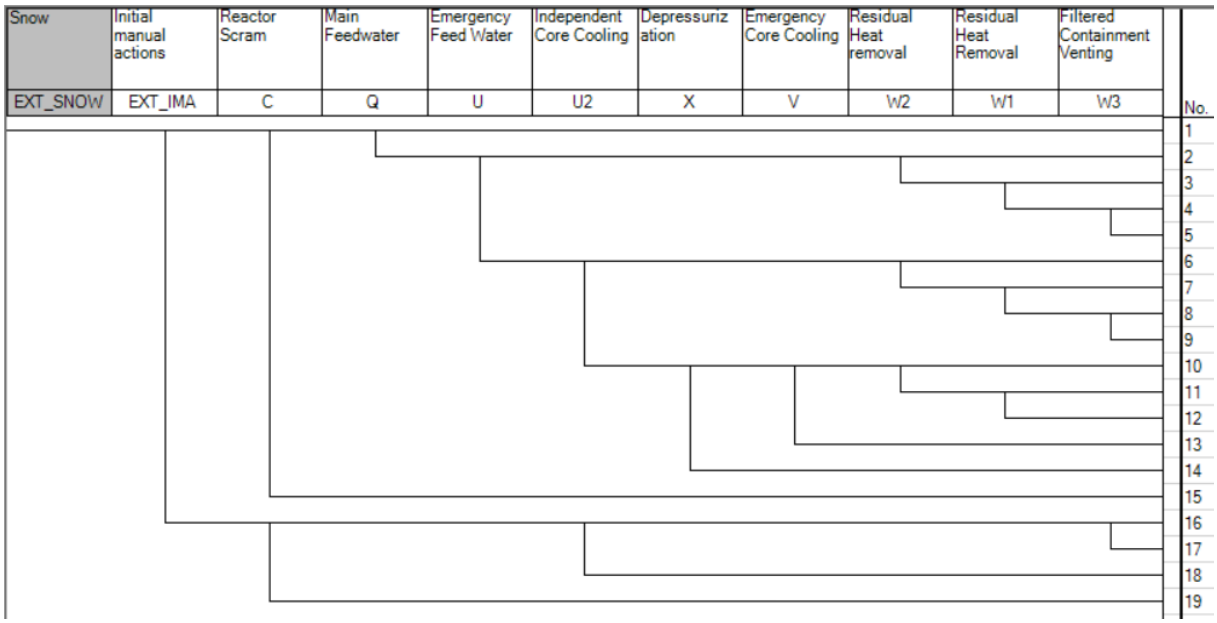

Figure 35. The event tree for the initiating event extreme snow in the PROSAFE core model.

A quite simplified assumption is made that the available time to repair the ICCS is 10 hours. Depending on when in the sequence the ICCS fails this may in reality be a non-conservative assumption. It would be possible to divide the failures into two or more events depending on when in the sequence the failure occurs. Each type of failure can then be combined with a specific grace time. Specifically, early failures such as failure to start may be assumed to be impossible to repair due to the short available time. This can then be modelled as an event that is not repairable or with no grace time.

For this simple pilot test a new basic event GRACE_TIME_10H is introduced to represent the available time before the ICC system has to start. The events that are modelled with repair is the initiating event and failure of the ICC diesel. The assumed sequence MTTR parameters are presented in Table 21.

Table 21. The basic events, including the initiating events, in the PROSAFE model that are assigned a sequence MTTR parameter. The last column, Total MTTR, is the parameter value.

Basic event	Description	Type	Execution MTTR [h] T-book 8	Diagnosis MTTR [h]	Total MTTR [h]
!IE-E_SNOW	Loss of Offsite Power initiating event	Frequency			24
GRACE_TIME_10H	Available Time to repair ICC diesels	Grace Time			
ICC10DG001_____A	Diesel generator fails to start	Mission Time	6	5	11
ICC10DG001_____D	Diesel generator fails to operate	Mission Time	10	5	15

The result is presented in Table 22.

Table 22. Results for the consequence analysis case studied in the pilot study for the PROSAFE Core model.

Conseq Analysis Case	Description	FREQ	I&AB	Diff
CORE-CD-EX_SNOW	Core Damage - External, extreme snow	2.01E-07	8.81E-08	-56%

The most dominating sequences for the studied analysis case in the original model are two sequences with failure of manual actions of snow removal combined with spurious stop of the ICC diesel. With the I&AB method the order of the top ten dominating MCS is unchanged, with the same sequences still dominating. However, the total contribution from the top two most contributing sequences are lower with the I&AB method. In other words, even though the order of the MCS is not changed in this case, the overall contribution from different sequences have changed.

Conclusions

In addition to the conclusions from the SFP model in section 6.1.3.1.4 the following conclusions can be made:

- Modelling of repairs and time windows can be relevant and has a significant impact on sequences related to the core when there is a reasonable amount of time available for repair.
- The timing of the failing events in the sequence could be of more importance when modelling reactor related sequences. This would encourage the use of different grace times in different scenarios.

6.1.3.3 Pilot Study – Full scale SFP model

A limited study is performed on a full scale PSA SFP model. The initiating event LOOP and consequences FAB and FD are studied.

The time windows are assumed to be the same as for the pilot study in the PROSAFE model:

- 24 hours from the initiating event until boiling of the spent fuel pool
- 72 hours from boiling until fuel damage (not credited in this pilot study)
- 336 hours (2 weeks) of extra time available if operation of the MU system can be established.

These time windows were modelled in the same manner as for the PROSAFE model pilot study.

A limited number of components were selected to be modelled with repair:

- SFPC pumps
- Diesel generators
- Diesel breaker
- Start-up batteries for diesel generators

The same sequence MTTR parameters as in the PROSAFE model pilot study were used for the corresponding components. The sequence MTTR parameters for diesel breakers and batteries were assumed to be the same as for diesel failures with spurious stop.

The results are summarized in Table 23. After applying I&AB and taking repair and time windows into account the frequency decrease with 83 % for consequence boiling and 91 % for consequence fuel damage.

Table 23. Results for the consequence analysis case studied in the pilot study for the full scale PSA model.

Analysis Case	**Difference**
LOOP with consequence boiling	-83%
LOOP with consequence fuel damage	-91%

Conclusions
The results from applying I&AB on a full scale model are in line with the results from the PROSAFE model pilot studies. The conclusions that could be drawn from the PROSAFE model pilot study holds also for the application on a full scale model.

6.1.4 Discussion

Uncertainties
The importance and uncertainty analysis in RiskSpectrum PSA is not supported by I&AB in the first version of the tool. Model uncertainties (e.g., the time window modelling) and completeness uncertainties (e.g., HFEs) could be handled as in regular PSA (identification, quantification etc). Some more general discussion of these uncertainties in relation to long time windows can be found in section 0.

Conclusions
The I&AB method includes dynamic aspects of failure and repair processes into the static PSA model. The method is suitable for modelling of sequences with long mission times/unknown mission times and long time-windows. It is easy to embed in an already existing RiskSpectrum model and it is possible to use I&AB on selected components/events, analysis cases or parts of the model. The additional information needed is

- Information about time windows
- MTTR for components/events
- MTTR for the initiating event

From the pilot studies it can be concluded that

- Modelling repair is of great significance for the overall frequency result.

- Taking the dynamic aspects, repair and time windows into consideration may change the overall risk picture of the system. In the pilot study it was shown that the most dominating MCS changed significantly when applying I&AB.
- Benefits of using the I&AB method is that the repair and time window modelling are integrated parts in the model. This means that when updates are performed on other parts of the model, no separate updates of the repair or time window modelling is needed. Also, it is possible to model repair and time windows for any selected parts in the model, and still run the common analysis results for the whole model at once.

6.2. Enhanced fault/event tree

6.2.1 Method

The method proposed here involves some degree of iteration with the following general steps that can be modified accordingly to the specific application, real-world conditions, and level of accuracy (since it uses a graded approach). To model repair in PSA, the steps to consider are:

1. Define a safe and stable state, a semi-unstable state and perhaps an unstable state.
2. Run analysis.
3. Identify important repairable failure events from importance list.
4. For these (steps 1 to 3) identify relevant time windows (by use of IE/function/time window matrix).
5. Model time windows acc. to steps 1 to 4 if necessary.
6. Run analysis.
7. Identify possible repairs to model from MCS list.
8. Perform repair analysis (several sub tasks).
9. Re-calculate MCS list with repair events added.
10. Iterate (if needed).

The method is based on requantifying the MCS-list and some fault tree modelling (to acquire relevant time windows for sequences).

1. Define a safe and stable state, a semi-unstable state under which repair is possible and perhaps an unstable state where repair is not possible

The starting point for the analysis is a pre-existing PSA model (M1). Define the safe and stable state. Consider what the failure state is. The failure state should be the unwanted consequence in PSA and when reached there should be no possibility for repair. Then consider all consequences that are neither in the safe state nor the failure state and consider those as semi stable states. Equip the relevant event trees with the relevant states accordingly.
Examples of semi stable states:

- SFP: Feed and boil of the spent fuel pool
- Core: Filtered containment venting
- Core: Feed and bleed?

If there are obvious repair opportunities, then those could be modelled in this step, but it is not a part of the method.

2. **Run analysis**

With the consequences and states set up, run the analysis. Also include the importance analysis producing fractional contribution (FC) or similar.

3. **Identify important repairable failure events from importance list**

Consider all events from the importance list (and perhaps from the MCS list) that there is a reasonable possibility to repair. Identify events that may be repairable from the PSA-results. The list of events is then analysed using HRA-techniques. The HRA-methods are further described in section 0, but in short it should be demonstrated that the proposed action is plausible. This is done by screening the basic event list of cases where no repair is possible. When there is enough available time in an accident sequence, potential new human actions, e.g. recovery actions and repair actions can be considered. These new human actions can only be modelled if they are plausible and feasible for the scenarios to which they will be applied. This step should be made in close cooperation with the HRA team to ensure that no relevant manual action is missed.

4. **For these (steps 1 to 3) identify relevant time windows for repair**

With the reduced list of repairable basic events identify, the type of repair (and/or recovery) with long time windows. Some repair possibilities can differ regarding time windows and the constraints the time windows put on the operator (in terms of stress etc.). Consider these two cases of failure events and the different functions that need to be operational:

1. Failure events that initially do not lead to the unwanted consequence, but there is considerable time pressure before the consequence is reached if nothing is done. This could for example be the spent fuel pool where both the regular cooling system and the Make-up cooling system fail and there is some time before the water starts boiling followed by the uncovering of the fuel.
2. Repair events needed to establish system functions to obtain a safe and stable state with prolonged time perspective. For example
    a. Operation of the Make-up cooling systems for the spent fuel pool when no immediate danger is present, but the feed and boil is considered a semi stable state. In this case it is preferred to repair the ordinary cooling system, both because the state of the reactor might not be fully “safe” since less equipment need to fail to cause fuel uncovering, and because there might be additional negative consequences in boiling water.
    b. Use of the filtered containment venting in the core model. This is considered safe within the current scope of level 1 PSA (24h) but might not be if longer time windows are considered.

These events with long available time are not yet considered in the present state of the art PSA modelling.

Investigate the surrounding time window aspects around these events (these could vary depending on initiating event). This is preferably summarized in an IH/function/time window matrix. A proposed structure for the spent fuel pool where no additional time window modelling is proposed can be according to Table 24 (the transient case). The 24 hours is the time to boil and the 72 hours is the time until uncovered fuel (assuming repair is only relevant after boiling has started).

Table 24. Time window matrix for the transient case (SFP).

IE	Time window	SFPC	SFPMU	
		SFPC	SFPMU:1	SFPMU:2
SFP Transient	Mission time	24	24	24
	Fill up SFPC	-	5	5
	Available time (repair)	24	72	72
…	…			

Then the LOOP case is shown in Table 25. The 24 hours is the time to boil and the 72 hours is the time until uncovered fuel (assuming repair is relevant after initiating event).

Table 25. Time window matrix for the LOOP case (SFP).

IE	Time window	Power supply
		Diesel generator
SFP LOOP	Mission time	24
	Available time (repair)	96 (24+72)
…	…	

In the core model, the core cooling and reactivity control is of interest for repair and especially the core cooling will need some additional time window modelling. An example of the core cooling for the external event is given in Table 26. The failure to run of the diesel generators is assumed non-repairable in the first 12 hours (0 available time) and repairable after 12 hours with 10 hours available time (time to fuel uncovery).

Table 26. Time window matrix for the external event (core model).

IH	Time window	Initial manual actions	Independent core cooling			
		Snow cleaning	Independent core cooling pump		Independent core cooling diesel generator	
			0-12 hours	12-24 hours	0-12 hours	12-24 hours
Core External	Mission time	12	12	12	12	12
	Available time (repair and manual actions)	12	0	10	0	10
…	…					

5. Model time windows acc. to steps 1 to 4 if necessary

If the conclusion is that additional time windows must be modelled, return to step 1, and consider all modifications that must be done at each step. Modelling of time windows is most likely best solved in the fault trees and/or with the use of exchange events in the static PSA model. Modelling it with recalculation of the MCS list might result in much extra work.

6. Run the analysis

With all event trees, repairable events and time windows set up, run the analysis.

7. Identify possible repairs to model from MCS-list

With the model updated according to previous steps, identify the repairable minimal cut sets/sequences from the MCS list. For each minimal cut set identify every repair that is possible regarding the individual events and the sequence. For example, are there basic events (including initiating events) in a minimal cut set that might make repair of another event more difficult or impossible? Repair will be more difficult if previously modelled HFEs are dominating since they represent failure of manual actions which might affect the repair events.

8. **Perform repair analysis**

Quantification is done by using statistical analysis with exponential distribution. The diagnosis should be considered if it cannot be shown to have a low contribution.
The following should be considered:

- If the basic events are all HFEs no quantification is possible (since the "repair" of the event is just the recovery modelling in HRA).
- If there are many repairable failure events, HRA should be used to quantify these minimal cut sets (to account for dependencies between human actions).
- If there are few repairable events, the execution part (MTTR) is probably dominating (consider on a case to case basis whether the diagnosis should be quantified).

9. **Re-calculate MCS list with repair events added.**

After identification of repairable events in the MCS modify the cut set list by inserting repair events.

10. **Iterate (if needed)**

If the level of required detail is not met iterate steps 1-9. It is preferred that the top cutsets (i.e. top 99% of probability mass) have either a repair basic event or are declared non-repairable (non-repairable components or HRA-basic events). This will ensure the relevant repairs have been considered.

The steps 1-5 probably do not have to updated if only small changes have been done in a model update.

6.2.2 PROSAFE SFP model

6.2.2.1 Model and assumptions

The pilot study handled the PROSAFE spent fuel pool model. The safe state is defined as the system for cooling of fuel is active and running. This is shown in Figure 36 as SaSS. There are four different states, the state of heating water (state HW, water is not boiling), the feed and boil state (state FAB, water is boiling and Make-up systems are running), the boil state (B, water is boiling with no Make-up system running) and the fuel damage state. There are three possible repairs: the repair of cooling before boiling, repair of cooling (with a Make-up system running in the Feed and Boil state) and the repair of a Make-up system. Repair of cooling from the Feed and Boil state will have long available time (2 weeks is assumed in the PROSAFE model). Repair of the Make-up system before uncovered fuel will have less available time (72 hours if calculated after boil or 96 hours if calculated after IE).

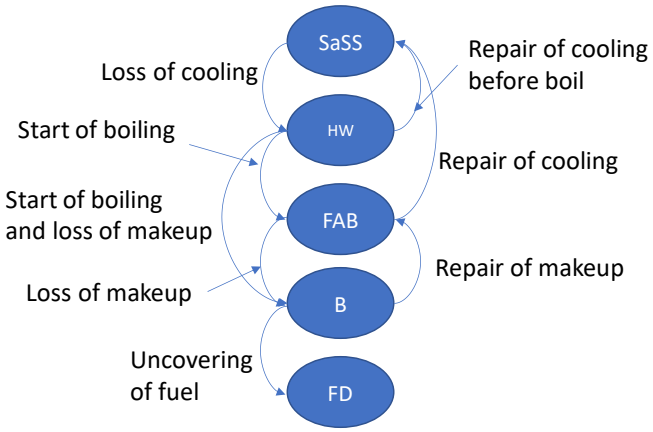

Figure 36. States for the spent fuel pool and transitions (failures and repairs) between states.

Repair of cooling before boiling and repair of Make-up can both easily be considered in the method. Repair of cooling with a Make-up system running can be considered with some additional work, in these pilot studies this repair is mainly investigated with a Markov analysis.

Timing of events are not considered in the method evaluation. To evaluate the initial state (i.e whether the repair analysis starts from Feed and boil (FAB) or the Boil (B) state) the mission time is set to 24 hours. Running the analysis with an unchanged mission time was chosen partly to better be able to compare the results with the ordinary PSA and since it is not clear how the failure data might be affected. This is possible since it is mostly the repair failure events that are affected by the longer time windows. For CCF events, only repair up to success criteria is considered. The most relevant parameters for the repair probabilities from the HRA repair analysis are shown in Table 27.

Table 27. Parameters

Parameter	**Value**
Diesel_repair	6,30E-02
Pump repair	8,09E-05

6.2.3 Pilot Study results SFP model

The quantitative results for the fuel damage give the highest impact of repair in the LOOP case, second highest in the Transient case and the lowest in the External event case. Sensitivity analysis (for all repair parameters congregated) gives the highest relative impact for the transient case and if the input probabilities are increased with a factor of 10 then the impact of the repair changes from -90 % to -54 % (in relation to the unrepaired frequency). The LOOP case changes the most relatively by almost a factor of 10 (by comparing the repaired frequency with the sensitivity frequency). The external event (the extreme snow) case changes the most in absolute value when applying the sensitivity analysis. This can be seen in Table 28.

Table 28. Results for SFP model.

IE	EX SNW	LOOP	TRANS
IE-freq [1/y]	1,00E-04	1,00E-01	1
No repair freq	4,36E-07	2,33E-07	6,26E-08
Repair freq	1,83E-07	1,02E-09	6,44E-09
	-58%	-100%	-90%
Repair sensh 10	2,59E-07	9,39E-09	2,89E-08
	-41%	-96%	-54%
Repair sensl 10	1,75E-07	1,87E-10	4,19E-09
	-60%	-100%	-93%

In Figure 37 the same effect is shown for the three initiating events of the spent fuel pool.

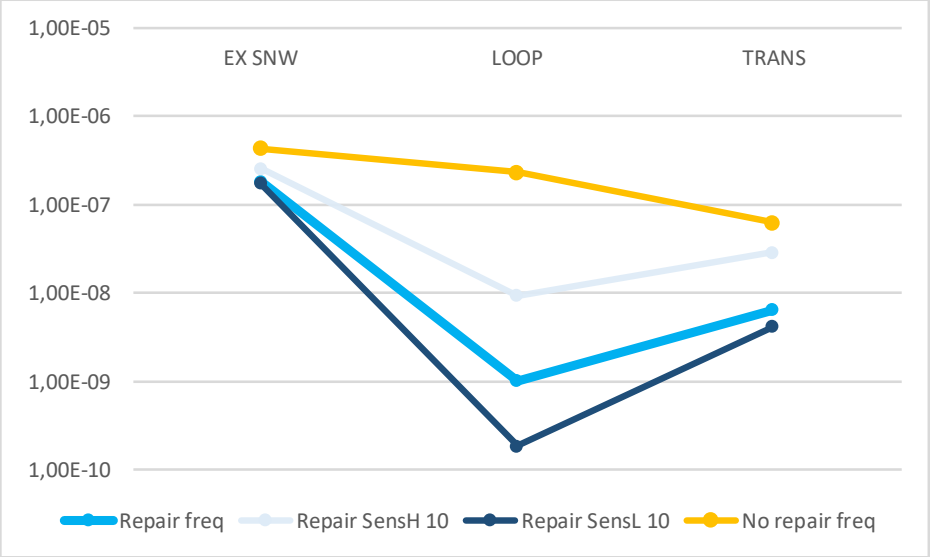

Figure 37. Results for SFP model.

SFP Transient case – Fuel damage

The initiating event is caused either by a failure of pump 1 or the heat exchanger, but the pump is dominating as can be seen in Table 29. The remaining trains and the Spent fuel pool Make-up pumps are made unavailable mostly by failure to execute manual actions e.g., start pumps or to do the diagnosis part. There is also a significant contribution from mechanical failures for pumps. Timing for the failures will impact the sequence, but since the time windows are long (several days) a conservative approach of not considering different timing of events was deemed sufficient for the pilot study. Since for example if you model an event not to occur simultaneously by adding some "extra time" the available time for repair changes less relatively speaking if you have a long time window for repair compared to a shorter one. In general, the diesel generators have a low contribution for the transient case but the diesel generator for the Spent fuel pool Make-up system 2 do appear in some contributing minimal cut sets.

Table 29. Most contributing MCS for Transient SFP before repair. HFEs are blue-marked and events (both independent and CCF) chosen for repair are yellow-marked. The "NEW" column is the MCS order number in the MCS list with repair events and the "No" column is the order number in this MCS list (before repair).

NEW	No	Probability	%	Initiating event	Event 1	Event 2	Event 3	Event 4	Event 5
5	1	4,28E-09	6,84E+00	SFPC_P1_____I___D	CCF-SFPM1-PM-A-ALL	SFPC_MANSTART_____H	SFPMU:2_DIAG_____H		
6	2	3,36E-09	5,36E+00	SFPC_P1_____I___D	CCF-SFPM1-PM-A-ALL	SFPC_MANSTART_____H	SFPMU:2_P1_____A		
63	3	3,31E-09	5,28E+00	SFPC_P1_____I___D	ACP__DG102_FLEX2___D	CCF-SFPM1-PM-A-ALL	SFPC_MANSTART_____H		
8	4	2,84E-09	4,53E+00	SFPC_P1_____I___D	SFPC_MANSTART_____H	SFPMU:1_P1_____A	SFPMU:1_P2_____A	SFPMU:2_DIAG_____H	
11	5	2,23E-09	3,56E+00	SFPC_P1_____I___D	SFPC_MANSTART_____H	SFPMU:1_P1_____A	SFPMU:1_P2_____A	SFPMU:2_P1_____A	
1	15	1,02E-09	1,62E+00	SFPC_P1_____I___D	SFPC_MANSTART_____H	SFPMU:1_MANSTART___H	SFPMU:2_DIAG_____H		
2	29	4,58E-10	7,31E-01	SFPC_P1_____I___D	SFPC_DIAG_____H	SFPMU:1_MANSTART___H	SFPMU:2_DIAG_____H		
3	36	3,74E-10	5,97E-01	SFPC_P1_____I___D	CCF-SFPC-PM--A-3AD	SFPMU:1_MANSTART___H	SFPMU:2_DIAG_____H		
4	39	3,46E-10	5,52E-01	SFPC_P1_____I___D	SFPC_MANSTART_____H	SFPMU:1_DIAG_____H	SFPMU:2_DIAG_____H		

The repair is inserted in the MCS-list as in Table 30.

Table 30. Most contributing MCS for Transient SFP after repair. HFEs are blue-marked and events (both independent and CCF) chosen for repair are yellow-marked. The "OLD" column is the MCS order number in the MCS list without repair events and the "No" column is the order number in this MCS list (considering repair).

OLD	No	Probability	%	Initiating event	Event 1	Event 2	Event 3	Event 4	Event 5
15	1	1,02E-09	1,58E+01	SFPC_P1_____I___D	SFPC_MANSTART_____H	SFPMU:1_MANSTART___H	SFPMU:2_DIAG_____H		
29	2	4,58E-10	7,11E+00	SFPC_P1_____I___D	SFPC_DIAG_____H	SFPMU:1_MANSTART___H	SFPMU:2_DIAG_____H		
36	3	3,74E-10	5,81E+00	SFPC_P1_____I___D	CCF-SFPC-PM--A-3AD	SFPMU:1_MANSTART___H	SFPMU:2_DIAG_____H		
39	4	3,46E-10	5,37E+00	SFPC_P1_____I___D	SFPC_MANSTART_____H	SFPMU:1_DIAG_____H	SFPMU:2_DIAG_____DH		
1	5	2,70E-10	4,19E+00	SFPC_P1_____I___D	CCF-SFPM1-PM-A-ALL	SFPC_MANSTART_____H	SFPMU:2_DIAG_____H	T_PUMP-REPAIR_____H	
2	6	2,12E-10	3,29E+00	SFPC_P1_____I___D	CCF-SFPM1-PM-A-ALL	SFPC_MANSTART_____H	SFPMU:2_P1_____A	T_PUMP-REPAIR_____H	
4	8	1,79E-10	2,78E+00	SFPC_P1_____I___D	SFPC_MANSTART_____H	SFPMU:1_P1_____A	SFPMU:1_P2_____A	SFPMU:2_DIAG_____H	T_PUMP-REPAIR_____H
5	11	1,40E-10	2,18E+00	SFPC_P1_____I___D	SFPC_MANSTART_____H	SFPMU:1_P1_____A	SFPMU:1_P2_____A	SFPMU:2_P1_____A	T_PUMP-REPAIR_____H
3	63	1,32E-11	2,04E-01	SFPC_P1_____I___D	ACP__DG102_FLEX2___D	CCF-SFPM1-PM-A-ALL	SFPC_MANSTART_____H	T_PUMP-REPAIR_____H	

The first MCS (in Table 29) in the MCS starts with the initiating event failure of pump 1 for the Spent fuel pool cooling system. The water in the Spent fuel pool will now start to heat, and the operators will try to start a redundant train of the Spent fuel pool cooling system before the water starts boiling after 24 hours. This execution will fail in this sequence and will cause the water level to decrease. Operators will then try to start one of the pumps in Spent fuel pool Make-up system 1 to initiate cooling but both will fail to start due to mechanical CCF. Then there is a failure of diagnosis of Spent fuel pool Make-up system 2 and that system is thus unable to start. This will lead to uncovered fuel and fuel damage if not repair is considered. Diagnosis for repair of Spent fuel pool Make-up system 1 can be started immediately after it is concluded that Make-up system 1 is not starting. Repair of Spent fuel pool Make-up system 2 is not possible since the manual action of diagnosis is preventing the usage of repair in this case (the recovery of the manual action should perhaps be investigated in more detail if needed).
The second and third sequence is similar to the first but the failure of diagnosis of start of Spent fuel pool Make-up system 2 is replaced by the failure to start mechanically or the failure of the diesel generator for Make-up system 2. It would be possible to model the repair of the component according to the enhanced MCS-method but repair of Spent fuel pool Make-up system 1 is preferred since it among other aspects does not provide sea water. The repair of Spent fuel pool Make-up system 1 is handled the same way as in the first sequence. The fourth, fifth and sixth sequence is similar to the first, second and third but with the pumps in Spent fuel

pool Make-up system 1 failing from independent failures instead of by CCF. Then sequences appear with failure to diagnose start of redundant trains in the Spent fuel pool cooling system.

SFP LOOP Case – Fuel damage

The initiating event causes the offsite power to fail and thus the cooling systems will be dependent on diesel generators or the gas turbine. In the sequence, the gas turbine is unavailable either by failure or maintenance. Then the sequences contain failure of diesel generator by CCF mainly 4oo4 (although 3oo4 appear in more unlikely cutsets). This combination will make the Spent fuel pool Cooling system unavailable and the Spent fuel pool Make-up system 1 pumps. Spent fuel pool Make-up system 2 fails by manual actions or by pump- or diesel generator failure. This can be seen in Table 31.

Table 31. Most contributing MCS for LOOP SFP before repair. HFEs are blue-marked and events (both independent and CCF) chosen for repair are yellow-marked. The "NEW" column is the MCS order number in the MCS list with repair events and the "No" column is the order number in this MCS list (before repair).

NEW	No	Probability	%	Initiating event	Event 1	Event 2	Event 3	Event 4
1	1	3,00E-08	1,29E+01	!IE-LOOP	ACN10GT001_____A	ACP-DG-------D-ALL	SFPMU:2_DIAG_____H	
2	2	2,36E-08	1,01E+01	!IE-LOOP	ACN10GT001_____A	ACP-DG-------D-ALL	SFPMU:2_P1_____A	
3	3	2,32E-08	9,95E+00	!IE-LOOP	ACN10GT001_____A	ACP-DG-------D-ALL	ACP__DG102_FLEX2___D	
4	4	1,38E-08	5,94E+00	!IE-LOOP	ACN10GT001_____M	ACP-DG-------D-ALL	SFPMU:2_DIAG_____H	
5	5	1,09E-08	4,66E+00	!IE-LOOP	ACN10GT001_____M	ACP-DG-------D-ALL	SFPMU:2_P1_____A	
6	6	1,07E-08	4,59E+00	!IE-LOOP	ACN10GT001_____M	ACP-DG-------D-ALL	ACP__DG102_FLEX2___D	
9	7	3,50E-09	1,50E+00	!IE-LOOP	ACN10GT001_____A	ACP-DG-------A-ALL	SFPMU:2_DIAG_____H	
7	518	2,07E-11	0,00891	!IE-LOOP	ACN10GT001_____A	RPSXXPU00XSW1____YS	SFPMU:2_DIAG_____H	

The repair is inserted in the MCS-list as in Table 32.

Table 32. Most contributing MCS for Transient SFP before repair. HFEs are blue-marked and events (both independent and CCF) chosen for repair are yellow-marked. The "OLD" column is the MCS order number in the MCS list without repair events and the "No" column is the order number in this MCS list (considering repair).

OLD	No	Probability	%	Initiating event	Event 1	Event 2	Event 3	Event 4
1	1	1,2E-10	11,7	!IE-LOOP	ACN10GT001_____A	ACP-DG-------D-ALL	LOOP_DIESEL-REPAIR_H	SFPMU:2_DIAG_____H
2	2	9,38E-11	9,19	!IE-LOOP	ACN10GT001_____A	ACP-DG-------D-ALL	LOOP_DIESEL-REPAIR_H	SFPMU:2_P1_____A
3	3	9,23E-11	9,04	!IE-LOOP	ACN10GT001_____A	ACP-DG-------D-ALL	ACP__DG102_FLEX2___D	LOOP_DIESEL-REPAIR_H
4	4	5,51E-11	5,39	!IE-LOOP	ACN10GT001_____M	ACP-DG-------D-ALL	LOOP_DIESEL-REPAIR_H	SFPMU:2_DIAG_____H
5	5	4,32E-11	4,23	!IE-LOOP	ACN10GT001_____M	ACP-DG-------D-ALL	LOOP_DIESEL-REPAIR_H	SFPMU:2_P1_____A
6	6	4,25E-11	4,16	!IE-LOOP	ACN10GT001_____M	ACP-DG-------D-ALL	ACP__DG102_FLEX2___D	LOOP_DIESEL-REPAIR_H
518	7	2,07E-11	2,03	!IE-LOOP	ACN10GT001_____A	RPSXXPU00XSW1____YS	SFPMU:2_DIAG_____H	
7	9	1,39E-11	1,36E+00	!IE-LOOP	ACN10GT001_____A	ACP-DG-------A-ALL	LOOP_DIESEL-REPAIR_H	SFPMU:2_DIAG_____H

The first sequence starts with the initiating event loss of offsite power. This, in combination with the failure to start the gas turbine, will make the power rely on diesel generators. Then the diesel generators fail to operate with a CCF dependency. Here it is assumed that the process to repair the diesel generators will start (an alternative is to try to repair the gas turbine if it is equally hard or easier, but in the analysis this is mainly considered in the sensitivity analysis). When the water starts to boil the operators will have to try to start Make-up system 2 (since Make-up 1 is unavailable because of no power), and this will probably have non-optimal conditions (e.g. no indication, light etc.). The failure to diagnose the start will render the Spent fuel pool Make-up system 2 unavailable, but the repair of the diesel generator can continue

since it will return both the Spent fuel pool Cooling system and the Spent fuel pool Make-up system 1 available for operation.
The second and third sequence is similar to the first but with the diagnosis failure exchanged for failure of the pump or the diesel generator for the Spent fuel pool Make-up system 2. It would be possible to repair the pump or the diesel instead of an ordinary diesel generator, but this is not preferred if it can be avoided since the Spent fuel pool Make-up system 2 utilize sea water. Thus, the repair will be similar as in the first sequence. The fourth, fifth and sixth sequence is similar to the first, second and third but the failure mode of the gas turbine changes. Then sequences appear with failure to start diesel generator (with CCF-dependency) and also failure of the execution of the start of Spent fuel pool Make-up system 2.

SFP External event (Extreme snow) – Fuel damage

External extreme snow as the initiating event will cause loss of offsite power and the blocking of ventilation for the diesel generators and the sea water intake for cooling. It can occur with or without a warning before the initiating event and this will make recovery of the snow cleaning manual actions more or less likely to fail.
The assumptions of the external event will impact the analysis and the sequences. There are also many additional uncertainties related to external events. Firstly, the timing of the return of offsite power is highly uncertain. (it does not necessarily happen at the end of the external event). Secondly, the assumption of blocking of sea water inlet will contribute to uncertainty and it is also possible to consider a total collapse of the diesel ventilation building. The minimal cut sets consists of failure of manual actions to prevent the blocking of the ventilation building (which will fail the diesel generators) and the failure of the Spent fuel pool Make-up system 2. This can be seen in Table 33.

Table 33. Most contributing MCS for Heavy snow SFP before repair. HFEs are blue-marked and events (both independent and CCF) chosen for repair are yellow-marked. The "NEW" column is the MCS order number in the MCS list with repair events and the "No" column is the order number in this MCS list (before repair).

NEW	No	Probability	%	Initiating event	Event 1	Event 2	Event 3	Event 4	Event 5
1	1	8,15E-08	1,87E+01	!IE-E_SNOW	EXT_SNW_S_____H	PREWAR1_F_____	SFPMU:2_DIAG_____H		
2	2	7,33E-08	1,68E+01	!IE-E_SNOW	EXT_SNW_SR_____H	EXT_SNW_S_____H	PREWAR1_S_____	SFPMU:2_DIAG_____H	
5	3	6,39E-08	1,47E+01	!IE-E_SNOW	EXT_SNW_S_____H	PREWAR1_F_____	SFPMU:2_P1_____A		
9	4	6,29E-08	1,44E+01	!IE-E_SNOW	ACP__DG102_FLEX2___D	EXT_SNW_S_____H	PREWAR1_F_____		
6	5	5,75E-08	1,32E+01	!IE-E_SNOW	EXT_SNW_SR_____H	EXT_SNW_S_____H	PREWAR1_S_____	SFPMU:2_P1_____A	
3	7	8,10E-09	1,86E+00	!IE-E_SNOW	EXT_SNW_S_____H	PREWAR1_F_____	SFPMU:2_MANSTART___H		
4	9	7,29E-09	1,67E+00	!IE-E_SNOW	EXT_SNW_SR_____H	EXT_SNW_S_____H	PREWAR1_S_____	SFPMU:2_MANSTART___H	

The repair is inserted in the MCS-list as in Table 34.

Table 34. Most contributing MCS for Heavy snow SFP after repair. HFEs are blue-marked and events (both independent and CCF) chosen for repair are yellow-marked. The "OLD" column is the MCS order number in the MCS list without repair events and the "No" column is the order number in this MCS list (considering repair).

OLD	No	Probability	%	Event	Event 1	Event 2	Event 3	Event 4	Event 5
1	1	8,15E-08	4,45E+01	!IE-E_SNOW	EXT_SNW_S_____H	PREWAR1_F_____	SFPMU:2_DIAG_____H		
2	2	7,33E-08	4,01E+01	!IE-E_SNOW	EXT_SNW_SR_____H	EXT_SNW_S_____H	PREWAR1_S_____	SFPMU:2_DIAG_____H	
7	3	8,1E-09	4,43E+00	!IE-E_SNOW	EXT_SNW_S_____H	PREWAR1_F_____	SFPMU:2_MANSTART___H		
9	4	7,29E-09	3,98E+00	!IE-E_SNOW	EXT_SNW_SR_____H	EXT_SNW_S_____H	PREWAR1_S_____	SFPMU:2_MANSTART___H	
3	5	4,03E-09	2,20E+00	!IE-E_SNOW	EXT_PUMP-REPAIR____H	EXT_SNW_S_____H	PREWAR1_F_____	SFPMU:2_P1_____A	
5	6	3,63E-09	1,98E+00	!IE-E_SNOW	EXT_PUMP-REPAIR____H	EXT_SNW_SR_____H	EXT_SNW_S_____H	PREWAR1_S_____	SFPMU:2_P1_____A
4	9	2,5E-10	1,37E-01	!IE-E_SNOW	ACP__DG102_FLEX2___D	EXT_DIESEL-REPAIR__H	EXT_SNW_S_____H	PREWAR1_F_____	

The first MCS is the initiating event in combination with no initial warning and failure of initial manual actions (snow cleaning). This will initiate the heating of water since the diesel generators will fail. With the start of boiling a failure to diagnose the start of the Spent fuel pool Make-up system 2 will lead to uncovered fuel and fuel damage. The repair in this case is not possible since only HFEs appear. However, it is possible to consider other types of repair and recovery (in combination with a probability to recover offsite power) to increase the level of detail in the analysis. The analysis could also consider the usage of diesel generators for some limited duration (or perhaps run a diesel generator to failure/heat protection stop) and thus buy more time in the sequence. These are indicators that the analysis for the external event is conservative, but it will show the principle of considering repair in these sequences.
The next minimal cut set considered is similar to the first but with a successful warning and that makes recovery on the initial manual actions possible. The third and fourth MCS is similar to the first but with failure of the pump and diesel generator for the Make-up 2 pump. These are the sequences that are considered repairable with corresponding repair events added (comparison between Table 33 and Table 34).

Investigation of the feed and boil/steaming end state
Repairing from the feed and boil state is required to reach the safe state in most cases. As can be seen in Figure 36 this state has two input states and is triggered by the loss of the cooling system (the sequences that end in the Feed and Boil consequence) and the states that come by the repair from the Boil state, which is investigated in section 0. The input from the first case can be seen in Table 35 (here the FAB2 case is show which is a more restrictive case with only Make-up system 2 working).

Table 35. Frequencies for the feed and boil state.

IE	EX SNW	LOOP	TRANS
IE-freq [1/y]	1,00E-04	1,00E-01	1
No repair freq (fab)	3,13E-06	2,75E-06	1,06E-04
No repair freq (fab2)	3,13E-06	1,68E-06	4,53E-07

The FAB case has more input states, long time windows and perhaps greater uncertainty about what actions to consider. Therefore, the quantification is perhaps more difficult. Since accident scenario is a stochastic process, Markov analysis could be used in the MCS-quantification to reduce simplifications. The Markov property states that the stochastic process must be "memoryless", that is the future states of the system only depends on the current states and not the previous ones. In general, this is not fulfilled for nuclear accident because the residual heat will decrease over time, increasing awareness of personnel further on in the event, or perhaps the failure data is best described with non-constant failure rates for safety systems. Markov analysis might however still be feasible and yield some insight for the Enhanced Fault/Event Tree method.

Consider the Markov transition matrix in Table 36. The Start column describes the initial state and the Target Row describes the state that is reached for each Markov iteration. The repair failure probability (6.30E-2) of Make-up system 1 and the repair failure probability of the cooling system with long time windows (8.09E-5) have been used. Other values have been estimated more loosely and should be taken as assumptions for the investigation with large uncertainties.

Table 36. Markov transition matrix for the spent fuel pool.

Start

	SaSS	BB	FAB	B	FD
SaSS	9,99E-01	1,00E-03	0,00E+00	0,00E+00	0,00E+00
BB	3,76E-01	0,00E+00	5,74E-01	5,00E-02	0,00E+00
FAB	9,99E-01	0,00E+00	0,00E+00	8,09E-05	0,00E+00
B	0,00E+00	0,00E+00	9,37E-01	0,00E+00	6,30E-02
FD	0,00E+00	0,00E+00	0,00E+00	0,00E+00	1,00E+00

Running the Markov analysis with this Markov transition matrix yields the result that is shown in Figure 38 for initial states of Feed and Boil (FAB) and Boil (B).

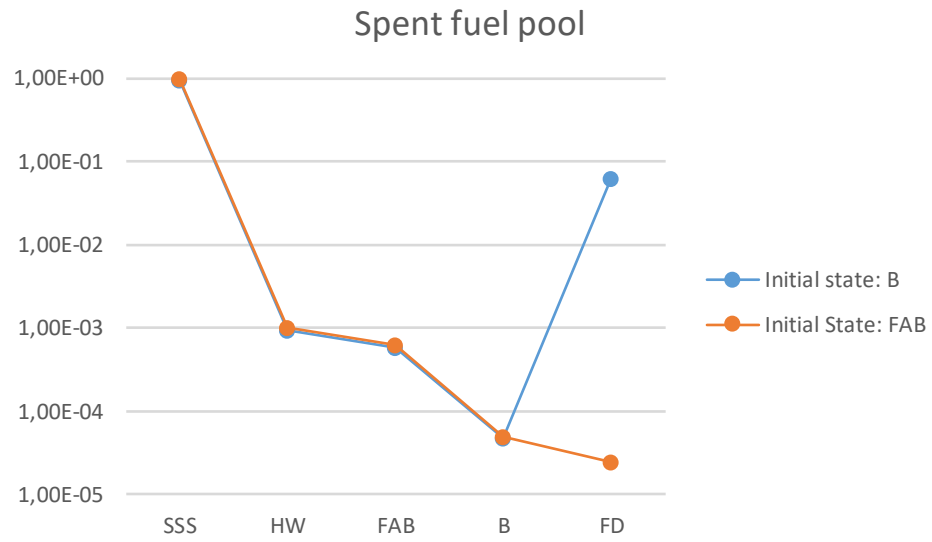

Figure 38. Results from Markov analysis.

When the initial state is Boil (B) the chains that end up in the Fuel Damage (FD) state is approximately the same as the repair failure probability for the Make-up system 1. When the initial state is Feed and Boil (FAB) the chains that end up in the Fuel Damage (FD) state is 2.40E-5 after 10 Markov iterations. The latter will probably increase some due to it not stabilizing fully.

6.2.4 Pilot Study – PROSAFE CORE model

The core model is the DIGREL model (Authén et al., 2015) modified with two extra function events, U2 independent core cooling and W2 residual heat removal. In PROSAFE this is only considered for the external event (heavy snow). Figure 39 show the extreme snow core model event tree.

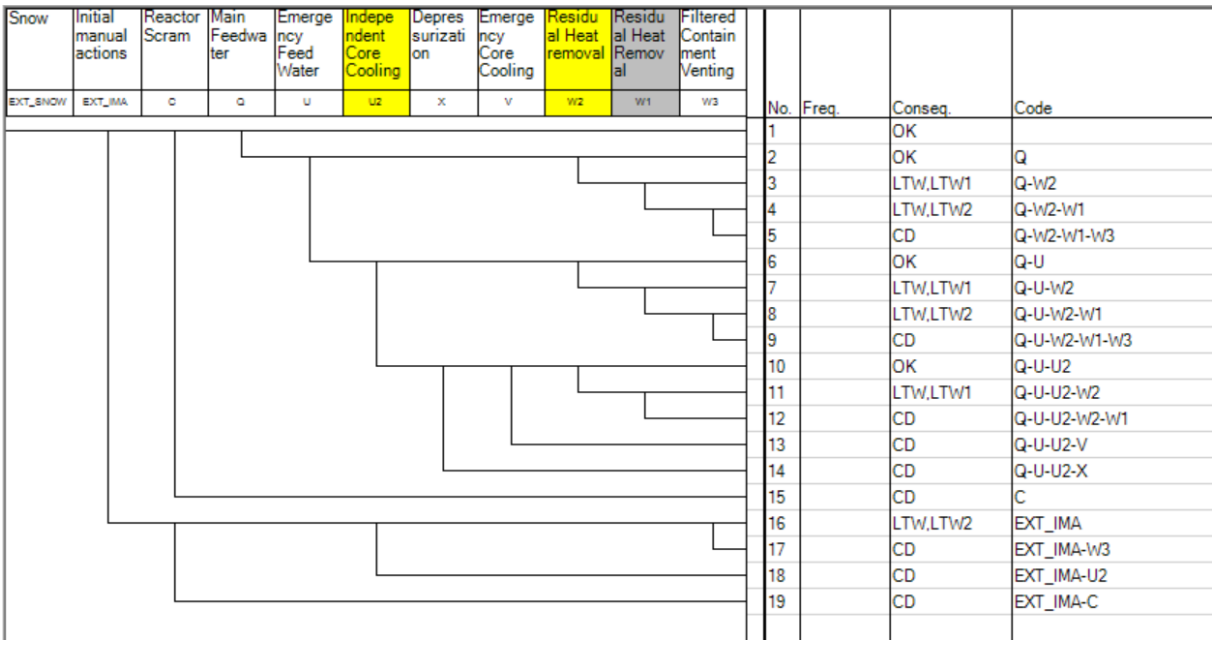

Figure 39. Core model event tree

For the Core case the decrease is not as large as for the spent fuel pool case and the initiating event can be seen in Table 37. The sensitivity analysis (with a factor of 2) is also shown.

Table 37. Results core model.

IE	**EX SNW**
IE-freq [1/y]	1,00E-04
No repair	2,04E-07
With repair	1,54E-07
	-25%
Repair sensh 2	1,76E-07
	-14%
Repair sensl 2	1,44E-07
	-29%

The core external event is the same as the external event for the spent fuel pool but applied to the core model. The initiating event is the external extreme snow event which will cause loss of offsite power and blocking of the ventilation for the diesel generators and the sea water intake for cooling. It can occur with or without a warning before the initiating event and this will make recovery of the snow cleaning manual actions more or less likely to fail. Here the assumptions of the external event will impact the analysis and the sequences. First there is probably a high uncertainty of the return of offsite power and when that could occur (since it does not necessarily happen at the end of the external event). Second, the assumption of blocking of sea water inlet will contribute to uncertainty. Third, it is possible to consider the total collapse of the diesel ventilation building. Here the time window modelling of the independent core cooling is present where during the initial time window of 12 hours the system is considered non-repairable and during the time window 12-24 hours the system is considered repairable. This can be seen in Table 38.

Table 38. Most contributing MCS for Heavy snow core model before repair. HFEs are blue-marked and events (both independent and CCF) chosen for repair are yellow-marked. The "NEW" column is the MCS order number in the MCS list with repair events and the "No" column is the order number in this MCS list (before repair).

NEW	No	Probability	%	Initiating event	Event 1	Event 2	Event 3	Event 4	Event 5
1	1	3,18E-08	1,56E+01	!IE-E_SNOW	EXT_SNW_S_____H	ICC10DG001__0-12H__D	PREWAR1_F_____		
5	2	3,18E-08	1,56E+01	!IE-E_SNOW	EXT_SNW_S_____H	ICC10DG001_12-24H__D	PREWAR1_F_____		
2	3	2,86E-08	1,40E+01	!IE-E_SNOW	EXT_SNW_SR_____H	EXT_SNW_S_____H	ICC10DG001__0-12H__D	PREWAR1_S_____	
6	4	2,86E-08	1,40E+01	!IE-E_SNOW	EXT_SNW_SR_____H	EXT_SNW_S_____H	ICC10DG001_12-24H__D	PREWAR1_S_____	
3	5	1,78E-08	8,74E+00	!IE-E_SNOW	EXT_SNW_S_____H	FCV10VS001_____Y	PREWAR1_F_____		
4	6	1,60E-08	7,87E+00	!IE-E_SNOW	EXT_SNW_SR_____H	EXT_SNW_S_____H	FCV10VS001_____Y	PREWAR1_S_____	

The first sequence is the initiating event in combination with a failure to receive initial warning. Then the independent core cooling fails to run within the time window 0-12 hours. This cutset is deemed non-repairable because the available time does not allow repair of the independent core cooling system (or any system that does not have a low MTTR). The second cutset is the same as the first but the failure of the ICC is deemed repairable. The fourth and fifth cutset is the same as the first two but with some warning of the initiating event and thus more time for manual actions. These cutsets that are set in a repairable time window appear lower in the MCS-list as can be seen in Table 39.

Table 39. Most contributing MCS for Heavy snow core model after repair. HFEs are blue-marked and events (both independent and CCF) chosen for repair are yellow-marked. The "OLD" column is the MCS order number in the MCS list without repair events and the "No" column is the order number in this MCS list (considering repair).

OLD	No	Probability	%	Initiating event	Event 1	Event 2	Event 3	Event 4	Event 5
1	1	3,18E-08	2,06E+01	!IE-E_SNOW	EXT_SNW_S_____H	ICC10DG001__0-12H__D	PREWAR1_F_____		
3	2	2,86E-08	1,85E+01	!IE-E_SNOW	EXT_SNW_SR_____H	EXT_SNW_S_____H	ICC10DG001__0-12H__D	PREWAR1_S_____	
5	3	1,78E-08	1,16E+01	!IE-E_SNOW	EXT_SNW_S_____H	FCV10VS001_____Y	PREWAR1_F_____		
6	4	1,6E-08	1,04E+01	!IE-E_SNOW	EXT_SNW_SR_____H	EXT_SNW_S_____H	FCV10VS001_____Y	PREWAR1_S_____	
2	5	9,53E-09	6,18E+00	!IE-E_SNOW	EXT_SNW_S_____H	ICC10DG001_12-24H__D	ICC_DG-REPAIR_____H	PREWAR1_F_____	
4	6	8,58E-09	5,56E+00	!IE-E_SNOW	EXT_SNW_SR_____H	EXT_SNW_S_____H	ICC10DG001_12-24H__D	ICC_DG-REPAIR_____H	PREWAR1_S_____

Repair from containment venting state

The containment venting state could be considered one of the semi stable states and could be investigated with Markov analysis similar to the feed and boil state. In this pilot study the core event considered is the external event and depending on assumptions there will be different ways to return to the safe and stable state given that the containment venting state is reached successfully. Table 40 gives some suggestion of the different possible repairs/recoveries whether the diesel building is collapsed or not. Other assumptions can impact as well.

Table 40. Assumptions for external events.

Assumption	Fail sequence (without repair)	Semi stable state (containment venting)
Collapse of diesel building	Repair of ICC	Mobile diesel generators, recover offsite power
Blocking of ventilation	Repair of ICC or recovery of snow clearing	Recovery of snow clearing

6.2.5 Pilot Study – Full scale SFP model

A limited study is performed on a full scale PSA SFP model. The initiating event LOOP and consequences FAB and FD are studied.

The time windows are assumed to be the same as for the pilot study in the PROSAFE model:

- 24 hours from the initiating event until boiling of the spent fuel pool
- 72 hours from boiling until fuel damage

These time windows were modelled in the same manner as for the PROSAFE model pilot study.

As previously described, the method starts by identifying the most relevant repairable events by investigating the importance list (fractional contribution). This means that the selected repairs generally differ according to chosen consequences to analyse. In the pilot study, two analyses per consequence have been performed. That is, results have been calculated for both one and two repairs, see Table 41.

Table 41. Credited repairs for different consequences

Analysed consequence	**One credited repair**	**Two credited repairs**
LOOP ST (steaming)	Pump	Pump and Diesel
LOOP FD (fuel damage)	Diesel	Diesel and Battery

Diesel generator breaker failures are included in the diesel failure repair.

The same sequence MTTR parameters as in the PROSAFE model pilot study were used for the corresponding components, see Table 42.

Table 42. MTTR parameters and values

Parameter	**Value**	**Model**
LOOP_BATTER_REPAIR_H	3,98E-03	Probability
PFD_BATTER-REPAIR_H	3,98E-03	Probability
PFD_DIESEL-REPAIR_H	3,98E-03	Probability
PST_DIESEL-REPAIR_H	1,94E-01	Probability
PST_PUMP-REPAIR____H	6,24E-01	Probability

After applying EFET and taking repair and time windows into account the frequency decreased with 45 % for consequence boiling and 96 % for consequence fuel damage, Table 43. Note that the difference between taking one and two repairs into account is quite large for both consequences which indicates the importance of making at least two iterations.

Table 43. Results using EFET on a full scale PSA model

Initiating Event	**Enhanced fault/event tree**				
	Static	**EFET R**	**EFET R2**	**DIFF R**	**DIFF 2R**
LOOP (PST)	1,0E-05	7,9E-06	5,5E-06	-21%	-45%
LOOP (PFD)	1,6E-06	1,4E-07	5,8E-08	-91%	-96%

6.2.6 Discussion

Uncertainties
Uncertainties in the method could be considered by ordinary means of uncertainty analysis. Parametric uncertainty (e.g., MTTR) can be considered by Monte Carlo simulation if a built-in post processing tool is used for quantification. Model uncertainties (e.g., the time window modelling) and completeness uncertainties (e.g., HFEs) could be handled as in regular PSA (identification, quantification etc.). Some more general discussion of these uncertainties in relation to long time windows can be found in section 0.

Conclusions
The enhanced fault/event tree method offers a simple method for modelling non static behaviour with static fault tree/event tree tools and minimizing need for additional software. It is based on a graded approach that can be tailored to the need for additional accuracy and perhaps restrictions in work resources. It enables a simplified representation of dynamic behaviour by considering the repair probability of cutsets, and is useful in both small and large existing PSA models.

The impact of repair is considerable and must be taken into consideration for long time windows, e.g. for events related to the spent fuel pool. It is also evident that it could be useful to model repair in modelling of the reactor core. The method does not require repair of the initiating event to reach safe and stable state and it is therefore able to use the definition as in the original PSA-study (or others if needed). Results also indicate that repair of a make-up system is most important.

All failures and repairs are modelled with a non-dynamic approach and can be considered to occur immediately after the IE. The available time for repair impacts the repair probabilities and decides in which time window it is possible to repair. The mission time is not dynamic and components cannot fail after they have been repaired (but calculations outside the method could handle this). The repairs that are included in the analysis could be considered to occur in parallel, if the quantification does not adjust the available time (that is to consider a lower available time for the second repair).

The method is easy to apply to an existing PSA model and uses a safety graded approach. The complexity can be considered low since it is fitted within the scope of the regular analysis with some extra work. The requirement to perform the analysis with the method is basic PSA competence, and no additional software is needed. The conclusions that could be drawn from the PROSAFE model pilot study is verified by the application on a full scale model.

6.3. Simulation-based event trees

6.3.1 Overview

PSA software FinPSA (VTT, 2020) includes a module for simulation-based event trees (Tyrväinen et al., 2016; Tyrväinen & Karanta, 2019). The module has been developed for level 2 PSA (containment event trees), but it is, in practise, a general-purpose probabilistic risk analysis tool. The module combines event trees with computation scripts written using FinPSA's own programming language, containment event tree language (CETL). In the script files, the user defines functions that calculate probabilities of event tree branches and possibly other variable values, such as magnitudes of consequences or timings of events. The script files enable use of various modelling approaches because contents of the scripts are not limited in any way, except that they must conform the CETL syntax.

The model includes a separate script file for each event tree section, for an initial section, and for a common section, which is common to all event trees in the project if there are multiple event trees. A function name is assigned to each event tree branch, and the function has to be defined in the script file of the corresponding event tree section. The function returns the probability of the event tree branch. It is also possible to write other functions that are called e.g. by branch functions. The model can include both global variables and local variables limited for a specific event tree section. Values of global variables can be chronologically updated when moving forward in an event tree sequence and can be utilised in the computation of event tree branch probabilities. For example, a time variable or a physical parameter, such as temperature, can be updated this way according to the events that occur during the sequence. Types of variables are ordinary data types, such as 'real', 'integer', 'Boolean' and 'string'. Probability distributions of a few different types can also be specified. A set of built-in functions is available, including some probability distribution operations.

To account for uncertainties related to variable values, it is possible to specify probability distributions for parameters and perform Monte Carlo simulations. At each simulation cycle, a value is sampled from each specified distribution, and based on that, numerical conditional probabilities are calculated for all event tree branches, and values are calculated for all variables at each end point of the event tree. After the simulations, statistical analyses are performed to calculate frequency and variable value distributions for each end point among other statistical results and correlation analyses. It is also possible just to calculate point values of the event tree based on the mean values of distributions. Event tree sequences can also be grouped by a binner routine, and combined results can be calculated for the specified consequence categories.

The simulation-based event trees of FinPSA provide only the frame for modelling. The tool can be used in many ways, and it is up to the user to select or develop the actual modelling approach for the application.

6.3.2 Modelling approach for spent fuel pool

The modelling approach selected here for spent fuel pool analysis integrates deterministic spent fuel pool behaviour and probabilistic analysis. The spent fuel pool water level and temperature are calculated in the simulations at every time point of interest, e.g. when a make-up system is started or fails. The time windows for probabilistic analysis are dynamically calculated based on the current spent fuel pool conditions. For example, the mission time of a make-up system is calculated based on how long it takes to reach the safe state, i.e. the water level is normal and the spent fuel pool cooling system is back in operation. Similarly, the time available to start a

make-up system is calculated based on how long it takes until the water level has decreased to the fuel level.

In the simulations, durations of manual actions are drawn from specified probability distributions to determine e.g. when a make-up system is started or when the spent fuel pool cooling system is repaired. Failure times of components are also drawn from uniform distributions covering the mission times of the components.[1]

Even with the abovementioned specifications, the model could be constructed in several different ways and with different scopes. Here, we want to have a correspondence between the static PSA model and the dynamic model, because it is convenient for the comparison of results, and modelling all possible failure combinations using the dynamic approach would make the model unnecessarily complex. We concentrate the dynamic analysis on the most important minimal cut sets of the static model, and construct the simulation-based event tree so that each of the top minimal cut sets of the static model corresponds to a sequence of the simulation-based event tree. Therefore, the branches of the simulation-based event tree correspond to basic events of the static model. For example, the event tree for loss of offsite power is presented in Figure 40. The idea is that the results of the simulations can be used to update the frequencies of the minimal cut sets of the static model to calculate the fuel damage frequency more realistically.

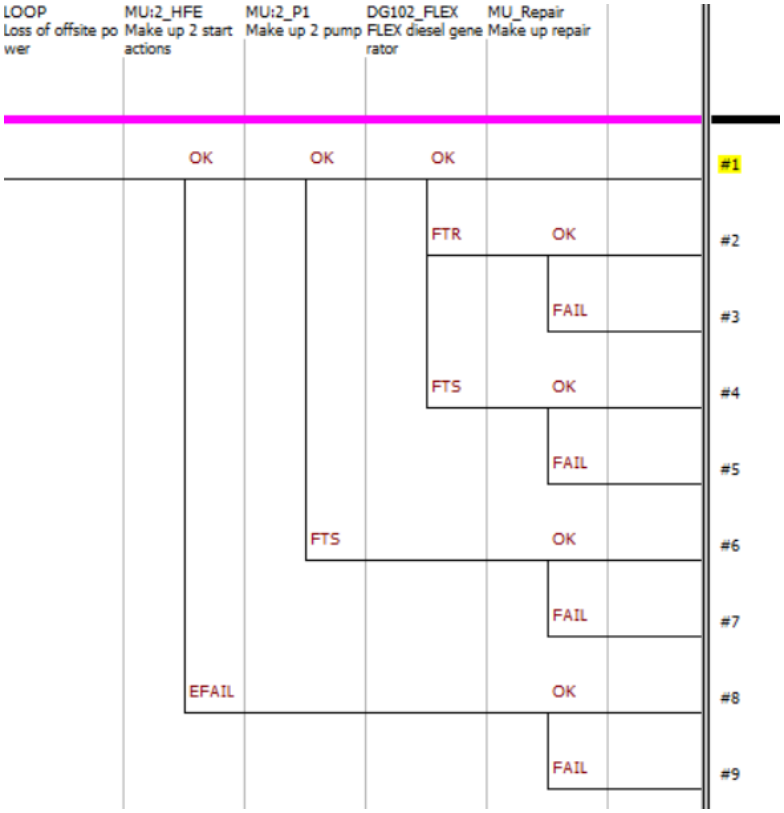

Figure 40. Simulation-based event tree for loss of offsite power.

The computation scripts related to the event tree are presented in Appendix B. Here, we present a few illustrative examples. For example, function OK in the MU:2_HFE section is defined in the following way:

[1] Failure times are in reality exponentially distributed (or can be assumed to be), but with a small failure rate, the uniform distribution gives a good approximation for failures occurring during mission time.

```
$ Make up 2 start is performed successfully
function nil OK
  $ Time available to start make up system 2.
  t_avail = (WLevel-FuelLevel)/BoilingRate

  $ The execution time of the make up system 2 start is drawn from uniform distribution.
  t_exe = 2*r2+1

  $ The diagnosis time of the make up system 2 start is drawn from lognormal distribution.
  r = r*cumul(MU2D,t_avail-t_exe)
  t_diag = icumul(MU2D,r)

  $ The start time of make up system 2.
  t_start2 = t_diag+t_exe

  $ The spent fuel pool water level is updated.
  WLevel = WLevel-t_start2*BoilingRate
return nil
```

This function determines the start time of make-up system 2, and updates the spent fuel pool water level and temperature based on how long the manual actions to start the system last. It is a nil function, which means that the probability of the corresponding event tree branch is calculated as the complement of the probability of the other branch.

The models for water level and temperature used here are only very simple models mimicking the time-dependent behaviour of those variables. For example, the temperature is assumed to increase linearly when there is no water injection before boiling. The water level is assumed to decrease linearly during boiling and increase linearly during make-up water injection. The temperature decrease rate during water injection depends on the difference between the pool temperature and the coolant temperature. For example, Figures 41 and 42 present the temperature and water level behaviour in a case where the spent fuel pool cooling is lost until a make-up system is started at time point 50 h. Despite of the simplicity of these assumptions, the behaviour is quite similar to some deterministic analysis results found from literature (Ramadan et al., 2018; Tynys, 2017; Wu et al. 2014; Zhang et al. 2017). Therefore, it is assumed that the impact of the simplifications on the results is not very large. Anyhow, integration of more realistic deterministic models to the analysis is one future development topic.

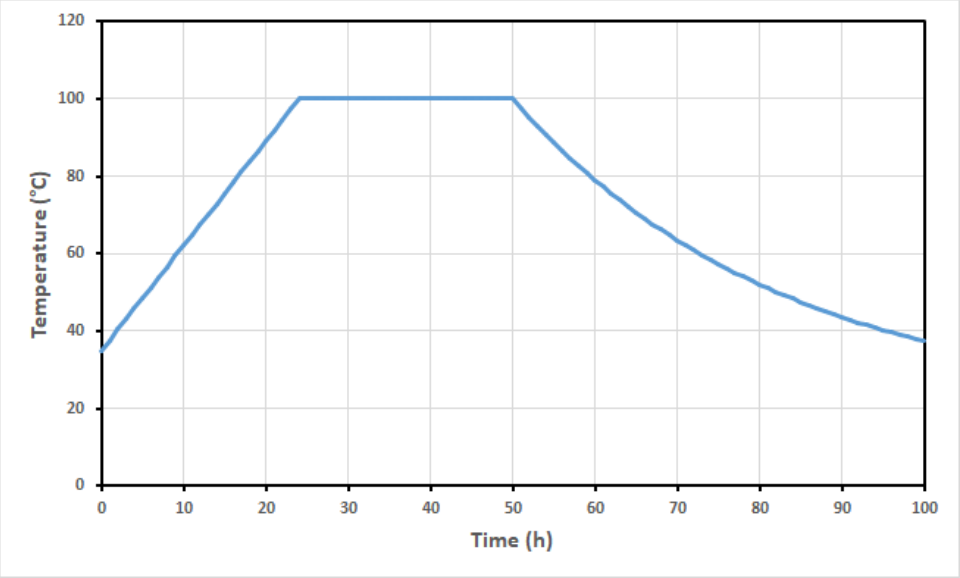

Figure 41. Spent fuel pool temperature as a function of time if a make-up system is started at time point 50 h.

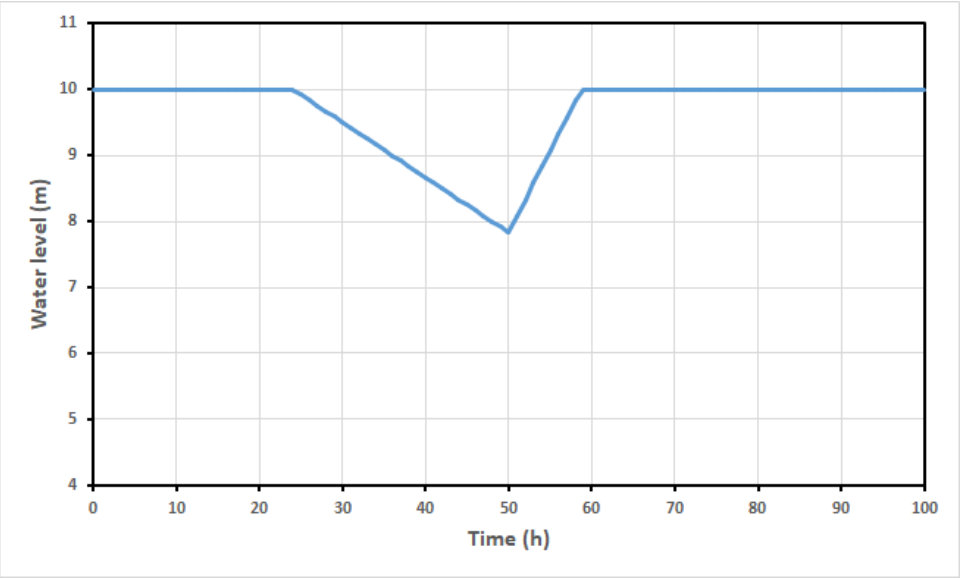

Figure 42. Spent fuel pool water level as a function of time if a make-up system is started at time point 50 h.

The failure to run probability of a diesel generator, which serves make-up system 2, is calculated by the following function:

```
function real FTR
  fr = FR_DG   $ Failure rate

  $ The mission time is tentatively calculated as the time to reach normal water level.
  t_mission2 = (InitWLevel-WLevel)/LevelIncRate

  $ Given the repair time of the spent fuel pool cooling system,
  $ the earliest allowed failure time is calculated.
  $ The EarliestTime function is defined in the common section.
  t_earliest = EarliestTime(Temperature,t_repair-t_start2)

  $ If the earliest allowed failure time based on the repair of the spent fuel pool cooling
  $ system is larger than the time to reach the normal water level, the mission time is
  $ determined based on that.
  if t_mission2 < t_earliest then t_mission2 = t_earliest

  $ The diesel generator failure probability is calculated.
  prob = 1-exp(-fr*t_mission2)

  $ The failure time of the diesel generator is determined.
  t_fail2 = t_mission2*r

  $ The spent fuel pool conditions are updated based on the failure time.
  $ The Cooldown function is defined in the common section.
  Temperature = Cooldown(Temperature,t_fail2)
  WLevel = WLevel+LevelIncRate*t_fail2
  if WLevel > InitWLevel then WLevel = InitWLevel

  $ The total time the make up 2 system was used.
  t_mu2 = t_start2+t_fail2

  $ Mean time to repair for repair modelling of this diesel generator.
  mttr1 = MTTR_DG_FTR
return prob
```

The function determines the mission time for the diesel generator based on the time to reach normal water level and repair time of the spent fuel pool cooling system. The diesel generator is allowed to fail some time before the repair of the spent fuel pool cooling system as long as the boiling does not start again before the repair. The earliest allowed failure time is calculated using the EarliestTime function, which can be found from Appendix B. A failure time is also drawn for the diesel generator on each simulation cycle, and the water level and temperature

are updated taking into account how long make-up system 2 operated. These water level and temperature conditions affect later in the analysis the probability to repair the diesel generator.

On each simulation cycle, a conditional probability for each sequence of the event tree is calculated given specific human action, failure and repair timings. Then, average probabilities are calculated for the sequences over the simulation cycles. These average probabilities are not conditional to specific timings, but reflect complete probability distributions of different timing variables. The accuracy of these probabilities depends on the number of simulation cycles, which should be sufficiently large.

6.3.3 Pilot study

6.3.3.1 Model and assumptions

This analysis covers the transient and LOOP scenarios of the PROSAFE spent fuel pool model. The simulation-based analysis is here connected to the minimal cut sets produced by the static PSA model. The simulation-based event trees are constructed so that their sequences correspond to the minimal cut sets of the static model. This way the results of the dynamic analysis can be incorporated to the minimal cut set lists. The simulation-based event tree for the spent fuel pool transient is presented in Figure 43 and for loss of offsite power in Figure 40. The event trees cover 32 most important minimal cut sets (as well as many other minimal cut sets), except those that include diagnosis failures of the make-up systems. The diagnosis failures are left out of the model, because the probabilities calculated for the static model are considered sufficient, and it would be challenging to find assumptions to model the dependency between diagnosis failures in a dynamic manner. The scripts related to the event trees are presented in Appendix B.

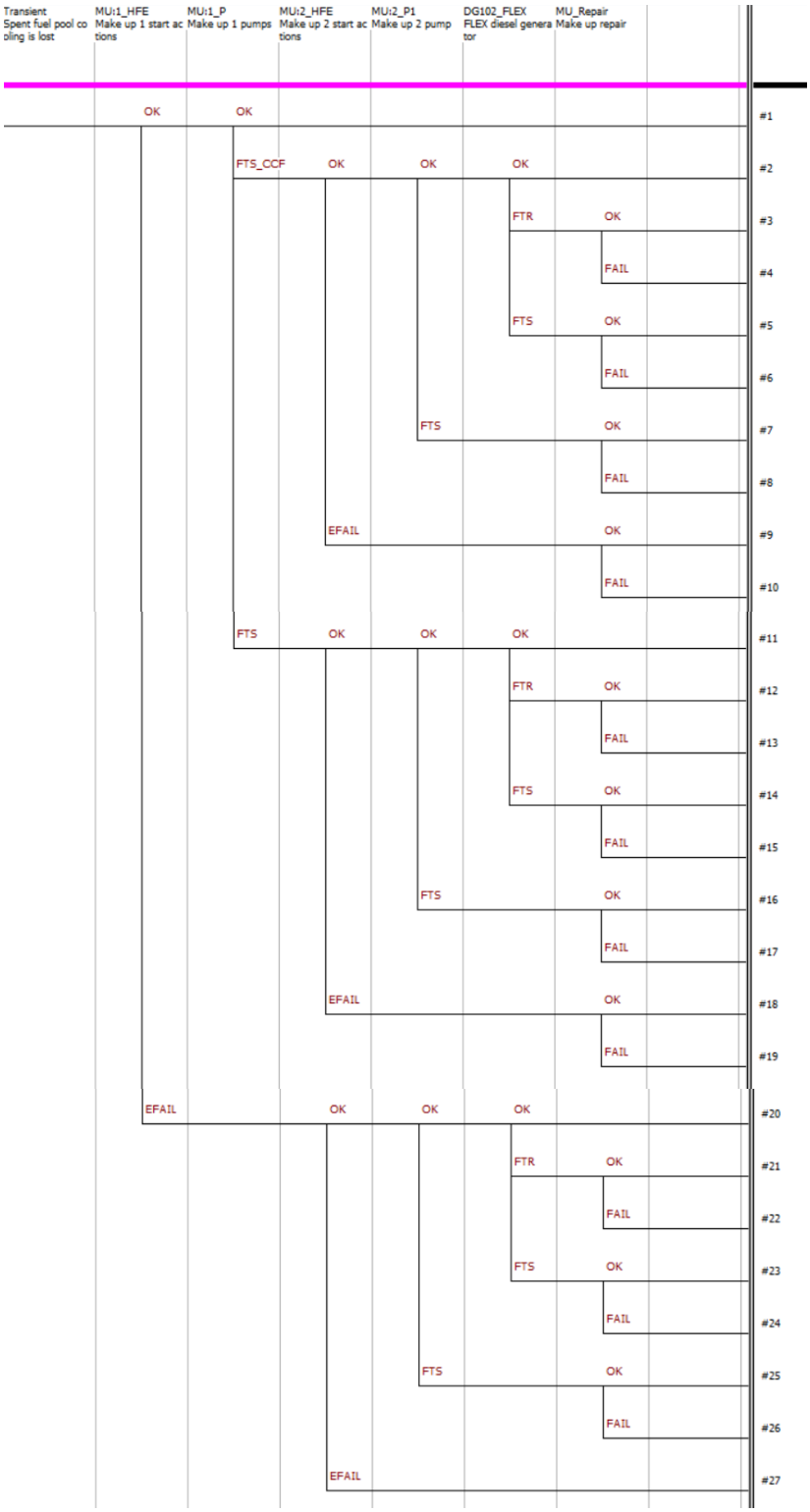

Figure 43. Simulation-based event tree for spent fuel pool transient.

The simulation models focus on the make-up systems and do not analyse spent fuel pool cooling system failures. For the spent fuel pool cooling system failures, the probabilities produced by the static model are used. The results of the simulations are conditional fuel damage probabilities given the failure of the spent fuel pool cooling system. The simulation of spent fuel pool conditions practically starts from the start of boiling. It is assumed that actions to start the make-up systems begin when the boiling starts.

Loss of offsite power and transient scenarios are partly different, and there are significant differences in their modelling. The power supply of make-up system 1 comes from the same source as for trains 3 and 4 of the spent fuel pool cooling system. This means that if the power supply for the spent fuel pool cooling system fails, make-up system 1 is also unavailable. Therefore, the focus is more on the modelling of make-up system 2 in the loss of offsite power case. If make-up system 2 fails and the spent fuel pool is boiling, it is either possible to repair make-up system 2 or repair the power supply (diesel generator) of make-up system 1. Repair of the power supply of make-up system 1 is a better option, because the power supply is also needed to restore the spent fuel pool cooling after the water level has been increased back to normal. Therefore, repair of the power supply of make-up system 1 is modelled primarily. However, if that repair takes too long time, the possibility to repair make-up system 2 in order to buy more time is modelled (only in that case). If make-up system 1 fails after the repair before the normal water level has been reached, it can still be repaired. If the second repair takes too long or the system fails after the repair, fuel damage is assumed. When the normal water level has been reached, the safe state is assumed, because operation with the spent fuel pool cooling system can be started. The modelling of all repairs is performed in the scripts of the last event tree section.

In the transient case, it is assumed that make-up system 1 is started first after boiling. If it fails, make-up system 2 is started. If it also fails, repair of either make-up system 1 or 2 is started depending on how make-up system 1 failed. If the repair is successful, but the system fails again, another repair of either make-up system 1 or 2 is modelled, but if it fails or the system fails after that, fuel damage is assumed. The modelling of both repairs is performed in the scripts of the last event tree section, i.e. the failure branch represents the failure of either of the repairs.

The simulations require probability distributions for the durations of human actions, which are information not generally available and not used by other methods presented here. For diagnosis actions, a lognormal distribution is assumed with a mean of two hours. The error factor for a diagnosis action is estimated based on HRA results (see Section 5.2.1.11) so that the probability to exceed the available time used in HRA is the HEP estimated in HRA. This way the distributions are in line with HRA results. The distributions are presented in Table 44. For start executions of the make-up systems, uniform distributions are used and the durations are assumed quite short, regardless if the actions are successful or not. Repairs are modelled using exponential distributions with the same MTTR values as used in I&AB analysis (Table 14). It would also be possible to model the diagnosis and execution for repair separately, and e.g. use lognormal distribution for diagnosis, but we want to use the same assumptions in different methods as much as possible.

Table 44. Probability distributions for the durations of human actions.

Action	**Distribution**	**Parameters**
MU:1 start diagnosis	Lognormal	Mean = 2 h, Error factor = 7.02
MU:1 start execution	Uniform	Min = 0.5 h, Max = 1.5 h
MU:2 start diagnosis	Lognormal	Mean = 2 h, Error factor = 8.29
MU:2 start execution	Uniform	Min = 1 h, Max = 3 h

The repair of the spent fuel pool cooling system or its power supply is assumed to start when the cooling is lost. Possibility to repair the cooling before boiling is modelled simply by

calculating the probability that the repair time exceeds the time to boiling. If the repair is successful before boiling, the safe state is reached directly. The repair time of the spent fuel pool cooling depends on the component(s) that fails and the failure mode. In the transient case, either the pump or the heat exchanger can fail. In the loss of offsite power case, it is assumed that diesel generator 3 or 4 (which supplies make-up system 1) is always repaired. The simulations are performed separately for different spent fuel pool cooling failure modes, because the MTTR parameter used in the simulations depends on how the cooling fails.

In the make-up system repair modelling, not only failure to repair is modelled, but also the possibility of another failure after the repair. The repaired system must start successfully and operate long enough so that the safe state is reached. It is taken into account that any component of the system can fail, not only the one that was repaired.

The time windows for human actions and operation of make-up systems are calculated based on the spent fuel pool conditions and vary dynamically based on timings of different events. The parameters used in the computation of the spent fuel pool water level and temperature have been selected so that the time windows are those that were selected for the benchmark study (Section 6.4.1). The temperature increase rate is such that the time to boiling from the normal temperature is 24 hours. The water level decrease rate is such that the time to fuel damage (water surface at fuel level) from the normal water level is 72 hours (from the start of boiling). The water level increase rate is such that the time from the fuel level to the normal level is 24 hours when a make-up system is working.

6.3.3.2 Results

Dynamic re-quantification is performed here for the most important minimal cut sets of the static model for the loss of offsite power and transient scenarios. The minimal cut sets are listed in Appendix A. A sequence in the dynamic model can be correspond to multiple minimal cut sets, because some minimal cut sets include the same make-up system failures.

The dynamic models were simulated 100000 times for each initiating event. For each sequence of the simulation-based event tree, a conditional fuel damage probability given the failure of the spent fuel pool cooling system was calculated over the simulations. Then, these probabilities were used to update the frequencies of the minimal cut sets of the static model.

Table 45 and Table 46 present the total results and results for the ten most important minimal cut sets. Complete lists of the analysed MCSs are presented in Appendix A. ‘Seq’ column indicates the corresponding sequence in the simulation-based event tree. ‘IE MTTR’ column indicated the mean time to repair the spent fuel pool cooling (even though in the LOOP case it is not exactly the initiating event that is repaired). The static frequency is the frequency calculated from the static model, and the dynamic frequencies are calculated based on the dynamic analysis. The dynamic frequencies are obtained by replacing the make-up system failure probabilities in the minimal cut sets by the corresponding simulation results. For transient, dynamic results are presented without considering repairs of the make-up systems (NR), with one make-up system repair (1R) and with two make-up system repairs (2R). For loss of offsite power, dynamic results are presented without considering repair of make-up system 1 (NR) and with a repair of make-up system 1 (R).

Table 45. Results for top minimal cut sets of the transient scenario.

MCS	Seq	IE MTTR (hour)	Static Freq (1/year)	Dynamic Freq NR (1/year)	Dynamic Freq 1R (1/year)	Dynamic Freq 2R (1/year)
Total			3.95E-8	1.50E-8	1.42E-9	8.83E-10
1	8	32	3.73E-9	1.75E-9	1.38E-10	8.23E-11
2	4	32	3.67E-9	1.21E-9	6.86E-11	2.66E-11
3	8	32	3.36E-9	1.58E-9	1.24E-10	7.42E-11
4	4	32	3.31E-9	1.09E-9	6.19E-11	2.40E-11
5	17	32	2.47E-9	1.16E-9	9.08E-11	5.32E-11
6	13	32	2.43E-9	8.02E-10	4.52E-11	1.68E-11
7	17	32	2.23E-9	1.05E-9	8.19E-11	4.80E-11
8	13	32	2.19E-9	7.23E-10	4.08E-11	1.51E-11
9	8	32	1.51E-9	7.10E-10	5.58E-11	3.33E-11
10	4	32	1.49E-9	4.92E-10	2.78E-11	1.08E-11

Table 46. Results for top minimal cut sets of the loss of offsite power scenario.

MCS	Seq	IE MTTR (hour)	Static Freq (1/year)	Dynamic Freq NR (1/year)	Dynamic Freq R (1/year)
Total			1.14E-7	7.99E-10	1.11E-10
1	7	15	2.36E-8	2.52E-10	3.39E-11
2	3	15	2.32E-8	7.29E-11	9.15E-12
3	7	15	1.09E-8	1.16E-10	1.56E-11
4	3	15	1.07E-8	3.36E-11	4.22E-12
5	9	15	2.99E-9	3.68E-11	9.15E-12
6	7	11	2.74E-9	1.57E-11	1.75E-12
7	3	11	2.70E-9	3.17E-12	3.28E-13
8	5	15	2.70E-9	2.75E-11	3.60E-12
9	7	15	2.03E-9	2.17E-11	2.91E-12
10	7	15	2.00E-9	2.14E-11	2.87E-12

It is clearly seen that repair modelling decreases the fuel damage frequency compared to the result calculated from the static model. Even without modelling make-up system repairs, the fuel damage frequency decreases 60% in the transient case. This is mainly because of the possibility to repair the spent fuel pool cooling system before boiling. Modelling one or two make-up system repairs decreases the result much more. The decrease gained by modelling one make-up system repair is near 90% in both scenarios.

In the transient case, the decrease from the second make-up system repair is smaller, 38%. The reason for this is that non-repairable diagnosis failures in minimal cut sets 29 and 32 (in Appendix A) become the most important failures. For those minimal cut sets, only smaller decrease in frequency was gained by considering the possibility to repair the spent fuel pool cooling system before boiling. Some decrease to the fuel damage frequency could still be achieved by modelling third make-up system repair, but the impact would be smaller.

In the loss of offsite power case, the fuel damage frequency is decreased more compared to the static result than in the transient case. The reason for this is that make-up system 1 is not really credited in the static model, because when the power supply to the whole spent fuel pool cooling system fails, also the power supply to make-up system 1 fails. However, when a diesel generator supplying the both systems is repaired, make-up system 1 can be used. The repair comes very likely before fuel damage, so make-up system 1 can be used in most scenarios, and a failure of make-up system 1 is therefore required for fuel damage, unlike in the static model.

The mission times of the make-up systems are on average shorter than 24 hours used in the static model, but also much larger values appear in the simulations. In the transient case, the mission time is 20-30% of the simulation cycles over 24 hours, and the largest mission time was over 300 hours. The reason for longer mission times is that the repair of the spent fuel pool cooling takes a long time, while the time to reach normal water level is typically quite short. The MTTR of the spent fuel pool cooling is therefore the determining factor with regard to mission times. In the transient case, the impact of the dynamic treatment of the mission times is quite small.

In the loss of offsite power case, mission times are on average much shorter than in the transient case, because the spent fuel pool cooling can be repaired faster. This can be seen in the results so that the frequencies of the minimal cut sets with failure to run events decrease much more than the frequencies of other minimal cut sets (compare e.g. MCS 1 and 2). In the transient case, the effect is much weaker.

In the transient case, the impacts of the MTTR values of the make-up system related components are visible in the minimal cut set results. Repair of a pump failure takes on average much longer than repair of a diesel generator failure. Therefore, the minimal cut sets including a diesel generator failure have significantly smaller frequencies when two make-up system repairs are modelled.

Comprehensive sensitivity analyses on modelling assumptions and parameters are presented in Appendix A. In the LOOP case, the results are quite sensitive to the repair time distribution of the spent fuel pool cooling, whereas the sensitivity is smaller in the transient case. Sensitivity on MTTR parameters in general is also significant in both cases. The results depend quite significantly on the time window from boiling to fuel damage and to a smaller extent on the time to boiling. Sensitivity on make-up system start times is relatively small, unless significantly longer manual action durations are used.

6.3.4 Discussion

6.3.4.1 Spent fuel pool physics

In this study, spent fuel pool water level and temperature were calculated using very simple models mimicking the time-dependent behaviour of those variables. It seems possible that simple models can be used to produce good approximations for PSA results as the behaviour in the models used here is quite similar to some deterministic analysis results found from literature (Ramadan et al., 2018; Tynys, 2017; Wu et al. 2014; Zhang et al. 2017). Anyhow, for real application, the physical modelling obviously has to be considered more in-depth. There could be two possible approaches to perform the modelling:

1. Physical equations would be modelled in FinPSA scripts. It should be considered how accurate modelling is practical to do in the scripts. It would likely be beneficial to use some conservative simplifications. For example, the model in (Ramadan et al., 2018) seems simple enough to be implemented in the scripts.

2. Deterministic analyses would be performed outside FinPSA, and the results of those would be implemented in the scripts. For example, conservatively estimated fits of temperature and water level behaviour curves could be used in FinPSA. This way FinPSA modelling could be kept quite simple, but the model parameters would be based on deterministic results.

6.3.4.2 Modelling approach

The script-based modelling offers quite a lot of flexibility for the development of the model. However, some limitations are set by the static event tree structure. The event tree -based approach works best when events are known to occur in specific order, e.g. make-up system 1 is used before make-up system 2. The analysis of the event tree only progresses in the order defined by the static structure. When modelling events that can occur in different orders, the event tree structure becomes easily very complex, i.e. the same events appear in multiple positions in the tree, or alternatively the scripts behind the event tree become very complex as the structure of the tree does not correspond to the chronology of the events. With the assumptions made in this study, there is no problem, but if e.g. the make-up systems would be used in parallel and either of them could be used first, the modelling would be more difficult.

An option to overcome the problems with the event tree modelling would be to build a simulation model without event tree, e.g. a discrete event simulation model. The modelling would, of course, be more challenging, but also more flexible. On the other hand, the event tree approach is very convenient for probabilistic analysis, so the modelling needs must be considered carefully when deciding about the modelling approach.

Another issue with regard to modelling approach is the scope of the model and its relation to static PSA. In this study, it was convenient to develop an event tree that corresponded to the most important minimal cut sets of the static PSA model. A simulation-based event tree model could also be developed as an independent spent fuel pool PSA. In this case, the model would need to be more comprehensive, covering all significant failures. The event tree structure would probably need to be different and could not have separate branches for all basic events. One approach could be to merge failures with same impacts, use system level failure modes in the model, and calculate the failure rates or probabilities for the system level failure modes in background. It could anyway be beneficial to use a static PSA model as a starting point for this

type of dynamic modelling, because all significant failure combinations need to be identified and the static approach is good for that. Since both the static fault tree modelling and script-based modelling have limitations, it could also be studied if those could be combined in some way.

6.3.4.3 Uncertainties

Uncertainty analysis in the context of simulation-based event trees has previously been studied in (Tyrväinen & Karanta, 2019). The aim in uncertainty analysis would be to estimate the epistemic uncertainty related to the fuel damage frequency, whereas the fuel damage frequency itself represents aleatory uncertainty with regard to the occurrence of the fuel damage. Because of this, epistemic and aleatory uncertainties should be separated. In practise, the simulation model should include epistemic and aleatory variables, which should be treated separately. The most straightforward way to perform the uncertainty analysis would then be to have two separate sampling loops in the Monte Carlo simulation, the outer loop for the epistemic uncertainties and the inner loop for aleatory uncertainties. This would require quite large number of simulations, but at least the simulation model in this study is not very computationally demanding. It would also be challenging to estimate the epistemic and aleatory uncertainties related timing variables. For example, a repair time varies naturally quite a lot between different trials, but there is also epistemic uncertainty related to the probability distribution of the repair time.

Model uncertainty is an uncertainty type that is more difficult to estimate than parameter uncertainties. In this case, there is uncertainty on the use of make-up systems and actions related to them, i.e. whether the actions are consecutive or parallel. It was also assumed that the actions on make-up systems start only when boiling starts, which is a conservative assumption. It is uncertain when the actions really start, and it can depend on how the spent fuel pool cooling system fails. The models for spent fuel pool water level and temperature are also sources of uncertainty.

6.3.4.4 Common cause failures

The simulation-based event tree approach is not very handy for the management of many CCF combinations, but in principle, CCFs can be modelled in the same way as single failures. If critical CCF combinations are identified beforehand (e.g. by producing minimal cut sets using a static PSA model), they can be modelled as separate event tree branches. It may be possible to merge some combinations if the impacts on accident progression are same. The modelling of a specific CCF event is identical to single failure modelling, given that the components fail at the same time. It would also be possible to model different failure times for the components participating in the CCF and take that into account in the computation of spent fuel pool conditions, if suitable data or assumptions could be found.

6.3.4.5 Modelling reactor accidents

The simulation-based event trees have been used for level 2 PSA. Level 2 PSA is quite natural application area for the simulation-based event trees, because it focuses on physical phenomena rather than failures of safety systems. The modelling approaches applied in level 2 have been quite different from the approach used in this study. Typically, probabilities have been determined in static or semi-dynamic manner, but source term computation has been dynamic. Okkonen (1995) studied more physics-based modelling for level 2 PSA, but it has not been

used at the same level of detail in real life models. Different level 2 PSA modelling techniques have also been studied in (Tyrväinen & Karanta, 2019) with a smaller scope.

Modelling level 1 PSA reactor accidents using the simulation-based event trees would be much more complicated than the modelling of the spent fuel pool accidents. Reactor behaviour cannot necessarily be approximated using simple deterministic models, like the spent fuel pool, and there are more variables and more systems impacting the accident progression. In principle, similar type of approach would be applicable, but it might require a heavy deterministic model to calculate the time-dependent behaviour of different variables, and the number of scenarios to be modelled would be a problem. Dynamic analysis can however be done with different scopes and levels of detail. It could be feasible to use such dynamic approach for the analysis of some specific limited scenario rather than full-scope PSA.

6.3.5 Pros and cons

Benefits of the simulation-based event tree approach include:

- Generally, the script-based modelling is flexible. The modelling approach can be tailored according to specific modelling needs. The method itself does not force the analyst to simplify the modelling, but the analyst has freedom to choose the assumptions and simplifications. Computation formulas can be customized, and various probability distributions can be used for the timings of events.

- Time-dependencies and timings can be modelled explicitly.

- It is possible to model time-dependent physical behaviour of the spent fuel pool, and determine the mission times and available times based on the spent fuel pool conditions.

Drawbacks include:

- The model may become quite complex. The model used in this study is well manageable, but it is not known if modelling of a real spent fuel pool would go as smoothly, because there would be more systems to be taken into account.

- Verification of the model is not easy.

- The analysis requires more input data than static analysis, particularly probability distributions for the durations of manual actions.

- The model is not tightly integrated to static PSA. In this study, the final results based on the minimal cut sets of the static model and the simulations with the dynamic model were calculated in Excel. Better tool support for the management of the analysis could, of course, be developed. A simulation-based event tree model could also possibly be developed to be independent from the static model so that such integration would not be needed.

- Computation of risk importance measures is not as straightforward as with the static approach, except for Fussell-Vesely. The same goes to uncertainty analysis. In general, the approach sets new challenges to minimal cut set management if applied on a large scale.

- Modelling of large number of failure combinations, such as CCFs, is challenging, and it seems necessary to make simplifications. It could be studied if fault trees could be integrated to the method to overcome this problem.

- As discussed in Section 6.3.4.2, the event tree approach has limitations in modelling parallel actions and events, e.g. if two make-up systems can be used at the same time. A simulation model not bound by a static event tree structure could overcome that problem.

6.4. PSA Benchmark

The methods that are compared in this section are

- Enhanced fault/event tree (EFET), see section 6.2

- Initiators & All Barriers (I&AB), see section 6.1

- Simulation-based event tree (SBET), see section 0

The methods have all been tested in pilot studies. The purpose of this benchmark is to compare the results and insights from the pilot studies. Also general features of the methods will be compared. The benchmark is thus divided into the following parts:

- Pilot study on PROSAFE SFP model, section 6.4.1

- Pilot study on PROSAFE Core model, section 6.4.2

- Pilot study on full scale SFP model, section 6.4.3

- General features of the methods, section 6.4.4

6.4.1 Pilot study on PROSAFE SFP model

The parameters that have been compared are:

- Qualitative interpretation

- Safe state definition

- Repair assumptions

- Parameters used in the model (repair probabilities, time windows)

- Results

    - Top frequency

    - Dominating MCS

Safe State

The definitions of the Safe State for all methods are in general that the cooling system should be back in operation, but there are some differences in the definitions.

In the EFET & SBET method the focus is on getting back the cooling system in operation. In SBET there is an additional requirement to this which is that the water level in the SFP must be back at normal levels. This requirement is modelled in a conservative way in EFET and I&AB, as it is not possible to start the cooling system after the pool has started to boil and the operation of a MU system has not been established.

In I&AB it is assumed that when the initiating event is repaired, the cooling system is back in operation again, since the initiating event caused the cooling system to stop in the first place. The difference in I&AB compared to the other methods is for example in the LOOP case that in the other methods a safe state would be reached if the cooling system is operating powered from the backup diesels. In I&AB the safe state is not reached until the cooling system is operating powered from the external grid. In SBET, it is an assumption used in this study that the cooling system operation with a diesel generator is a safe state, but it would also be possible to use the definition used by I&AB.

Repair assumptions

Partly different repairs and available times have been modelled by different methods. In I&AB, repairs of all failed components of the spent fuel pool cooling system and its support systems have been modelled to some extent, whereas only one repair of the spent fuel pool cooling has been modelled by the other methods. I&AB considers repairs of the spent fuel pool cooling system and make-up systems within 24 hours, whereas the other methods consider longer available times for make-up system repairs. All repairs are assumed parallel in I&AB. In SBET, make-up system repairs have been assumed consecutive, i.e. one make-up system repair is performed at a time.

Parameters

Table 47 shows the repair parameters used in each method. In the EFET method HEP is used as the parameter where in I&AB and SBET a MTTR is used. How the parameters have been determined is described in the pilot study for each method. The HEP and the MTTR is related through the exponential distribution equation, see section 5.1.4.

It can be noted that the SFPC system and the MU:1 system are powered by the same diesel. However, the HEP will be different depending on which system will be credited after the repair, as the available time is different. This has been taken into account in the SBET method. In EFET, only repair for MU:1 is considered.

Table 47. A summary of the input parameters used in the three pilot studies.

Component	Failure Mode	System	EFET	I&AB	SBET
			HEP	MTTR [h]	MTTR [h]
Heat exchanger	Failure	SFPC	-	19	19
Pump	Fail to start	SFPC	-	20	-
Pump	Fail to run	SFPC	-	32	32
Diesel	Fail to start	SFPC	-	11	11
Diesel	Fail to run	SFPC	-	15	15
Pump	Fail to start	MU1	6,3E-02	20	20
Pump	Fail to run	MU1	6,3E-02	32	-
Diesel	Fail to start	MU1	4,0E-03	11	11
Diesel	Fail to run	MU1	4,0E-03	15	15
Pump	Fail to start	MU2	-	20	20
Pump	Fail to run	MU2	-	32	-
Diesel	Fail to start	MU2	-	11	11
Diesel	Fail to run	MU2	-	15	15
Gas Turbine	Failure	SFPC/MU1	-	12	-

The same time windows are used in all pilot studies, 24 hours until boiling and then 72 from boiling to fuel damage.

Results

The results from the pilot study of the PROSAFE SFP model is presented in this section. The FD frequencies calculated with the different methods are presented in Table 48.

Some remarks:

- Only results for consequence FD are presented here. The pilot study with I&AB did also include consequence FAB.
- For SBET the results with the maximum number of repairs modelled are presented, even though also results with fewer make-up system repairs are presented in Section 6.3.3.2.
- Some assumptions that have an impact on the results are different in the pilot study models, for example:
    - I&AB: Available time for repair in FD sequences are modelled conservatively
    - EFET: Only repair of the failure mode with the longest execution repair MTTR is used to calculate the used HEP for all component failure modes
    - SBET: Diagnosis HEP of make-up system 2 is different in the static model, and the basic event does not appear in top minimal cut sets

Table 48. The FD frequency for the three studied initiating events using the three different methods.

Initiating Event	Enhanced fault/event tree			Initiators & All Barriers			Simulation-based event tree		
	Static[1)]	EFET	Diff	Static[2)]	I&AB	Diff	Static[3)]	SBET	Diff
Extreme snow	4,4E-07	1,8E-07	-58%	4,2E-07	8,8E-08	-79%	-	-	-
LOOP	2,3E-07	1,0E-09	-100%	2,2E-07	2,6E-10	-100%	1,1E-07	1,1E-10	-100%
Transient	6,3E-08	6,4E-09	-90%	6,0E-08	4,5E-09	-93%	4,0E-08	8,8E-10	-98%

1) Results obtained from MCS Analysis Cases
2) Results obtained from Consequence Analysis Cases
3) Results obtained from 32 first MCS from a slightly different static PSA model

Although the pilot studies differ somewhat regarding assumptions and input parameters, two main conclusions from the comparing the results for the FD frequency can be concluded:

- The fully dynamic method, SBET, entails the largest decrease in the results. The static approach, EFET, entails the least decrease. It should also be noted that the modelling used for the I&AB results for consequence FD contains conservative assumptions, i.e. it is possible to make a more detailed model and lower the results more if the user desires.

- The methods are consistent on the decrease in the result, with LOOP being the case that is the most conservative without the consideration of repair. All methods conclude that modelling without consideration of repair is greatly conservative.

A very important aspect of the results is also to identify the main risk drivers in the analysed system. This is done by ranking the MCS in the order of contribution to the total consequence frequency. From the pilot studies it was found that the methods did change the rank of the individual MCS. The general observations from comparing the MCS before and after applying the method are described below for each method.

- EFET:
    - The importance of MCS with HFEs (and especially all HFEs-MCS) tends to increase and thus also the parametric uncertainty.
    - The repair probabilities impact the composition of the repaired MCS-list.
    - The risk contribution from non-repairable sequences becomes significantly higher.

- I&AB: The following findings were noted after applying the method:
    - When there are two or more Failure in Function (FIF) events in a MCS the significance of these MCS tends to decrease, whereas MCS with maximum one FIF tend to be of higher significance to the total risk.
    - The contribution to the risk for each MCS also depends on the repair rates of components and available time in each MCS.

- SBET: The following changes were observed compared to the results of the static model:
    - The importance of MCSs with HFEs increases in general. In the transient case, MCSs with make-up system diagnosis failures become the most important MCSs, because the diagnosis failures cannot be repaired.
    - MCSs with smaller MTTR of the spent fuel pool cooling become less important.
    - In the transient case, MCSs with FLEX diesel generator failure become less important, because diesel generator failures can be repaired on average significantly faster than pump failures.
    - In the LOOP case, the significance of MCSs with failure to run of the FLEX diesel generator decreases, because the mission times are on average significantly shorter than 24 hours.

The reader should be aware of the slight differences in parameters and modelling assumptions that have been used in the three different pilot studies, which means the comparisons of results are somewhat approximate, but still gives a good indication of the different behaviours of the methods.

6.4.2 Pilot study on PROSAFE Core model

A limited pilot study on the PROSAFE reactor model has been performed with the EFET and I&AB methods.

Safe State
The differences in the definition of the safe state are in general the same for the core model as described for the SFP in section 6.4.1.

In I&AB the safe state is defined as the success to repair the initiating event, which is modelled by assigning a MTTR to the initiating event extreme snow. This MTTR can be interpreted as the time during which the barriers, including repairs, need to withstand in order to avoid the undesired consequence. It can thus in some sense be compared to the mission time modelled in a static PSA. The MTTR for the initiating event extreme snow has been assumed to be 24 hours, based on the mission time used in the original study.

In EFET the safe state definition does not differ from the original study. This means that the barriers, including repairs, need to withstand during the fixed mission time of 24 hours. The difference between the methods here is that in EFET (as applied in these pilot studies) there are no requirements on restoring the initiating event.

Repair assumptions
Regarding repair assumptions, the same principles as described in section 6.4.1 applies.

Parameters

How the parameters are determined and how they are used are presented in section 6.4.1. The specific parameters for the core modelled are presented below.

Table 49. A summary of the input parameters used in the pilot studies for core events.

Component	Failure Mode	System	EFET	I&AB
			HEP	MTTR [h]
Heat exhanger	Failure		-	-
Pump	Fail to start		-	-
Pump	Fail to run		-	-
Diesel (ICC)	Fail to start		0.3	11
Diesel (ICC)	Fail to run		0.3	15
Pump	Fail to start		0.3	-
Pump	Fail to run		0.3	-

In I&AB the available time for repair is assumed to be 10 hours.

Results

The results from the pilot study of the PROSAFE Core model are presented in this section. The CD frequencies calculated with the different methods are presented in Table 50.

Some remarks:

- I&AB: The assumed available time to repair the ICC diesels is 10 hours, regardless of when during the sequence they fail.
- EFET: Only repair of the failure mode with the longest execution repair MTTR is used to calculate the used HEP for all component failure modes. Also, repair of the independent core cooling (ICC) pump and diesel is modelled (during time window 12-24 hours).

Table 50. The CD frequency for the studied initiating event using the two different methods.

Initiating Event	Enhanced fault/event tree			Initiators & All Barriers		
	Static[1)]	EFET	Diff	Static[2)]	I&AB	Diff
Extreme Snow	2,0E-07	1,5E-07	-25%	2,0E-07	8,8E-08	-56%

1) Results obtained from MCS Analysis Cases
2) Results obtained from Consequence Analysis Cases

A very important aspect of the results is to identify the main risk drivers in the analysed system. This is done by ranking the MCS in the order of contribution to the total consequence frequency. From the pilot studies it was found that the methods did change the rank of the individual MCS. The general observations from comparing the MCS before and after applying the method is described below for each method.

- EFET: In the original model, the dominating failure combination is failure of snow removal together with failing ICC diesel. When crediting repair, late diesel failures become less important since these are considered repairable. Early diesel failures are still important since repairs are not credited for these events.

- I&AB: With the I&AB method the order of the dominating MCS is unchanged. However, even though the order of the MCS is not changed in this case, the overall contributions from different sequences have changed. Note that in this simplified study it was assumed that there was no difference in available time to repair between early or late failures.

In this studied case the I&AB method resulted in a greater decrease of the core damage frequency than the EFET method. However, the results should not be directly compared as many assumptions in each study are different. The differences are mainly explained by these factors:

- The EFET method uses HEP for repair based on the most conservative failure mode. In I&AB a different MTTR is used for failure to start versus failure to run for the ICC diesel.

- I&AB credits the extra time that is available during the period of time when the diesel is running before it fails.

- In the EFET study the failures were divided into early and late failures with different prerequisites regarding possibilities to repair. This distinction was not made in the I&AB study. It would be possible to do it in the same manner with the I&AB method.

6.4.3 Pilot study on full scale SFP model

Limited pilot studies have been performed on a full scale PSA-model with the EFET and I&AB methods.

Safe State
The same assumptions as for the PROSAFE SFP model are used, see section 6.4.1.

Repair assumptions and Parameters
The same principles as for the PROSAFE SFP model apply, see section 6.4.1. The specific parameters used for the R4 model are presented below.

Table 51. A summary of the input parameters used in the pilot studies for the full scale SFP model.

Component	**Failure Mode**	**System**	**EFET**	**I&AB**
			HEP	**MTTR [h]**
Heat exhanger	Failure		-	19
Pump	Fails to start		6,2E-01	20
Pump	Fails to run		6,2E-01	32
Diesel	Fails to start		4,0E-02	11
Diesel	Fails to run		4,0E-02	15
Diesel Generator Breaker (assumed same as for diesel)	Fails to close		4,0E-02	10[1)]
Battery (assumed same as for diesel)	Fails to supply power		4,0E-02	15

1) The diagnosis part of the MTTR is assumed to be the same as for the diesel failure (5 hours). The execution part of the MTTR is obtained from generic data in the T-book 8 table 9.2.1 (5 hours).

Results
The steaming (ST) and fuel damage (FD) frequencies calculated with the different methods are presented in Table 52. For the EFET method, the analysis has been run with both one and two repairs (diesels and batteries for consequence FD and diesels and pumps for consequence ST). For the consequence ST, it is clear that the inclusion of a second repair is important. For consequence FD the diesel repair is the most crucial to include. This highlights the importance of carefully examining of how many iterations that are needed when applying the EFET method.

For consequence steaming the I&AB method results in a greater decrease of the frequency. This is explained by more realistic MTTR parameters, whereas in the EFET the most conservative failure mode is always assumed when calculating the corresponding HEP. The main driver for the lower result with the I&AB method is in this case that I&AB is considering the dynamic aspects of having components running, failing and repaired during the available time.

On the contrary the EFET method does not have the additional constraint that the initiating event also need to be repaired, as is required with the I&AB method to reach the safe state. This factor does instead affect the results to be lower using the EFET method.

For consequence fuel damage the EFET method results in slightly greater decreases of the frequency. The explanation to this is that some conservative assumptions regarding available time have been made in the analysis using the I&AB method. The available time has conservatively been assumed to be 24 hours for all repairs using the I&AB method, whereas the available time for repair of the make-up systems has been assumed to be 72 hours using the EFET method.

Table 52. The ST/FD frequency for the initiating event LOOP using the two different methods.

Initiating Event	**Enhanced fault/event tree**					**Initiator & All Barriers**		
	Static	**EFET R**	**EFET R2**	**DIFF R**	**DIFF 2R**	**Static**	**I&AB**	**Diff**
LOOP (PST)	1,0E-05	7,9E-06	5,5E-06	-21%	-45%	1,0E-05	1,8E-06	-83%
LOOP (PFD)	1,6E-06	1,4E-07	5,8E-08	-91%	-96%	1,6E-06	1,6E-07	-90%

6.4.4 General features of the methods

The findings and experiences based on the pilot studies together with general knowledge are also generalized to the overall features of the methods. Different aspects are compared for the three methods in Table 53 below.

Table 53. Features of each method.

Feature	**EFET**	**I&AB**	**SBET**
Safe State	The safe state definition does not differ from the original PSA study.	Initiating Event is repaired	The user can freely choose which definition to follow
Timing	All events happen immediately after the IE.	All failure on demand events happen immediately after the IE. Failure in function events have dynamic modelling of time windows.	Events can be assumed to take place at any point in time

Feature	EFET	I&AB	SBET
Multiple Component Failure	A component cannot fail after it has been repaired	A component can fail (and be repaired) several times during the analysed time window	A component can fail (and be repaired) several times during the analysed time window (each repair and failure needs to be modelled separately)
Mission Times	Static	Dynamic	Dynamic
Repair of initiating event	Not handled differently from other repairs	Required to reach safe state	Possible to model
Parallel repairs	Repairs are parallel	Repairs are parallel	Repairs can be parallel or consecutive
Integration with existing PSA	Separate analysis. Is performed as a separate task based on the MCS list.	Integrated. If other updates are made in the model, no separate updates are required of the repair and time windows modelling.	Separate analysis. Is performed as a separate task based on the MCS list.

Scope/Limitations	• Use existing model with fault trees/event trees
	• Safety graded approach
	• Cannot capture the dynamic behavior of repairs directly (but it can be adjusted in the repair probability calculations)
	• The quantification can consider dependencies with some additional work
		• Suitable for modelling of sequences with long mission times/unknown mission times and long time windows
		• A few features in RS PSA are as of today not supported by I&AB, for example:
		  • Importance & uncertainty analysis
		  • Negated events
		  • Mutually exclusive events
			• In principle, there are no limitations, but the model can become too large and complex if the case includes many failure combinations and complex dependencies.
			• The modelling approach used in this study was developed for spent fuel pool and its applicability to other problems has not been studied.

Additional input information required	• Information about time windows • Repair probabilities	• Information about time windows • MTTR for components/events • MTTR for the initiating event	• Probability distributions for the durations of manual actions • It needs to be known when specific actions start • Physical behaviour of the spent fuel pool needs to be modelled
Complexity	In general low complexity	In general low complexity	Medium/high complexity (depends on complexity of the analysed system, assumptions and simplifications)
Required Compentence	Basic PSA competence	• Basic PSA competence • The base method modelling repair of components does require very low training • The time window extension requires some more understanding of how to model time	• Good programming skills • Deep understanding of the related math and the time-dependencies • Capability to model the physical behaviour of the spent fuel pool

Feature	EFET	I&AB	SBET
		windows in different sequences	
Software	PSA software with either: • Post Processing capability • MCS addon • If none of these are available: complex (or at least time consuming) manual calculations are needed	RiskSpectrum PSA with the I&AB add-on	FinPSA includes a module for this purpose, and it's unique. The calculations could also be programmed with any mathematical programming language, but it would require more work than with the ready-made tool. Excel was used to integrate the minimal cut sets of the static model and the simulation results. A better tool could be developed for this purpose
Fulfilment of requirement specification (from 2019 report)	The method is compatible with general requirements regarding workload and it is adaptable due to a graded approach. The method satisfies the repair modelling requirements, but some modelling might not be explicit (i.e. modelling/quantification of CCF repair). The method satisfies most time window modelling requirements but since it is not dynamic it can at most do a static representation of dynamic behaviour. The method has limitations with regard to dynamic success criteria (because of limitations of the FT/ET base).	The general requirements regarding workload and integration with already used methods and software tools are fulfilled. The workload is flexible as I&AB can be used for selected parts of the model, since it is integrated with the existing model. RiskSpectrum software tools are used to apply I&AB. In general, the method satisfies all repair modelling requirements. However, dependencies between multiple repairs is not considered in the method but have to be modelled explicit by the analyst. The method satisfies all time window modelling requirements. Modelling dynamic success criteria is not integrated in the method but would have to be done explicitly by the analyst as for a normal static PSA study.	The method could be made compatible with ET/FT tool with further development work. In general, the method satisfies repair modelling requirements related to MCS quantification. The method satisfies all time window modelling requirements. The method could be suitable for modelling dynamic success criteria in some simpler cases, but it has not been studied.

Pros and Cons

The main pros and cons for each method is presented in Table 54.

Table 54. Pros and cons for each method.

Method	Pros	Cons
EFET	• Can use existing Fault Trees and Event Trees • Simple • Additional software not required • Safety graded approach	• Can be time consuming if many time windows/repairs are considered • Not dynamic • Quantification is a simplification since the repaired MCS list is not requantified by the software

I&AB	• It includes dynamic aspects into the static PSA model
	• It is easy to embed in an existing RiskSpectrum model
		• A few features in RS PSA are as of today not supported by I&AB, for example:
		  ○ Importance & uncertainty analysis
		  ○ Negated events
		  ○ Mutually exclusive events
		• Requires additional software add-on

SBET	• Flexibility • Modelling can be tailored according to specific modelling needs • Freedom to choose the assumptions and simplifications • Explicit modelling of time-dependencies • Modelling of time-dependent behaviour of spent fuel pool conditions	• Complexity • Verification of the model is not easy • More input data needed • No tight integration to static PSA currently available • Modelling of large number of failure combinations, e.g. CCFs, is challenging

Summary and conclusions

The three investigated methods all have several different features. The most significant features of each method are summarized in Table 55 below.

Table 55. Summary of features for each method.

Method	Summary
EFET	• Easy to apply on spent fuel pool (more work to apply on the core model) • The impact of repair on the result is large (especially the spent fuel pool)
I&AB	• Realistic application of failure and repair processes • Convenient to apply with the add-on on the existing PSA-model • A trade-off between the static PSA and a fully dynamic Markov-quantification
SBET	• Most realistic of the methods, but also the most complex • Flexible and case specific modelling of time-dependencies

From these insights we can formulate conditions for when each method is suitable to use depending on the requirements from the analyst, see Table 56 below.

Table 56. Conditions for use of each method.

Method	**When is the approach applicable?**
EFET	• Simple method that can be used with existing tools • Works on non-complex and complex models • For a limited number of conservatisms (time windows or repairs)
I&AB	• Manages that different initiators can require different time to the end state • Manages dynamic behaviour within sequence, both with regard to multiple components in operation/repair and also “grace times” • Can be applied to a full scale PSA models • Integrates the repair and time window modelling into the existing model, i.e. it is not a stand-alone analysis that requires additional updates
SBET	• When the analyst needs the freedom to define event timings, integrate deterministic computation, model complex time-dependencies, etc. • Limited usability when many failure combinations are involved in the analysis

7. Common cause failure

The impact of long time windows (or time windows in general) for “repair” of common cause failure is probably significant. Aspects to consider are the success criteria and the timing of events.

Consideration of repair of common cause failures needs (at least) to correlate with the required number of trains to successfully perform the required safety function. Here it matters for example in a case with success criteria 2 out of 4 whether the CCF is 3oo4 or 4oo4. For a case with 4oo4 two components needs to be repaired to fulfil the success criteria, while in the case of a 3-fold CCF only one component needs to be repaired. Also, the probability for the component to fail again needs to be considered (although that is also the case for independent failures). Conditional probabilities for components to fail again after repair should perhaps be investigated (this is also relevant for singe events failures). For the PROSAFE model success criteria w.r.t. CCF is not a problem since the spent fuel pool mostly has a 1oo2 or 1oo4 criterion.

The timing of events also must be considered. State of the art static PSA use the assumption that all events in a CCF occur at the same time. For repair of CCF this assumption is perhaps too simple. For failure modes that are not associated with a mission time (e.g. failure to start) this assumption is valid but that is not the case for failure modes that are associated with a mission time (e.g. failure to run). For the failure to run case the time windows can be investigated with some assumptions. Assume that the standard mission time of 24 hours is used and that the failures of a 4oo4 CCF will occur during that time. Also assume that the failure times are independent within this 24 hour time frame. Using a 12 hour mean time to failure for 4 components (3 hours MTTF per component) in a Poisson process results in the conditional time dependent probabilities of a 4oo4 CCF shown in Figure 44.

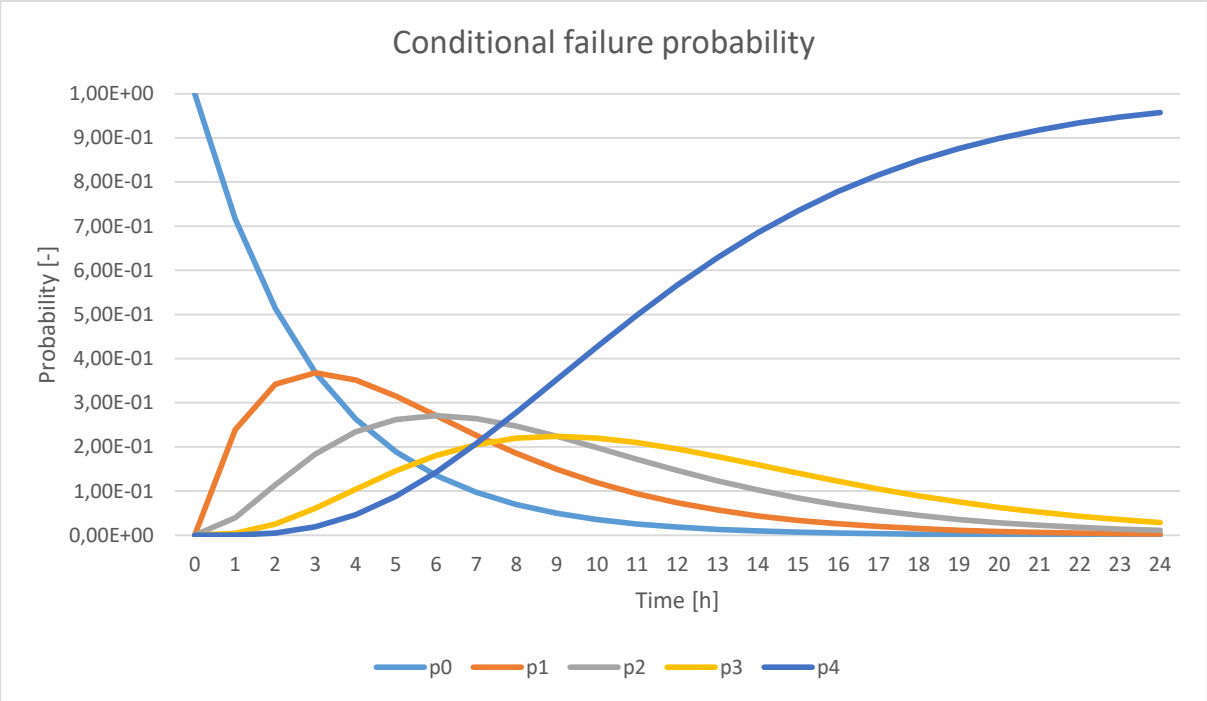

Figure 44. Time dependent conditional distribution of the failure to run 4oo4 CCF.

In Figure 44 p0 represents the probability that there are 0 failures at a specific time, p1 represents 1 failure etc. The timing between events follows an exponential distribution

according to Figure 45. It can also be noted that this model breaks down for values over 5 since the total time will exceed 24 hours.

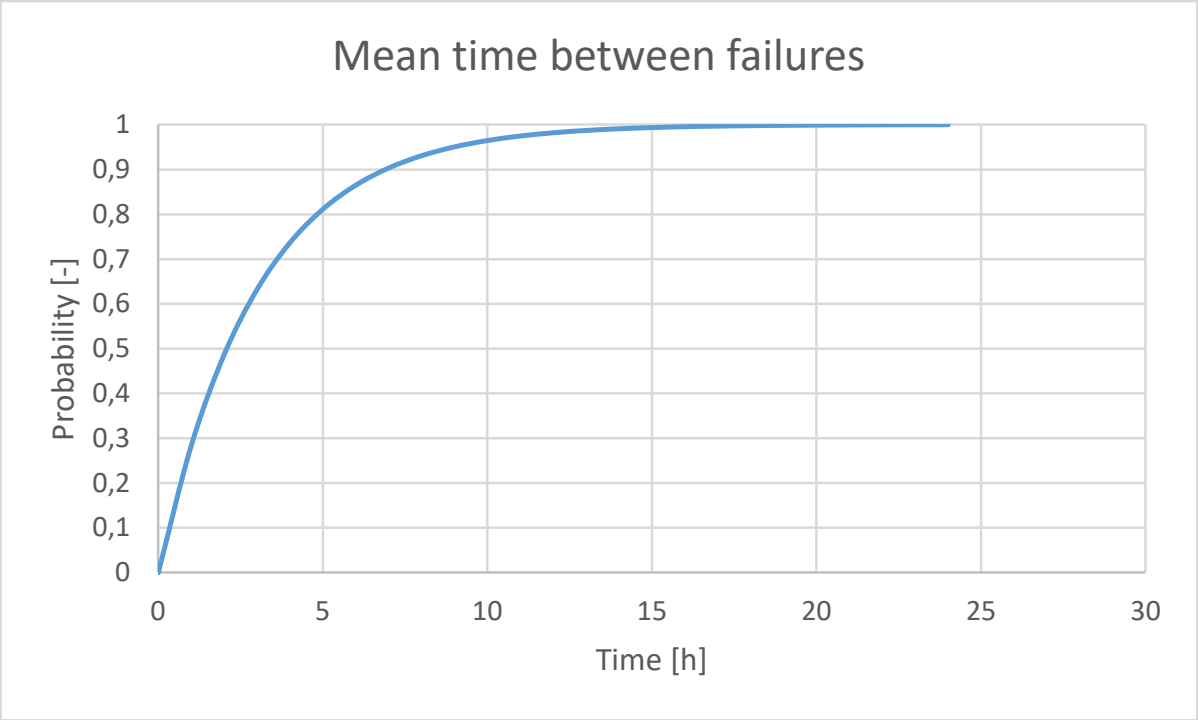

Figure 45. Mean time between failures for the 4oo4 CCF.

One approach to consider the impact of this extra time is to compare repair probabilities. If the extra time is 9 hours (time to go from one fault to four) then repair failure probabilities decrease according to Table 57.

Table 57. Reduction in repair failure probability.

MTTR	EXTRA TIME	REPAIR PROBABILITY
8	9	-68%
24	9	-31%

Another way to investigate this is to use Markov analysis. The Markov transition matrix in Table 58 is used for investigation in this section. The analysis starts from 4oo4 faults and has the distribution from Figure 44 at hour 9 (when there is a high probability to reach at least one fault). This results in a repair failure probability decrease of 62%.

Table 58. Markov transition matrix.

	Start						
Target	-	0/4 faults	1/4 faults	2/4 faults	3/4 faults	4/4 faults	FD
	0/4 faults	9,39E-01	5,00E-02	1,00E-02	1,00E-03	5,00E-04	0,00E+00
	1/4 faults	7,13E-01	2,26E-01	5,00E-02	1,00E-02	1,00E-03	0,00E+00
	2/4 faults	0,00E+00	7,13E-01	2,27E-01	5,00E-02	1,00E-02	0,00E+00
	3/4 faults	0,00E+00	0,00E+00	7,13E-01	2,37E-01	5,00E-02	0,00E+00
	4/4 faults	0,00E+00	0,00E+00	0,00E+00	7,13E-01	0,00E+00	2,87E-01
	FD	0,00E+00	0,00E+00	0,00E+00	0,00E+00	0,00E+00	1,00E+00

Conclusions

These two ways of estimating a better repair probability is not entirely comparable but gives result that indicate a moderate reduction in the repair failure probability. The conclusion of these limited tests is that the repair failure probability is highly dependent on the timing of the events in a CCF. It further needs to be shown whether the timing between events is not low for CCF-events.

8. Safe and stable state

As stated by e.g. IAEA-SSG-3, a successful end state in a PSA model should correspond to a safe plant state. In general terms, in PSA context, a safe state can be defined as a state, where the risk is negligible compared to overall PSA results. Then by definition, the analysis can be terminated when a safe state is reached, whereas the analysis needs to be continued when a safe state has not been reached. One could define some limit value for what the negligible risk compared to overall results means. However, that kind of quantitative definition would not be very useful, because its application would require computation of the risk at the state of interest. For practical use, a qualitative and more specific definition of a safe state is needed. One approach to develop such definition is to identify what are the plant conditions that imply negligible risk. It is however not an easy task, and the conditions may be plant-specific, particularly if nuclear facilities other than nuclear reactors are considered.

Literature offers several different safe state definitions for nuclear power plant PSA and deterministic safety analyses. Some of these are presented in Table 59. For example, STUK defines safe state as a plant state, where the reactor has been shut down and is non-pressurized, and removal of decay heat has been secured. Most other definitions do not consider reactor pressure. Some definitions state more generally that safety functions need to be maintained. ASME PRA standard, on the other hand, defines a safe state so that the reactor coolant system conditions are controllable and near desired values. This definition is vague and more difficult to apply directly. Sometimes, the safe state definition is also associated with a mission time, e.g. that cooling needs to be maintained for 24 hours to reach a safe state.

Table 59: Definitions for safe and stable state.

Source	Definition
ASME/ANS RA-S-2009	**Safe stable state:** A plant condition, following an initiating event, in which [reactor coolant system] RCS conditions are controllable at or near desired values.
STUK Y/1/2018	**Safe state** shall refer to a state where the reactor has been shut down and is non-pressurised, and removal of its decay heat has been secured. **Controlled state** shall refer to a state where a reactor has been shut down and the removal of its decay heat has been secured. **Controlled state following a severe reactor accident** shall refer to a state where the removal of decay heat from the reactor core debris and the containment has been secured, the temperature of the reactor core debris is stable or decreasing, the reactor core debris is in a form that poses no risk of re-criticality, and no significant volumes of fission products are any longer being released from the reactor core debris. **Safe state following a severe reactor accident** shall refer to a state where the conditions for the controlled state of a severe reactor accident are met and, in addition, the pressure inside the containment is low enough that leak from the containment is minor, even if the containment is not leak-tight.
IAEA-SSG-2	Typically, it is assumed that a **safe and stable end state** is achieved when the core is covered and long term heat removal from both the core and the containment is achieved, and the core is, and will remain, subcritical by a given margin.

Source	Definition
IAEA-SSR-2/1	**Safe state:** Plant state, following an anticipated operational occurrence or accident conditions, in which the reactor is subcritical and the fundamental safety functions can be ensured and maintained stable for a long time. **Controlled state:** Plant state, following an anticipated operational occurrence or accident conditions, in which the fundamental safety functions can be ensured and which can be maintained for a time sufficient to effect provisions to reach a safe state.
IAEA-TECDOC-1804	**Safe stable state:** A plant state, following an initiating event, in which plant conditions are controllable at or near desired values and within the success criteria for maintenance of safety functions. A safe stable state is achieved when the following criteria are met: • All required safety functions are successfully performed during the defined mission time. • The safety functions are not expected to be lost at a point close-in-time after the specified mission time (i.e. there is compelling evidence that the successful safety functions have adequate operating capacity to be maintained for an indefinite period following the end of the specified mission time, or that there are adequate alternative means of performing the safety functions that can be implemented with high confidence after the specified mission time).
NUREG-2122	**Safe stable state:** Condition of the reactor in which the necessary safety functions are achieved. In a PRA, safe stable states are represented by success paths in modeling of accident sequences. A safe stable state implies that the plant conditions are controllable within the success criteria for maintenance of safety functions.

STUK's definition seems to be a good candidate for practical use. However, it could benefit from being more precise, e.g. what it means that removal of decay heat is secured. Based on the PROSAFE questionnaire, there are also PSAs, where the reactor does not need to be non-pressurized in a successful end state. This in fact corresponds to STUK's definition for a controlled state. It would require some in-depth consideration to say, whether the risk can be considered negligible when the reactor has not been depressurised. In reality, the conditions that imply a safe state could also be case-specific.

PSA for the spent fuel pool is partly different from the reactor PSA with regard to safe state considerations. The spent fuel pool does not need to be shut down or depressurized. In that sense, the consideration is simpler. Only the spent fuel pool cooling matters. Still, it is not trivial, what it means that spent fuel pool cooling is secured.

In the transient scenario of the PROSAFE example, we have assumed that the main spent fuel pool cooling system has to be back in operation to secure long term cooling. A scenario with another failure of the main cooling system resulting in fuel damage would have a negligible probability. On the other hand, we have assumed that cooling by a make-up system is not a safe state, because the risk of a make-up system failure and consequent fuel damage is significant. To be accurate, it depends on the failure rate of the make-up system, the time the make-up system can be operated and the repair time distribution of the main cooling system. In the

PROSAFE model, failure to run of the FLEX diesel generator supporting make-up system 2 contributes significantly to the total risk, because it has a quite large failure rate. Therefore, operation with make-up system 2 is clearly not a safe state. Failure to run events of make-up system 1 have quite small risk contribution, but not necessarily small enough so that operation with make-up system 1 could be considered as a safe state.

In the loss of offsite power scenario, it is not clear whether the recovery of the offsite power is needed or whether operation of the spent fuel pool cooling system with a diesel generator is a safe state. The safe state definition in the LOOP scenario should be analysed further, i.e. whether the total risk increases because of the additional risk contribution from sequences where another failure of the main cooling system occurs before the recovery of the offsite power.

9. Uncertainties

No exhaustive investigation of the many different parameter, model or completeness uncertainties is performed in the PROSAFE pilot studies but some cases (i.e., by sensitivity analyses) are considered in both the HRA and PSA part.

The time window is one parameter that is considered to have a large impact on the results when repair is modelled. This section elaborates on how the time window (both long and short) impacts completeness, parameter and model uncertainties. The elaboration is a qualitative assessment from the project. The assessment uses an index stretching from 1 to 3 (1 is low and 3 is high) for both the strength of the uncertainty (high or low variation) and the impact or sensitivity of the uncertainty (if a high or low change in the uncertainty propagates to a high or low change in the results).

Completeness uncertainty aspect of manual actions (what manual actions are not considered in the analysis that should be considered): For a "shorter" time window of 0-24 hours after initiating event, the actions that could be considered have likely been analysed thoroughly (assigned 1) but the impact or sensitivity is still at least moderate (assigned 2). For a longer time window of 24-72 hours the strength is moderate since there is perhaps not as many instructions/training (and it increases the likelihood that the analysis has missed crucial actions) as for short time windows (assigned 2) and here the impact of manual actions could be considered higher since it likely requires manual actions to counteract technical failures in the shorter time window (assigned 3). For even longer time windows of over 72 hours the uncertainty strength must be considered high (assigned 3) since often the analysis does not consider this time. Both strength and impact are then assigned 3. This can be seen in Figure 46.

Parametric uncertainty of the mean time to repair (without consideration of the diagnosis): The parameter uncertainty is assigned a strength of 2 in all time windows. But the available time (which in combination with MTTR determines the repair probability) is likely correlated with the time window. For 0-24 hours we likely have a short time window and thus the impact from MTTR will be low since the available time could in some cases be too short to even consider repair and is assigned 1. For 24-72 hours, the available time is likely more reasonable to consider repair and the impact is assigned 3. For over 72 hours the available time is likely large in relation to MTTR and thus the impact of changing MTTR is low and assigned 1. This can be seen in Figure 46.

Model uncertainty of time window modelling: For 0-24 hours the uncertainty strength is probably low since knowledge of what time windows to model for repairable events is not too difficult to evaluate (assigned 1) but the sensitivity is high since it will determine if repair is to be considered (assigned 3). For 24-72 hours the strength and the impact are probably low (both assigned 1) since the time window should not be too variable (if that is not the case this assignment is obviously not valid). For the longest time windows of 72+ hours we have higher uncertainty strength (assigned 2) since it is harder to say if the time windows will have some variability, but the impact is probably still low. This can be seen in Figure 46.

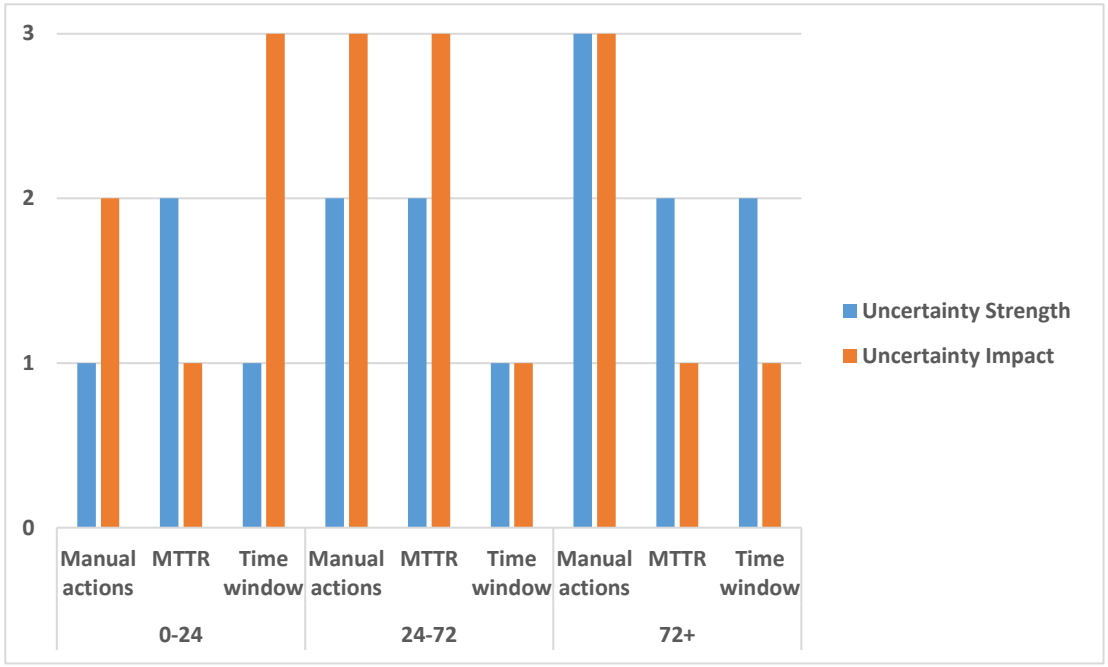

Figure 46. An illustration of uncertainties and their impact for different time windows.

10. Conclusions

The PROSAFE project was performed with the objective to improve the quality of safety assessment methods with respect to safe and stable state definition and assessment of long time windows, including human reliability analysis, crediting repair and modelling of different time windows. The scope of the project is broad and the addressed issues quite complex in nature. It is however necessary to start addressing these issues in order to find a better balance between the level of realism of PSA-models and practicality of the modelling approaches. Although further work is needed within several of the investigated areas, PROSAFE have provided important findings and some of the keys needed for a more realistic consideration of long time windows in future PSA:s.

The conclusions of the PROSAFE project and some remaining open issues is presented below. Since PROSAFE has covered the two separate, but interconnected, disciplines of HRA and PSA, these are presented separately for increased clarity.

10.1. HRA

The HFEs studied in PROSAFE have long available time windows, ranging from 2 hours to a few days (maximum 2 weeks). Quantitative analysis has been performed for the selected HFEs using the selected F/R HRA method, SPAR-H and ASEP. Through the pilots, a better understanding is reached about the Repair, FLEX and 'normal' category C human actions involved in the PROSAFE scenarios.

In summary, main HRA related conclusions/findings are:

- Diagnosis HEPs of these HFEs are in general low (compared with their execution HEPs)
    - Long time window does not guarantee a large time margin (required diagnosis time/available diagnosis time). However for the PROSAFE HFEs the time margins are quite sufficient and thus the basis diagnosis HEP is low.
    - There are negative PSFs for diagnosis in some situations, however they do not increase the diagnosis HEP significantly. These PSFs are assumed based on the our judgement for the scenarios in the pilot studies. The applied PSF multipliers could be large if we need to change our assumptions and then the derived HEPs will be higher.
    - Recovery factor that can further lower the diagnosis HEP is not considered in the Swedish pilot study as the diagnosis HEP is already low. In the Finnish pilot study, recovery from wrong diagnosis is a part of the recovery model (see section 5.2.2.2.1).
- Both F/R and SPAR-H method consider important PSFs together with the available time in the diagnosis HEP evaluation; ASEP diagnosis does not consider PSFs in general.
    - F/R might produce lower HEP than SPAR-H, as its 5 PSF multipliers for pessimistic situations are typically smaller than those in SPAR-H.
    - It is possible to use upper or lower boundary curves in ASEP (some factors are considered, e.g. stress level).
- 5.2.2.2.1Dependencies between two diagnosis HFEs (for the two make-up systems) is justified to LD as there are long time window, different crews, different procedures, etc.
- Execution HEP is typically higher than diagnosis HEP in the pilot studies.
    - F/R method for execution is simplified but conservative .
        - It relies on 'experts' to select suitable Grades for the post-diagnosis action as a whole.

        - It has good coverage of important PSFs in the descriptions.
    - ASEP method is simplified, it is a conservative version of THERP.
    - For repair execution: The MTTR exponential approach is very sensitive to the ratio of the available time T_a and MTTR, which makes it a good engineering choice for repair execution HEP.
        - The obvious drawback is that it does not consider other PSFs. HEP can be extremely small when T_a is large, thus it is important to take diagnosis HEP into account.
        - Note: the availability of equipment, tools, and personnel needed for repair action should be evaluated and considered in the repair execution HEP, however this part is not included in the pilot study.

The following items are considered important and suggested for future development:

- Diagnosis
    - In the performed pilot study, the diagnosis HEP is not dominating. This is based on our expert judgement of the levels of PSFs in the selected scenarios. It is suggested to perform more studies with more inputs from the plant personnel to confirm our judgements used in the pilot study. Further works can also be performed to develop clear criteria on when the diagnosis HEPs can be ignored without risk of underestimation.
    - Guidance to consider important PSFs can be improved to better consider the specific challenges in FLEX and repair. Typical challenges are: the operators might be reluctant to take some actions e.g. use seawater; Prioritization when order is not specified but order is important to success.
- Execution
    - Both F/R and SPAR-H methods are not task decomposition based.
        - It is relied on expert judgement and thus good documentation of interview and clear guidance for expert judgement is important.
        - The qualitative task analysis is very important. However, it is quite resource intensive to reach a good quality and the task analysis in the project became limited. More plant inputs and discussions would be needed to reach the quality the project was aiming for.
    - F/R execution
        - Description guidance for selection of probability scale can be further improved so that expert judgement can be easier.
        - Criteria for recovery consideration can be further tested, e.g. (1) possibility of detecting the errors (e.g. a slip of action) based on the 'rapid' system feedback (2) have time to redo the action by same personnel or different personnel.
- The accuracy of HEP estimates of individual activities plays an important role in ASEP. The HEP values listed in section 8 of (Swain, 1987) are generic and mainly meant for main control room activities. Therefore, further study aiming at finding HEP estimates of various repair activities would improve the accuracy, reliability and credibility of HRA of tasks involving repair activities and conducted using ASEP.
- Further HRA benchmark on PROSAFE scenarios and comparing with the findings from other peer studies (literatures)
- Further collect information on industry drills, e.g. on FLEX and repairs. As MTTRs are needed for repair execution HEP estimation, there is a need to find reasonable MTTRs for the failed components. If an industry generic MTTR is used, there is a need to find reasonable ways to adjust the 'generic' MTTR for the specific situations.

10.2. PSA

Three different PSA methods have been presented, tested in pilot studies and compared. These methods are Initiator and all barriers (I&AB), Enhanced fault/event tree method and simulation-based event tree method. All three methods enable more realistic modelling of time windows and repairs, but they are quite different and have different benefits and limitations.

The I&AB method offers an integrated solution to model the dynamic behaviour of failure and repair processes in an already existing RiskSpectrum PSA model. The method can be used with a graded approach as the user has the freedom to select to which extent repair should be modelled. The method is a good trade-off between static PSA quantifications and dynamic methods.

The enhanced fault/event tree method offers a simple method for modelling non static behaviour with static fault tree/event tree tools and minimizing need for additional software. It is based on a graded approach that can be tailored to the need for additional accuracy and perhaps restrictions in work resources. It enables a simplified representation of dynamic behaviour by considering the repair probability of cutsets and is useful in both small and large existing PSA models.

The simulation-based event tree method offers flexibility and possibility to tailor the modelling approach according to specific modelling needs. It enables explicit modelling of dynamic behaviour of the system and time-dependencies. On the other hand, the method can be quite complex to apply depending on the scope and size of the analysis problem. However, the fictive spent fuel pool model presented in this report is not excessively complex.

The results of different methods were more or less consistent, even though there were some differences in the assumptions and inputs. As expected, repair modelling decreased the fuel damage frequencies significantly compared to the static model that did not include repairs. Time-dependencies related to available times for manual actions and mission times are also significant for the results, though not as important as the repair assumptions.

The three methods offer a comprehensive set of tools applicable to modelling scenarios with long time windows in PSA. The most suitable method depends on the problem and the desired level of realism. The enhanced fault/event tree method is useful when the analyst wants to adjust existing full scope PSA model with some new repairs and time windows without extensive amount of work. With I&AB, Markov-based dynamic failure and repair computation on selected parts can easily be implemented and integrated in a full scope PSA. The simulation-based event tree method gives freedom to define timings of events, integrate deterministic computation and model complex time-dependencies.

Repair modelling was the most determining factor for the spent fuel pool results calculated in this report. Therefore, it would be important to study open issues related to repairs further. An important question is how realistic the used repair assumptions are. The assumption that repair execution time is exponentially distributed has not been validated. It is also important to consider how many repairs can be performed in parallel, and whether repair failures can be dependent. This consideration is particularly relevant for initiating events that affect both the spent fuel pool and the reactor core since several repairs might have to be considered. In addition, repair data should be investigated more. It could be useful to gather repair and failure

data related to different failure mechanisms, because the repair time depends on how the component fails.

Several different definitions of safe (and stable) state can be found from literature. In general, the safe state of a nuclear reactor can e.g. be defined as a plant state, where the reactor has been shut down and is non-pressurized, and removal of decay heat has been secured (STUK, 2018). A spent fuel pool can be considered safe when the cooling is secured. However, it is not always clear how such general definition should be applied in specific scenarios. For example, in the spent fuel pool LOOP scenario, it is not clear whether the recovery of the offsite power is needed or whether operation of the spent fuel pool cooling system with a diesel generator is a safe state. The different methods tested in the pilot studies did all have different definitions of the safe state, why it should be important to investigate whether these differences are of significance to the results. It could be studied whether there is significant additional risk after the spent fuel pool cooling has been established with a diesel generator. Likewise, the general assumption made in reactor PSA that a safe state is reached if the core damage has been avoided for 24 hours can be validated, or if needed revised. Perhaps analysing a 24 hour time window is a good assumption for some initiating events with faster development of the sequence of events (for example transients), whereas for some initiating events (like LOCA or external events for example) the development of events is slower and a longer time window should be studied before one can conclude that the remaining risk is negligible. The Fukushima NPP accidents in 2011 pointed out that it might be relevant to consider longer time windows in some accident scenarios.

In the models that were used in the pilot studies CCFs are modelled for a group of components where some components are in operation and some are in standby. One example is in the PROSAFE model where one MCS represents the initiating event LOOP followed by CCF failure to run for all four SFPC system pumps. One could reflect upon if this MCS is well represented in a dynamic model (as well as the static representation). Right before the initiating event one pump is in operation (functioning) and the other three in standby. A question that arises is, is it then reasonable to model all of them in one CCF group for this sequence? Does the modelling of this sequence contain some significant conservatisms? Since the failure mode is failure to run, the pumps will be started and then fail after some time. The pumps may not fail at the same time, which allows for extra time for repair. And also, since one pump already was running for some time before the initiating event, is the CCF probability significantly lower than if all components were in standby?

These questions above also highlight the issue regarding timings of failures in CCF, as this aspect becomes more important when crediting repair.

For practical use of any of the investigated methods, guidelines for how to practically implement the methods should be developed.

The methods that were used will impact the uncertainties that have to be considered in the PSA. A quantitative (parametric) uncertainty evaluation should be developed since it is likely that crediting repair will increase the parametric uncertainty. Also, some investigation regarding if the identified qualitative uncertainties are large compared to current uncertainties should be considered.

11. Acknowledgements

The work has been co-financed by SAFIR2022 (The Finnish Research Programme on Nuclear Power Plant Safety 2019–2022), Forsmark Kraftgrupp AB, Ringhals AB, Swedish Radiation Safety Authority (SSM), Svensk Kärnbänslehantering (SKB) and Nordic nuclear safety research (NKS).

NKS conveys its gratitude to all organizations and persons who by means of financial support or contributions in kind have made the work presented in this report possible.

12. Disclaimer

13. References

Aldemir, T. (2013). A survey of dynamic methodologies for probabilistic safety assessment of nuclear power plants, Annals of Nuclear Energy, 52, 113-124

American Society of Mechanical Engineers. (2009). ASME PRA standard: ASME/ANS RA-Sa-2009 Standard for Level 1/Large Early Release Frequency Probabilistic Risk Assessment for Nuclear Power Plant Applications.

Authén, S., Holmberg, J.-E., Tyrväinen, T., Zamani, L. (2015). Guidelines for reliability analysis of digital systems in PSA context – Final Report, NKS-330, Nordic nuclear safety research (NKS), Roskilde.

Bouissou, M. & Hernu, O. (2017). *Boolean approximation for calculating the reliability of a very large repairable system with dependencies among components.* Risk, Reliability and Safety: Innovating Theory and Practice – Walls Revie &Bedford (Eds), Ch 217. ISBN 978-1-138-02997-2

Bouissou, M. (2018). *Extensions of the I&AB method for the reliability assessment of the spent fuel pool of EPR.* European Safety and Reliability Conference (ESREL 2018), Trondheim, Norway, 17-21 June, 2018.

Burgazzi, L., Davidovich, N., Meloni, P., Lo Frano, R. (2014). Risk analysis of nuclear power plants against external events, Italian National Agency for New Technologies (ENEA), Report RdS/PAR2013/089, Rome.

EPRI (2018). HRA for Diverse and Flexible Mitigation Strategies (FLEX) and Use of Portable Equipment, TR-3002013018, Electric Power Research Institute, Inc.

EPRI/NRC-RES (2012). Fire Human Reliability Analysis Guidelines – Final Report. NUREG-1921.

Grant, G.M., Poloski, J.P., Luptak, A.J., Gentillon, C.D., Galyean, W.J. (1999). Reliability Study: Emergency Diesel Generator Power System 1987-1993, NUREG/CR-5500, Vol. 5, INEL-95/0035, Idaho National Engineering and Environmental Laboratory, Idaho Falls, ID.

He, X. (2015). Dependencies in HRA. NPSAG Report 41-001: 01.

He, X. (2017). Dependencies in HRA Phase II. LR Report no: 212171_R001 Rev: V1.0.

Holmberg, J.-E. (2019). HRA Methodology for Forsmark NPP and Ringhals NPP. NPSAG REPORT 53-002.

International Atomic Energy Agency. (2010). Development and application of level 1 probabilistic safety assessment for nuclear power plants, specific safety guide series No. SSG-3, Vienna.

International Atomic Energy Agency. (2016). Attributes of full scope level 1 probabilistic safety assessment (PSA) for applications in nuclear power plants. IAEA-TECDOC-1804, Vienna.

International Atomic Energy Agency. (2016). Safety of nuclear power plants: Design, Specific safety requirements No. SSR-2/1 (Rev. 1). IAEA-SSR-2/1, Vienna.

International Atomic Energy Agency. (2019). Deterministic safety analysis for nuclear power plants, Specific safety guide No. SSG-2 (Rev. 1). IAEA-SSG-2, Vienna.

Julius, J. (2019). Advancing FLEX HRA in the USA, September 2019, Jensen Hughes.

Kim, J., Jung, W., & Park, J. (2018). Human Reliability Analysis of the FLEX/MACST Actions deploying Portable Equipment, Transactions of the Korean Nuclear Society Autumn Meeting, Jeosu, Korea, October 25-26, 2018.

Kirimoto, Y., Hirotsu, Y., Nonose, K., & Sasou, K. (2020). Development of a human reliability analysis (HRA) guide for qualitative analysis with emphasis on narratives and models for tasks in extreme conditions. Nuclear Engineering and Technology. https://doi.org/10.1016/j.net.2020.10.004

Kirwan, B., Umbers, I., Edmunds, J., et al. (2008). Quantifying the unimaginable – the case for human performance limiting values. PSAM9-0260. 9th International conference on probabilistic safety assessment and management (PSAM9), Hong Kong, China, 18-23 May, 2008.

Kolaczkowski, A., Forester, J., Lois, E., & Cooper, S. (2005). Good Practices for Implementing Human Reliability Analysis (NUREG-1792). U.S. Nuclear Regulatory Commission.

MacLeod, D. E., Parry, G. W., Sloane, B. D., Lawrence, P., Chan, E. M., & Trifanov, A. V. (2014). Simplified human reliability analysis process for emergency mitigation equipment (EME) deployment. Proc. Probabilistic Safety Assessment and Management Conf. (PSAM12), 22–27.

NEI (2016). Crediting Mitigating Strategies in Risk-Informed Decision Making, NEI 16-06 (Rev 0), August 2016, Nuclear Energy Institute, Washington D. C.

Okkonen, T. (1995). Development of a parametric containment event tree model for a severe BWR accident, STUK-YTO-TR81, Finnish centre for radiation and nuclear safety, Helsinki.

Parry, G.W., et al. (1992). An approach to the analysis of operator actions in probabilistic risk assessment. EPRI TR-100259.

Presley (2017). NEI/NRC Public Meeting on FLEX, November 15, 2017, Electric Power Research Institute, Inc.

Radiation and Nuclear Safety Authority (STUK). (2018). Radiation and nuclear safety authority regulation on the safety of a nuclear power plant. Regulation STUK Y/1/2018, Helsinki.

Ramadan, A., Hasan, R. & Penlington, R. (2018). Zero-dimensional transient model of large-scale cooling ponds using well-mixed approach, Annals of Nuclear Energy, 114, 342-353.

Reisi-Fard, M. (2017, May 30). Assessment of the NEI 16-06, "Crediting Mitigating Strategies in Risk-Informed Decision Making," Guidance for Risk-Informed Changes to Plants Licensing Basis. [NRC Memorandum].

Swain, A.D. & Guttmann, H.E. (1983). Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications. NUREG/CR-1278. Sandia National Laboratories for the U.S. Nuclear Regulatory Commission, Washington, DC.

Swain, A.D. (1987). Accident Sequence Evaluation Program human reliability analysis procedure. NUREG/CR-4772. Sandia National Laboratories for the U.S. Nuclear Regulatory Commission, Washington, DC.

Swedish Radiation Safety Authority (SSM). (2009) The Swedish Radiation Safety Authority's Regulations and General Advice concerning Safety in Nuclear Facilities. SSMFS 2008:1

Tynys, H. (2017). Safety assessment of interim spent nuclear fuel storage [Master's thesis], Lappeenranta University of Technology, Lappeenranta, Finland.

Tyrväinen, T. & Karanta, I. (2019). Dynamic containment event tree modelling techniques and uncertainty analysis, VTT-R-06892-18, VTT Technical Research Centre of Finland Ltd, Espoo, Finland.

Tyrväinen, T., Karanta, I., Kling, T., He, X., Olofsson, F., Bäckström, O., Massaiu, S., Sparre, E., Eriksson, C., Cederhorn, E. & Authén, S. (2020). Prolonged available time and safe state, NKS-432, Nordic nuclear safety research (NKS), Roskilde.

Tyrväinen, T., Silvonen, T. & Mätäsniemi, T. (2016). Computing source terms with dynamic containment event trees. 13th International conference on probabilistic safety assessment and management (PSAM13), Seoul, Korea, 2-7 October, 2016.

United States Nuclear Regulatory Commission. (2005). Good Practices for Implementing Human Reliability Analysis (HRA). NUREG-1792.

United States Nuclear Regulatory Commission. (2005). The SPAR-H Human Reliability Analysis Method. NUREG/CR-6883.

United States Nuclear Regulatory Commission. (2013). Glossary of risk-related terms in support of risk-informed decision making. NUREG-2122, Washington DC.

United States Nuclear Regulatory Commission. (2017). Letter ML17031A269, May 30, 2017.

United States Nuclear Regulatory Commission. (2017). An Integrated Human Event Analysis System (IDHEAS) for Nuclear Power Plant Internal Events At-Power Application. NUREG-CR 2199.

VTT Technical Research Centre of Finland Ltd (2020). FinPSA – Tool for promoting safety and reliability. https://www.simulationstore.com/finpsa (link accessed 20.11.2020)

Wu, X., Li, W., Zhang, Y., Tian, W., Su, G. & Qiu, S. (2014). Analysis of the loss of pool cooling accident in a PWR spent fuel pool with MAAP5, Annals of Nuclear Energy, 72, 198-213.

Xing, J., Kichline, M., Hughey, J., & Humberstone, M. (2019, May 28). The use of expert judgment to support Human Reliability Analysis of implementing FLEX equipment. PSA 2019, Charleston, SC.

Zhang, Z.W., Du, Y. & Liang, K.S. (2017). Advanced modeling techniques of a spent fuel pool with both RELAP5 and MELCOR and associated accident analysis, Annals of Nuclear Energy, 110, 160-170.

Appendix A: Detailed results from simulation-based event tree analysis

Tables 60 and 62 present the minimal cut sets selected for SBET analysis in the transient and LOOP cases. The results of the SBET analyses are presented in Tables 61 and 63. In the result tables, 'Seq' column indicates the corresponding sequence in the simulation-based event tree. 'IE MTTR' column indicated the mean time to repair the spent fuel pool cooling (even though in the LOOP case it is not exactly the initiating event that is repaired). The static frequency is the frequency calculated from the static model, and the dynamic frequencies are calculated based on the SBET analysis. For transient, dynamic results are presented without considering repairs of the make-up systems (NR), with one make up system repair (1R) and with two make-up system repairs (2R). For loss of offsite power, dynamic results are presented without considering repair of make-up system 1 (NR) and with a repair of make-up system 1 (R).

Table 60: Minimal cut sets used for SBET analysis in the transient case.

Mc_num	Freq	Basic event names				
1	3.73E-09	SFPC_P1____I___D	CCF-SFPC-PM--A-BCD	CCF-SFPM1-PM-A-AB	SFPMU:2_P1_____A	
2	3.67E-09	SFPC_P1____I___D	ACP__DG102_FLEX2___D	CCF-SFPC-PM--A-BCD	CCF-SFPM1-PM-A-AB	
3	3.36E-09	SFPC_P1____I___D	CCF-SFPM1-PM-A-AB	SFPC_MANSTART_H	SFPMU:2_P1_____A	
4	3.31E-09	SFPC_P1____I___D	ACP__DG102_FLEX2___D	CCF-SFPM1-PM-A-AB	SFPC_MANSTART_H	
5	2.47E-09	SFPC_P1____I___D	CCF-SFPC-PM--A-BCD	SFPMU:1_P1_____A	SFPMU:1_P2_____A	SFPMU:2_P1_____A
6	2.43E-09	SFPC_P1____I___D	ACP__DG102_FLEX2___D	CCF-SFPC-PM--A-BCD	SFPMU:1_P1_____A	SFPMU:1_P2_____A
7	2.23E-09	SFPC_P1____I___D	SFPC_MANSTART_H	SFPMU:1_P1_____A	SFPMU:1_P2_____A	SFPMU:2_P1_____A
8	2.19E-09	SFPC_P1____I___D	ACP__DG102_FLEX2___D	SFPC_MANSTART_H	SFPMU:1_P1_____A	SFPMU:1_P2_____A
9	1.51E-09	SFPC_P1____I___D	CCF-SFPM1-PM-A-AB	SFPC_DIAG_____H	SFPMU:2_P1_____A	
10	1.49E-09	SFPC_P1____I___D	ACP__DG102_FLEX2___D	CCF-SFPM1-PM-A-AB	SFPC_DIAG_____H	
11	1.00E-09	SFPC_P1____I___D	SFPC_DIAG_____H	SFPMU:1_P1_____A	SFPMU:1_P2_____A	SFPMU:2_P1_____A
12	9.85E-10	SFPC_P1____I___D	ACP__DG102_FLEX2___D	SFPC_DIAG_____H	SFPMU:1_P1_____A	SFPMU:1_P2_____A
13	8.85E-10	SFPC_P1____I___D	CCF-SFPC-PM--A-BCD	SFPMU:1_MANSTART_H	SFPMU:2_P1_____A	
14	8.70E-10	SFPC_P1____I___D	ACP__DG102_FLEX2___D	CCF-SFPC-PM--A-BCD	SFPMU:1_MANSTART_H	
15	7.98E-10	SFPC_P1____I___D	SFPC_MANSTART_H	SFPMU:1_MANSTART_H	SFPMU:2_P1_____A	
16	7.84E-10	SFPC_P1____I___D	ACP__DG102_FLEX2___D	SFPC_MANSTART_H	SFPMU:1_MANSTART_H	
17	7.47E-10	SFPC_H1____I___X	CCF-SFPC-PM--A-BCD	CCF-SFPM1-PM-A-AB	SFPMU:2_P1_____A	
18	7.35E-10	SFPC_H1____I___X	ACP__DG102_FLEX2___D	CCF-SFPC-PM--A-BCD	CCF-SFPM1-PM-A-AB	
19	6.73E-10	SFPC_H1____I___X	CCF-SFPM1-PM-A-AB	SFPC_MANSTART_H	SFPMU:2_P1_____A	
20	6.62E-10	SFPC_H1____I___X	ACP__DG102_FLEX2___D	CCF-SFPM1-PM-A-AB	SFPC_MANSTART_H	
21	4.95E-10	SFPC_H1____I___X	CCF-SFPC-PM--A-BCD	SFPMU:1_P1_____A	SFPMU:1_P2_____A	SFPMU:2_P1_____A
22	4.87E-10	SFPC_H1____I___X	ACP__DG102_FLEX2___D	CCF-SFPC-PM--A-BCD	SFPMU:1_P1_____A	SFPMU:1_P2_____A
23	4.73E-10	SFPC_P1____I___D	CCF-SFPC-PM--A-BCD	CCF-SFPM1-PM-A-AB	SFPMU:2_MANSTART_H	
24	4.46E-10	SFPC_H1____I___X	SFPC_MANSTART_H	SFPMU:1_P1_____A	SFPMU:1_P2_____A	SFPMU:2_P1_____A
25	4.39E-10	SFPC_H1____I___X	ACP__DG102_FLEX2___D	SFPC_MANSTART_H	SFPMU:1_P1_____A	SFPMU:1_P2_____A
26	4.27E-10	SFPC_P1____I___D	ACP__DG102_FLEX2___A	CCF-SFPC-PM--A-BCD	CCF-SFPM1-PM-A-AB	
27	4.26E-10	SFPC_P1____I___D	CCF-SFPM1-PM-A-AB	SFPC_MANSTART_H	SFPMU:2_MANSTART_H	
28	3.85E-10	SFPC_P1____I___D	ACP__DG102_FLEX2___A	CCF-SFPM1-PM-A-AB	SFPC_MANSTART_H	
29	3.83E-10	SFPC_P1____I___D	CCF-SFPC-PM--A-BCD	SFPMU:1_DIAG___H	SFPMU:2_DIAG___HD	
30	3.59E-10	SFPC_P1____I___D	SFPC_DIAG_____H	SFPMU:1_MANSTART_H	SFPMU:2_P1_____A	
31	3.53E-10	SFPC_P1____I___D	ACP__DG102_FLEX2___D	SFPC_DIAG_____H	SFPMU:1_MANSTART_H	
32	3.45E-10	SFPC_P1____I___D	SFPC_MANSTART_H	SFPMU:1_DIAG___H	SFPMU:2_DIAG___HD	

Table 61: SBET analysis results for top minimal cut sets in the transient case.

MCS	Seq	IE MTTR (hour)	Static Freq (1/year)	Dynamic Freq NR (1/year)	Dynamic Freq 1R (1/year)	Dynamic Freq 2R (1/year)
Total			3.95E-8	1.50E-8	1.42E-9	8.83E-10
1	8	32	3.73E-9	1.75E-9	1.38E-10	8.23E-11
2	4	32	3.67E-9	1.21E-9	6.86E-11	2.66E-11
3	8	32	3.36E-9	1.58E-9	1.24E-10	7.42E-11
4	4	32	3.31E-9	1.09E-9	6.19E-11	2.40E-11
5	17	32	2.47E-9	1.16E-9	9.08E-11	5.32E-11
6	13	32	2.43E-9	8.02E-10	4.52E-11	1.68E-11
7	17	32	2.23E-9	1.05E-9	8.19E-11	4.80E-11
8	13	32	2.19E-9	7.23E-10	4.08E-11	1.51E-11
9	8	32	1.51E-9	7.10E-10	5.58E-11	3.33E-11
10	4	32	1.49E-9	4.92E-10	2.78E-11	1.08E-11
11	17	32	1.00E-9	4.69E-10	3.67E-11	2.15E-11
12	13	32	9.85E-10	3.25E-10	1.83E-11	6.81E-12
13	26	32	8.85E-10	4.16E-10	4.38E-11	1.99E-11
14	22	32	8.70E-10	2.88E-10	2.29E-11	3.30E-12
15	26	32	7.98E-10	3.75E-10	3.95E-11	1.80E-11
16	22	32	7.84E-10	2.59E-10	2.07E-11	2.97E-12
17	8	19	7.47E-10	2.10E-10	1.65E-11	9.77E-12
18	4	19	7.35E-10	7.71E-11	4.70E-12	2.03E-12
19	8	19	6.73E-10	1.89E-10	1.49E-11	8.80E-12
20	4	19	6.62E-10	6.94E-11	4.23E-12	1.83E-12
21	17	19	4.95E-10	1.39E-10	1.09E-11	6.32E-12
22	13	19	4.87E-10	5.10E-11	3.10E-12	1.27E-12
23	10	32	4.73E-10	2.24E-10	1.79E-11	1.01E-11
24	17	19	4.46E-10	1.25E-10	9.85E-12	5.69E-12
25	13	19	4.39E-10	4.60E-11	2.79E-12	1.15E-12
26	6	32	4.27E-10	1.93E-10	1.51E-11	8.60E-12
27	10	32	4.26E-10	2.01E-10	1.62E-11	9.13E-12
28	6	32	3.85E-10	1.74E-10	1.36E-11	7.75E-12
29	-	32	3.83E-10	1.81E-10	1.81E-10	1.81E-10
30	26	32	3.59E-10	1.69E-10	1.78E-11	8.09E-12
31	22	32	3.53E-10	1.17E-10	9.30E-12	1.34E-12
32	-	32	3.45E-10	1.63E-10	1.63E-10	1.63E-10

Table 62: Minimal cut sets used for SBET analysis in the LOOP case.

Mc_num	Freq	Basic event names				
1	2.36E-08	!IE-LOOP	ACN10GT001_____A	ACP-DG--------D-ALL	SFPMU:2_P1_____A	
2	2.32E-08	!IE-LOOP	ACN10GT001_____A	ACP-DG--------D-ALL	ACP__DG102_FLEX2___D	
3	1.09E-08	!IE-LOOP	ACN10GT001_____M	ACP-DG--------D-ALL	SFPMU:2_P1_____A	
4	1.07E-08	!IE-LOOP	ACN10GT001_____M	ACP-DG--------D-ALL	ACP__DG102_FLEX2___D	
5	2.99E-09	!IE-LOOP	ACN10GT001_____A	ACP-DG--------D-ALL	SFPMU:2_MANSTART___H	
6	2.74E-09	!IE-LOOP	ACN10GT001_____A	ACP-DG--------A-ALL	SFPMU:2_P1_____A	
7	2.70E-09	!IE-LOOP	ACN10GT001_____A	ACP-DG--------A-ALL	ACP__DG102_FLEX2___D	
8	2.70E-09	!IE-LOOP	ACN10GT001_____A	ACP-DG--------D-ALL	ACP__DG102_FLEX2___A	
9	2.03E-09	!IE-LOOP	ACN10GT001_____A	ACP-DG--------D-3AC	SFPC_P2_____A	SFPMU:2_P1_____A
10	2.00E-09	!IE-LOOP	ACN10GT001_____A	ACP-DG--------D-3AD	ACP10DG001_____D	SFPMU:2_P1_____A
11	2.00E-09	!IE-LOOP	ACN10GT001_____A	ACP-DG--------D-3AA	ACP40DG001_____D	SFPMU:2_P1_____A
12	2.00E-09	!IE-LOOP	ACN10GT001_____A	ACP-DG--------D-3AB	ACP30DG001_____D	SFPMU:2_P1_____A
13	2.00E-09	!IE-LOOP	ACN10GT001_____A	ACP-DG--------D-3AC	ACP20DG001_____D	SFPMU:2_P1_____A
14	2.00E-09	!IE-LOOP	ACN10GT001_____A	ACP-DG--------D-3AC	ACP__DG102_FLEX2___D	SFPC_P2_____A
15	1.97E-09	!IE-LOOP	ACN10GT001_____A	ACP-DG--------D-3AB	ACP30DG001_____D	ACP__DG102_FLEX2___D
16	1.97E-09	!IE-LOOP	ACN10GT001_____A	ACP-DG--------D-3AD	ACP10DG001_____D	ACP__DG102_FLEX2___D
17	1.97E-09	!IE-LOOP	ACN10GT001_____A	ACP-DG--------D-3AC	ACP20DG001_____D	ACP__DG102_FLEX2___D
18	1.97E-09	!IE-LOOP	ACN10GT001_____A	ACP-DG--------D-3AA	ACP40DG001_____D	ACP__DG102_FLEX2___D
19	1.38E-09	!IE-LOOP	ACN10GT001_____M	ACP-DG--------D-ALL	SFPMU:2_MANSTART___H	
20	1.26E-09	!IE-LOOP	ACN10GT001_____M	ACP-DG--------A-ALL	SFPMU:2_P1_____A	
21	1.24E-09	!IE-LOOP	ACN10GT001_____M	ACP-DG--------A-ALL	ACP__DG102_FLEX2___D	
22	1.24E-09	!IE-LOOP	ACN10GT001_____M	ACP-DG--------D-ALL	ACP__DG102_FLEX2___A	
23	9.37E-10	!IE-LOOP	ACN10GT001_____M	ACP-DG--------D-3AC	SFPC_P2_____A	SFPMU:2_P1_____A
24	9.22E-10	!IE-LOOP	ACN10GT001_____M	ACP-DG--------D-3AA	ACP40DG001_____D	SFPMU:2_P1_____A
25	9.22E-10	!IE-LOOP	ACN10GT001_____M	ACP-DG--------D-3AC	ACP20DG001_____D	SFPMU:2_P1_____A
26	9.22E-10	!IE-LOOP	ACN10GT001_____M	ACP-DG--------D-3AD	ACP10DG001_____D	SFPMU:2_P1_____A
27	9.22E-10	!IE-LOOP	ACN10GT001_____M	ACP-DG--------D-3AC	ACP__DG102_FLEX2___D	SFPC_P2_____A
28	9.22E-10	!IE-LOOP	ACN10GT001_____M	ACP-DG--------D-3AB	ACP30DG001_____D	SFPMU:2_P1_____A
29	9.07E-10	!IE-LOOP	ACN10GT001_____M	ACP-DG--------D-3AC	ACP20DG001_____D	ACP__DG102_FLEX2___D
30	9.07E-10	!IE-LOOP	ACN10GT001_____M	ACP-DG--------D-3AA	ACP40DG001_____D	ACP__DG102_FLEX2___D
31	9.07E-10	!IE-LOOP	ACN10GT001_____M	ACP-DG--------D-3AB	ACP30DG001_____D	ACP__DG102_FLEX2___D
32	9.07E-10	!IE-LOOP	ACN10GT001_____M	ACP-DG--------D-3AD	ACP10DG001_____D	ACP__DG102_FLEX2___D

Table 63: SBET analysis results for top minimal cut sets in the LOOP case.

MCS	Seq	IE MTTR (hour)	Static Freq (1/year)	Dynamic Freq NR (1/year)	Dynamic Freq R (1/year)
Total			1.14E-7	7.99E-10	1.11E-10
1	7	15	2.36E-8	2.52E-10	3.39E-11
2	3	15	2.32E-8	7.29E-11	9.15E-12
3	7	15	1.09E-8	1.16E-10	1.56E-11
4	3	15	1.07E-8	3.36E-11	4.22E-12
5	9	15	2.99E-9	3.68E-11	9.15E-12
6	7	11	2.74E-9	1.57E-11	1.75E-12
7	3	11	2.70E-9	3.17E-12	3.28E-13
8	5	15	2.70E-9	2.75E-11	3.60E-12
9	7	15	2.03E-9	2.17E-11	2.91E-12
10	7	15	2.00E-9	2.14E-11	2.87E-12
11	7	15	2.00E-9	2.14E-11	2.87E-12
12	7	15	2.00E-9	2.14E-11	2.87E-12
13	7	15	2.00E-9	2.14E-11	2.87E-12
14	3	15	2.00E-9	6.29E-12	7.89E-13
15	3	15	1.97E-9	6.19E-12	7.77E-13
16	3	15	1.97E-9	6.19E-12	7.77E-13
17	3	15	1.97E-9	6.19E-12	7.77E-13
18	3	15	1.97E-9	6.19E-12	7.77E-13
19	9	15	1.38E-9	1.70E-11	4.22E-12
20	7	11	1.26E-9	7.24E-12	8.04E-13
21	3	11	1.24E-9	1.46E-12	1.51E-13
22	5	15	1.24E-9	1.26E-11	1.65E-12
23	7	15	9.37E-10	1.00E-11	1.35E-12
24	7	15	9.22E-10	9.85E-12	1.32E-12
25	7	15	9.22E-10	9.85E-12	1.32E-12
26	7	15	9.22E-10	9.85E-12	1.32E-12
27	3	15	9.22E-10	2.90E-12	3.64E-13
28	7	15	9.22E-10	9.85E-12	1.32E-12
29	3	15	9.07E-10	2.85E-12	3.58E-13
30	3	15	9.07E-10	2.85E-12	3.58E-13
31	3	15	9.07E-10	2.85E-12	3.58E-13
32	3	15	9.07E-10	2.85E-12	3.58E-13

Sensitivity analysis

The analysis includes many assumptions on issues that are uncertain, such as probability distributions of time delays and start times of specific actions. Therefore, it is important to study the sensitivity of the results to different assumptions. The sensitivity analyses are performed with a smaller number of simulations (50000 for LOOP and 20000 for transient), but different cases are analysed based on the same random numbers so that natural variation has little impact on relative results. The analyses are performed with all the repairs that were modelled (two make-up system repairs for transient and one repair of make-up system 1 for LOOP)

Repair of the spent fuel pool cooling

The repair of the spent fuel pool cooling was assumed to be started at the time of the failure, and exponential distribution was used for the repair time. The repair time of the spent fuel pool cooling system is quite important variable, because it impacts the probability to repair the cooling before boiling and the mission times of both make-up systems. It creates a dependency between the failure probabilities of the make-up systems, including failures after repairs.

Table 64 presents the sensitivity analysis cases and results. The start time of the repair process and the distribution of the repair time are varied in these cases. The fuel damage frequency is presented for both LOOP and transient, as well as the percentage compared to the baseline result.

Table 64: Sensitivity analyses for the repair of the spent fuel pool cooling.

Case	LOOP	Transient
Baseline	1.12E-10	8.80E-10
MTTR is 40 h	-	1.04E-9 (118%)
MTTR is 30 h	8.85E-10 (791%)	-
MTTR is 20 h	2.74E-10 (244%)	-
MTTR is 10 h	3.46E-11 (31%)	4.37E-10 (50%)
MTTR is 5 h	2.45E-12 (2.2%)	-
Repair time is fixed to the 95th percentile of the exponential distribution	4.83E-10 (432%)	1.82E-9 (207%)
Repair starts 12 h after the failure	2.51E-10 (224%)	1.14E-9 (129%)
Repair starts 24 h after the failure	5.65E-10 (505%)	1.53E-9 (174%)
Lognormal distribution for repair time, error factor = 2, mean = baseline value	2.68E-11 (24%)	1.00E-9 (114%)
Lognormal distribution for repair time, error factor = 5, mean = baseline value	2.41E-10 (215%)	8.40E-10 (96%)

It can be seen that variations in the probability distribution of the repair change the results significantly, particularly when the mean time is changed. The shape and the tail of the distribution are also important. The sensitivity is greater in the LOOP case than in the transient case. There are a few reasons for this:

- When the repair time distribution has a longer tail, the available time to repair the diesel generator is more likely exceeded, and then make-up system 1 cannot be used in the LOOP case. There is no similar effect in the transient case, because the repair time of the spent fuel pool cooling has no impact on the operation of the make-up systems.
- Diagnosis failures are important in the transient results, and the impact of the repair time distribution is small on the minimal cut sets with diagnosis failures.
- The repair time of the spent fuel pool cooling is on average shorter in the LOOP case, and the cooling is repaired more likely before boiling. Variations in the repair success probability are larger because of that in the LOOP case.

The results on the use of lognormal distribution are quite opposite in the LOOP and transient cases. When the error factor is larger, the repair time distribution is wider. In the LOOP case, the wider distribution increases the result significantly, because the available time to repair the diesel generator is exceeded much more likely. In the transient case, the result decreases slightly due to wider distribution, because the probability to repair the spent fuel pool cooling before boiling increases.

The examination of the simulation results also reveals that the largest sensitivities are not related to mission times, but on the impacts discussed above.

Manual actions on make-up systems

In this section, the sensitivity of the results to the start times of the make-up systems and parameters related to that is studied. There is uncertainty related to the probability distributions of the manual actions, but also related to when the diagnosis actions start. It was assumed that

the diagnosis for the first make-up system starts when boiling starts, and the diagnosis for the second make-up system starts when the first make-up system fails. Another possibility would be e.g. to perform the actions for both make-up systems in parallel. The diagnosis actions were modelled using lognormal distributions estimated based on HRA information. The distributions are quite uncertain since they are not based on real diagnosis time data.

The sensitivity analysis cases and results are presented in Table 65. It needs to be noted that diagnosis or execution failure probabilities are not varied here, but only the distributions of the make-up system start times, even though the changes in the distributions would also change the failure probabilities in reality. The results are not very sensitive to the make-up system start times, but those have some significance nevertheless. When execution times are assumed ten times longer, the results increase significantly, because the available times to perform repairs decrease and mission times increase. Sensitivity is smaller in the LOOP case, because the start of make-up system 1 requires also the diesel generator repair, and therefore, the normal start actions have smaller significance.

Table 65: Sensitivity analyses for manual actions on make-up systems.

Case	LOOP	Transient
Baseline	1.12E-10	8.80E-10
Mean diagnosis times are 4 h	1.25E-10 (111%)	1.00E-9 (114%)
Mean diagnosis times are 1 h	1.10E-10 (98%)	8.35E-10 (95%)
Error factors for diagnosis action durations are 20	1.19E-10 (106%)	8.89E-10 (101%)
Start executions of make-up systems last 10 times longer	1.85E-10 (165%)	2.19E-9 (250%)
Make-up systems can be started immediately	1.12E-10 (100%)	7.69E-10 (87%)
Diagnosis for both make-up systems starts when boiling starts[2]	1.10E-10 (99%)	8.40E-10 (96%)

Repairs of the make-up systems

The sensitivity of the results to make-up system repair assumptions is studied in Table 66. The results are somewhat sensitive to the MTTR values. The sensitivity is slightly larger in the transient case.

Table 66: Sensitivity analysis for make-up system repair assumptions.

Case	LOOP	Transient
Baseline	1.12E-10	8.80E-10
MTTR values are doubled	2.45E-10 (219%)	2.97E-9 (338%)
MTTR values are halved	6.79E-11 (61%)	4.12E-10 (47%)
Repairs start immediately after failure[3]	-	7.55E-10 (86%)

In the baseline case for transient, it was assumed that the repair of make-up system 1 starts only after make-up system 2 has failed, and the repair of make-up system 2 starts only after make-up system 1 has failed again. These assumptions were revised for a sensitivity case so that the repairs start immediately after failure. The result decreased 14%, i.e. it makes some difference whether the repairs are assumed consecutive or parallel.

[2] In the transient case, if the diagnosis and execution for make-up system 2 are ready before make-up system 1 has failed, it is assumed that make-up system 2 is started when make-up system 1 fails. In the LOOP case, it is the other way around, except that also diesel generator repair is needed so that make-up system 1 can be started.

[3] If the repair of make-up system 1 is ready before make-up system 2 has failed, it is assumed that make-up system 1 is started again when make-up system 2 fails, and vice versa when both systems are repaired.

Spent fuel pool conditions

In this section, the sensitivity of the results to the parameters used in the computation of spent fuel pool conditions and time windows is studied. In the baseline case, the time to boiling is 24 hours, the time to fuel damage is 72 hours, and the time to increase the water level from fuel level to normal is 24 hours.

The sensitivity analysis cases and results are presented in Table 67. The failure probabilities of manual actions to start the make-up systems were not changed, even when the time to fuel damage was changed. Still, the largest sensitivity is related to the time to fuel damage, because it has a large impact on the repair probabilities. Sensitivity related to the time to boiling is also significant, because the probability to repair the spent fuel pool cooling before boiling depends on it. Sensitivities related to temperature increase and water level increase parameters are smaller.

Table 67: Sensitivity analysis for spent fuel pool conditions and time windows.

Case	**LOOP**	**Transient**
Baseline	1.12E-10	8.80E-10
The spent fuel pool cooling rate is doubled	1.07E-10 (96%)	8.51E-10 (97%)
The spent fuel pool cooling rate is halved	1.17E-10 (104%)	9.14E-10 (104%)
Time to increase water level from fuel level to normal is 12 h	1.02E-10 (91%)	8.69E-10 (99%)
Time to increase water level from fuel level to normal is 48 h	1.34E-10 (119%)	9.01E-10 (102%)
Time to boiling is 12 h	2.64E-10 (236%)	1.21E-9 (138%)
Time to boiling is 48 h	2.10E-11 (19%)	5.70E-10 (65%)
Time to fuel damage from the start of boiling is 36 h	6.25E-10 (558%)	3.28E-9 (373%)
Time to fuel damage from the start of boiling is 144 h	4.03E-11 (36%)	3.99E-10 (45%)

Appendix B: Scripts of the simulation-based event trees

The scripts of the SBETs for LOOP and transient are presented in the following. The common section containing global variables and functions is presented last.

Initial section for LOOP

```
$ Most global variables are defined in the common section.

$ Random variables for timing determination
real rr, r11, r12

$ Variable values that are collected to results
Collect t_mission2, t_mu1, t_mu2, t_start1, t_start2, t_fail2, t_repair

$ Routine init is executed first
routine init
  FD = false

  $ Boiling conditions are the starting point for dynamic analysis.
  Temperature = BoilingTemp
  WLevel = InitWLevel

  $ Boiling time is calculated.
  boiltime = (BoilingTemp-NormalTemp)/HeatUpRate

  $ Mean time to repair a diesel generator.
  sfpcmrt = 15

  $ Probability that the repair is not performed before boiling.
  BINFREQ = EXP(-boiltime/sfpcmrt)

  $ Repair time of the spent fuel pool cooling (DG) from exponential distribution.
  $ Time point 0 is when the boiling starts.
  rr = 1-random()*BINFREQ
  t_repair = -LN(1-rr)*sfpcmrt-boiltime

  $ Make up system 1 start time is determined.
  r11 = random()
  r12 = random()
  t_start1 = icumul(MU1D,r11)+r12+0.5

  $ Initialization
  t_mu1 = 0
  mttr1 = 0
  mttr2 = 0
  rr2 = random()
  MU1EFAIL = false
  MU2EFAIL = false
return


routine finish
  $ No final calculations in this model.
return

$ Routine binner is used to categorise accident sequences based on e.g. Boolean variables.
Class FD
routine binner active
(true, 'FD'),
(*,    'OK')
return
```

MU:2_HFE for LOOP

```
$ Local variables
real prob, r2, r, t_avail, t_diag, t_exe

routine init
  r = random()   $ Random value between 0 and 1
  r2 = random()
```

```
return


$ Make up 2 start is performed successfully
function nil OK
  $ Time available to start make up system 2.
  t_avail = (WLevel-FuelLevel)/BoilingRate

  $ The execution time of the make up system 2 start is drawn from uniform distribution.
  t_exe = 2*r2+1

  $ The diagnosis time of the make up system 2 start is drawn from lognormal distribution.
  r = r*cumul(MU2D,t_avail-t_exe)
  t_diag = icumul(MU2D,r)

  $ The start time of make up system 2.
  t_start2 = t_diag+t_exe

  $ The spent fuel pool water level is updated.
  WLevel = WLevel-t_start2*BoilingRate
return nil


$ Execution fails
function real EFAIL
  $ Time available to start make up system 2.
  t_avail = (WLevel-FuelLevel)/BoilingRate

  $ The execution time of make up system 2 start is drawn from uniform distribution.
  t_exe = 2*r2+1

  $ The diagnosis time of make up system 2 start is drawn from lognormal distribution.
  r = r*cumul(MU2D,t_avail-t_exe)
  t_diag = icumul(MU2D,r)

  $ Time when execution attempt is finished.
  t_start2 = t_diag+t_exe

  $ The spent fuel pool water level is updated.
  WLevel = WLevel-t_start2*BoilingRate

  $ Execution failure probability
  prob = P_EXE2

  t_mu2 = t_start2

  MU2EFAIL = true
return prob
```

MU:2_P1 for LOOP

```
real prob

routine init

return


function nil OK
  $ Nil-function returns 1-prob
return nil


function real FTS
  prob = P_PUMP_FTS

  t_mu2 = t_start2

  mttr1 = MTTR_pump
return prob
```

DG102_FLEX for LOOP

```
$ Local variables
```

```
real prob, r, t_earliest, fr

routine init
  r = random()    $ Random value between 0 and 1
return


function nil OK
  $ Nil-function returns 1-prob
return nil

$ Failure to run
function real FTR
  fr = FR_DG   $ Failure rate

  $ The mission time is tentatively calculated as the time to reach normal water level.
  t_mission2 = (InitWLevel-WLevel)/LevelIncRate

  $ Given the repair time of the spent fuel pool cooling system,
  $ the earliest allowed failure time is calculated.
  $ The EarliestTime function is defined in the common section.
  t_earliest = EarliestTime(Temperature,t_repair-t_start2)

  $ If the earliest allowed failure time based on the repair of the spent fuel pool cooling
  $ system is larger than the time to reach the normal water level, the mission time is
  $ determined based on that.
  if t_mission2 < t_earliest then t_mission2 = t_earliest

  $ The diesel generator failure probability is calculated.
  prob = 1-exp(-fr*t_mission2)

  $ The failure time of the diesel generator is determined.
  t_fail2 = t_mission2*r

  $ The spent fuel pool conditions are updated based on the failure time.
  $ The Cooldown function is defined in the common section.
  Temperature = Cooldown(Temperature,t_fail2)
  WLevel = WLevel+LevelIncRate*t_fail2
  if WLevel > InitWLevel then WLevel = InitWLevel

  $ The total time the make up 2 system was used.
  t_mu2 = t_start2+t_fail2

  $ Mean time to repair for repair modelling of this diesel generator.
  mttr1 = MTTR_DG_FTR
return prob

$ Failure to start
function real FTS
  prob = P_DG_FTS

  t_mu2 = t_start2

  mttr1 = MTTR_DG_FTS
return prob
```

MU_Repair for LOOP

```
$ Local variables
real prob, t_boiling, r, r1, r2, r3, t_earliest, t_start, t_mission, t_avail, p_fts, t_fail, mttr,
     p_ftr, t_st, p_exe, fr

routine init
  r = random()    $ Random value between 0 and 1
  r1 = random()
  r2 = random()
  r3 = random()
return


function nil OK
  $ Nil-function returns 1-prob
return nil
```

```
$ Failure to repair the diesel generator supplying the SFPCS in time or
$ bring to water level back to normal by make up system 1.
$ Repair of make up system 2 is also modelled, when it is needed to buy more time.
$ This function essentially calculates conditional probability for fuel damage
$ after the failure of make up system 2.
function real FAIL
 $ Time available for repair.
 t_boiling = (BoilingTemp-Temperature)/HeatUpRate
 t_avail = t_boiling + (WLevel-FuelLevel)/BoilingRate

 p_fts = P_ALL_FTS   $ Failure to start probability
 p_exe = P_EXE1      $ Make up 1 start execution failure probability
 fr = FR_DG+FR_PUMP  $ Failure rate

 $ If the SFPC (DG) repair or make up 1 start does not come before fuel damage,
 $ repair of make up 2 can be performed to buy more time.
 if (t_avail < t_repair-t_mu2) or (t_avail < t_start1) then
 begin
  if MU2EFAIL then
  begin
   prob = 1   $ If make up 2 start execution failed, repair is not possible.
  end
  else
  begin
   $ Three failure modes of make up system 2 are evaluated in the following:
   $ Failure to repair, failure to start and failure to run.
   $ The probabilities of the failure modes are summed.

   $ Failure mode 1: repair failure
   $ -------------------------------

   $ The repair failure probability is calculated assuming exponential distribution
   $ for the repair time.
   prob = EXP(-t_avail/mttr1)

   $ The repair time is drawn from exponential distribution.
   r1 = r1*(1-EXP(-t_avail/mttr1))
   t_start = -LN(1-r1)*mttr1

   $ The spent fuel pool conditions are updated depending on
   $ if the system is started before or after boiling.
   if t_start < t_boiling then
   begin
    Temperature = Temperature+HeatUpRate*t_start
   end
   else
   begin
    Temperature = BoilingTemp
    WLevel = WLevel-(t_start-t_boiling)*BoilingRate
   end

   $ Failure mode 2: failure to start
   $ ---------------------------------

   $ Failure to start probability is added.
   prob = prob+(1-prob)*p_fts

   $ Failure mode 3: failure to run
   $ -------------------------------

   $ The mission time is tentatively calculated as the time to reach normal water level.
   t_mission = (InitWLevel-WLevel)/LevelIncRate

   $ Given the repair time of the spent fuel pool cooling system,
   $ the earliest allowed failure time is calculated.
   $ The EarliestTime function is defined in the common section.
   t_earliest = EarliestTime(Temperature,t_repair-t_start-t_mu1-t_mu2)

   $ If the earliest allowed failure time based on the repair of the spent fuel pool cooling
   $ system is larger than the time to reach the normal water level, the mission time is
   $ determined based on that.
   if t_mission < t_earliest then t_mission = t_earliest

   $ Failure to run probability after repair.
   p_ftr = 1-exp(-fr*t_mission)
```

```
$ The failure time of the diesel generator is determined.
t_fail = t_mission*r

$ The spent fuel pool conditions are updated based on the failure time.
$ The Cooldown function is defined in the common section.
Temperature = Cooldown(Temperature,t_fail)
WLevel = WLevel+LevelIncRate*t_fail
if more(WLevel,InitWLevel) then WLevel = InitWLevel

$ Given that make up 2 has operated some time, the available time to repair
$ the diesel generator (for SFPCS) is calculated.
t_boiling = (BoilingTemp-Temperature)/HeatUpRate
t_avail = t_boiling + (WLevel-FuelLevel)/BoilingRate

$ If boiling is going on or starts before the diesel generator repair.
$ If not, SFPCS operation can be started and safe state is reached.
if (WLevel < InitWLevel) or (t_boiling < t_repair-t_mu2-t_start-t_fail) then
begin
 $ If the repair comes before fuel damage.
 if t_avail > t_repair-t_mu2-t_start-t_fail then
 begin
  $ If make up system 1 can be started before fuel damage.
  if t_avail > t_start1 then
  begin
   $ Three failure modes of make up system 1 are evaluated in the following:
   $ start execution failure, failure to start and failure to run.
   $ In each case, also repair possibility is considered.
   $ The probabilities of the failure modes (including repair failures) are summed.

   $ The spent fuel pool conditions are updated depending on
   $ if the system is started before or after boiling.
   if t_start1 < t_boiling then
   begin
    Temperature = Temperature+HeatUpRate*t_start1
   end
   else
   begin
    Temperature = BoilingTemp
    WLevel = WLevel-(t_start1-t_boiling)*BoilingRate
   end

   $ Failure mode 1: start execution failure
   $ ----------------------------------------

   $ Probability that make up 1 start execution fails
   $ and FLEX diesel generator repair fails.
   prob = prob+(1-prob)*p_ftr*p_exe*RepairFail(Temperature, WLevel, MTTR_DG_FTR, t_start1)

   $ Failure mode 2: failure to start
   $ --------------------------------

   $ Start time for make up system 1 is determined.
   t_st = t_repair-t_mu2-t_start-t_fail
   if t_st < t_start1 then t_st = t_start1

   $ The spent fuel pool conditions are updated.
   if t_start1 > t_boiling then
   begin
    WLevel = WLevel-(t_st-t_start1)*BoilingRate
   end
   else
   begin
    WLevel = WLevel-(t_st-t_boiling)*BoilingRate
   end
   Temperature = BoilingTemp

   $ MTTR depends on whether pump or DG fails to start.
   if r2 < CP_DG_FTS then mttr = MTTR_DG_FTS else mttr = MTTR_pump

   $ Probability that make up 1 fails to start and its repair fails.
   prob = prob+(1-prob)*p_ftr*p_fts*RepairFail(Temperature, WLevel, mttr, t_st)

   $ Failure mode 3: failure to run
   $ ------------------------------

   $ Mission time for make up system 1 is the time to normal water level.
```

```
        t_mission = (InitWLevel-WLevel)/LevelIncRate

        $ The failure time of the diesel generator is determined.
        t_fail = t_mission*r3

        $ The spent fuel pool conditions are updated based on the failure time.
        $ The Cooldown function is defined in the common section.
        Temperature = Cooldown(Temperature,t_fail)
        WLevel = WLevel+LevelIncRate*t_fail
        if more(WLevel,InitWLevel) then WLevel = InitWLevel

        $ Diesel generator could still be repaired.
        mttr = MTTR_DG_FTR

        $ Probability for scenario 3: diesel generator fails to run and its repair fails.
        prob = prob+(1-prob)*p_ftr*(1-exp(-fr*t_mission))*RepairFail(Temperature, WLevel, mttr, t_st+t_fail)
       end
       else
       begin
        $ Make up system 1 cannot be started before fuel damage.
        $ Failure to run probability of make up 2 is added as such.
        prob = prob+(1-prob)*p_ftr
       end
      end
      else
      begin
       $ The SFPC (DG) repair does not come before fuel damage.
       $ Failure to run probability of make up 2 is added as such.
       prob = prob+(1-prob)*p_ftr
      end
    end
  end
end
else $ The SFPC (DG) repair and make up 1 start come before fuel damage.
begin
  $ If boiling is going on or starts before the diesel generator repair.
  if (WLevel < InitWLevel) or (t_boiling < t_repair-t_mu2) then
  begin
    $ Three failure modes of make up system 1 are evaluated in the following:
    $ start execution failure, failure to start and failure to run.
    $ In each case, also repair possibility is considered.
    $ The probabilities of the failure modes (including repair failures) are summed.

    $ The spent fuel pool conditions are updated depending on
    $ if the system is started before or after boiling.
    if t_start1 < t_boiling then
    begin
      Temperature = Temperature+HeatUpRate*t_start1
    end
    else
    begin
      Temperature = BoilingTemp
      WLevel = WLevel-(t_start1-t_boiling)*BoilingRate
    end

    $ Failure mode 1: start execution failure
    $ ----------------------------------------

    $ Make up 1 start execution fails and make up 2 repair fails or is not possible.
    if MU2EFAIL then
    begin
      $ Make up 2 start execution failed, so the system cannot be repaired.
      $ Probability that make up 1 start execution fails.
      prob = p_exe
    end
    else
    begin
      $ Probability that make up 1 start execution fails and repair of make up 2 fails.
      prob = p_exe*RepairFail(Temperature, WLevel, mttr1, t_start1)
    end

    $ Failure mode 2: failure to start
    $ ---------------------------------

    $ Start time for make up system 1 is determined.
    t_st = t_repair-t_mu2
```

```
    if t_st < t_start1 then t_st = t_start1

    $ The spent fuel pool conditions are updated.
    if t_start1 > t_boiling then
    begin
      WLevel = WLevel-(t_st-t_start1)*BoilingRate
    end
    else
    begin
      WLevel = WLevel-(t_st-t_boiling)*BoilingRate
    end
    Temperature = BoilingTemp

    $ MTTR depends on whether pump or DG fails to start.
    if r2 < CP_DG_FTS then mttr = MTTR_DG_FTS else mttr = MTTR_pump

    $ Probability that make up 1 fails to start and its repair fails.
    prob = prob+(1-prob)*p_fts*RepairFail(Temperature, WLevel, mttr, t_st)

    $ Failure mode 3: failure to run
    $ -----------------------------

    $ Mission time for make up system 1 is the time to normal water level.
    t_mission = (InitWLevel-WLevel)/LevelIncRate

    $ The failure time of the diesel generator is determined.
    t_fail = t_mission*r

    $ The spent fuel pool conditions are updated based on the failure time.
    $ The Cooldown function is defined in the common section.
    Temperature = Cooldown(Temperature,t_fail)
    WLevel = WLevel+LevelIncRate*t_fail
    if more(WLevel,InitWLevel) then WLevel = InitWLevel

    $ Diesel generator could still be repaired.
    mttr = MTTR_DG_FTR

    $ Probability that diesel generator fails to run and its repair fails.
    prob = prob+(1-prob)*(1-exp(-fr*t_mission))*RepairFail(Temperature, WLevel, mttr, t_st+t_fail)
   end
   else
   begin
    $ DG repair comes before boiling, SFPCS operation can be started and safe state is reached.
    prob = 0
   end
  end

  FD = true
return prob
```

Initial section for transient

```
$ Most global variables are defined in the common section.

$ Random variable for repair time determination
real rr

$ Variable values that are collected to results
Collect t_mission2, t_mu1, t_mu2, t_start1, t_start2, t_fail2, t_repair

$ Routine init is executed first
routine init
  FD = false

  $ Boiling conditions are the starting point for dynamic analysis.
  Temperature = BoilingTemp
  WLevel = InitWLevel

  $ Boiling time is calculated.
  boiltime = (BoilingTemp-NormalTemp)/HeatUpRate

  $ Mean time to repair the spent fuel pool cooling system.
  sfpcmrt = 32
```

```
  $ Probability that the repair is not performed before boiling.
  BINFREQ = EXP(-boiltime/sfpcmrt)

  $ Repair time of the spent fuel pool cooling system from exponential distribution.
  $ Time point 0 is when the boiling starts.
  rr = 1-random()*BINFREQ
  t_repair = -LN(1-rr)*sfpcmrt-boiltime

  $ Initialization
  mttr1 = 0
  mttr2 = 0
  rr2 = random()
  MU1EFAIL = false
  MU2EFAIL = false
return


routine finish
  $ No final calculations in this model.
return

$ Routine binner is used to categorise accident sequences based on e.g. Boolean variables.
Class FD
routine binner active
(true, 'FD'),
(*,    'OK')
return
```

MU:1_HFE for transient

```
$ Local variables
real prob, r2, r, t_avail, t_diag, t_exe

routine init
  r = random()   $ Random value between 0 and 1
  r2 = random()
return


$ Make up 1 start is performed successfully
function nil OK
  $ Time available to start make up system 1.
  t_avail = (WLevel-FuelLevel)/BoilingRate

  $ The execution time of make up system 1 start is drawn from uniform distribution.
  t_exe = r2+0.5

  $ The diagnosis time of make up system 1 start is drawn from lognormal distribution.
  r = r*cumul(MU1D,t_avail-t_exe)
  t_diag = icumul(MU1D,r)

  $ The start time of make up system 1.
  t_start1 = t_diag+t_exe

  $ The water level is updated.
  WLevel = WLevel-t_start1*BoilingRate
return nil


$ Execution fails
function real EFAIL
  $ Time available to start make up system 1.
  t_avail = (WLevel-FuelLevel)/BoilingRate

  $ The execution time of make up system 1 start is drawn from uniform distribution.
  t_exe = r2+0.5

  $ The diagnosis time of make up system 1 start is drawn from lognormal distribution.
  r = r*cumul(MU1D,t_avail-t_exe)
  t_diag = icumul(MU1D,r)

  $ Time when execution attempt is finished.
  t_start1 = t_diag+t_exe

  $ The water level is updated.
```

```
  WLevel = WLevel-t_start1*BoilingRate

  $ Execution failure probability
  prob = P_EXE1

  t_mu1 = t_start1

  MU1EFAIL = true
return prob
```

MU:1_P for transient

```
real prob

routine init

return


function nil OK
  $ Nil-function returns 1-prob
return nil

$ Common cause failure of make up 1 pumps
function real FTS_CCF
  prob = 2.11E-3

  t_mu1 = t_start1

  mttr1 = MTTR_pump
return prob

$ Make up 1 pumps fail independently
function real FTS_2
  prob = 3.74E-2*3.74E-2

  t_mu1 = t_start1

  mttr1 = MTTR_pump
return prob
```

MU:2_HFE for transient

```
$ Local variables
real prob, r2, r, t_avail, t_diag, t_exe, t_boiling

routine init
  r = random()   $ Random value between 0 and 1
  r2 = random()
return


$ Make up 2 start is performed successfully
function nil OK
  $ Time available to start make up system 2.
  t_boiling = (BoilingTemp-Temperature)/HeatUpRate
  t_avail = t_boiling + (WLevel-FuelLevel)/BoilingRate

  $ The execution time of the make up system 2 start is drawn from uniform distribution.
  t_exe = 2*r2+1

  $ Is there time to make the execution?
  if t_exe < t_avail then
  begin
    $ The diagnosis time of the make up system 2 start is drawn from lognormal distribution.
    r = r*cumul(MU2D,t_avail-t_exe)
    t_diag = icumul(MU2D,r)

    $ The start time of make up system 2.
    t_start2 = t_diag+t_exe

    $ The spent fuel pool conditions are updated depending on
    $ if the system is started before or after boiling.
    if t_start2 < t_boiling then
```

```
    begin
      Temperature = Temperature+HeatUpRate*t_start2
    end
    else
    begin
      Temperature = BoilingTemp
      WLevel = WLevel-(t_start2-t_boiling)*BoilingRate
    end
  end
return nil


$ Execution fails
function real EFAIL
  $ Time available to start make up system 2.
  t_boiling = (BoilingTemp-Temperature)/HeatUpRate
  t_avail = t_boiling + (WLevel-FuelLevel)/BoilingRate

  $ The execution time of the make up system 2 start is drawn from uniform distribution.
  t_exe = 2*r2+1

  $ Is there time to make the execution?
  if t_exe < t_avail then
  begin
    $ The diagnosis time of the make up system 2 start is drawn from lognormal distribution.
    r = r*cumul(MU2D,t_avail-t_exe)
    t_diag = icumul(MU2D,r)

    $ Time when execution attempt is finished.
    t_start2 = t_diag+t_exe

    $ The spent fuel pool conditions are updated depending on
    $ if the system start attempt is finished before or after boiling.
    if t_start2 < t_boiling then
    begin
      Temperature = Temperature+HeatUpRate*t_start2
    end
    else
    begin
      Temperature = BoilingTemp
      WLevel = WLevel-(t_start2-t_boiling)*BoilingRate
    end

    t_mu2 = t_start2

    $ Execution failure probability
    prob = P_EXE2
  end
  else $ No time to start the system
  begin
    prob = 1

    Temperature = BoilingTemp
    WLevel = FuelLevel
  end

  MU2EFAIL = true

  $ If start executions fail for both make up systems, fuel damage is assumed.
  if MU1EFAIL then FD = true
return prob
```

MU:2_P1 for transient

```
real prob

routine init

return


function nil OK
  $ Nil-function returns 1-prob
return nil
```

```
function real FTS
  prob = P_PUMP_FTS

  t_mu2 = t_start2

  $ This pump is either the first or second make up component to be repaired,
  $ depending on if make up 1 start execution failed.
  if MU1EFAIL then mttr1 = MTTR_pump else mttr2 = MTTR_pump
return prob
```

DG102_FLEX for transient

```
real prob, r, t_earliest, fr

routine init
  r = random()    $ Random value between 0 and 1
return



function nil OK
  $ Nil-function returns 1-prob
return nil

$ Failure to run
function real FTR
  fr = FR_DG    $ Failure rate

  $ The mission time is tentatively calculated as the time to reach normal water level.
  t_mission2 = (InitWLevel-WLevel)/LevelIncRate

  $ Given the repair time of the spent fuel pool cooling system,
  $ the earliest allowed failure time is calculated.
  $ The EarliestTime function is defined in the common section.
  t_earliest = EarliestTime(Temperature,t_repair-t_start2-t_mu1)

  $ If the earliest allowed failure time based on the repair of the spent fuel pool cooling
  $ system is larger than the time to reach the normal water level, the mission time is
  $ determined based on that.
  if t_mission2 < t_earliest then t_mission2 = t_earliest

  $ The diesel generator failure probability is calculated.
  prob = 1-exp(-fr*t_mission2)

  $ The failure time of the diesel generator is determined.
  t_fail2 = t_mission2*r

  $ The spent fuel pool conditions are updated based on the failure time.
  $ The Cooldown function is defined in the common section.
  Temperature = Cooldown(Temperature,t_fail2)
  WLevel = WLevel+LevelIncRate*t_fail2
  if WLevel > InitWLevel then WLevel = InitWLevel

  $ The total time the make up 2 system was used.
  t_mu2 = t_start2+t_fail2

  $ This diesel generator is either the first or second make up component to be repaired,
  $ depending on if make up 1 start execution failed.
  if MU1EFAIL then mttr1 = MTTR_DG_FTR else mttr2 = MTTR_DG_FTR
return prob

$ Failure to start
function real FTS
  prob = P_DG_FTS

  t_mu2 = t_start2

  $ This diesel generator is either the first or second make up component to be repaired,
  $ depending on if make up 1 start execution failed.
  if MU1EFAIL then mttr1 = MTTR_DG_FTS else mttr2 = MTTR_DG_FTS
return prob
```

MU_Repair for transient

```
$ Local variables
real prob, t_boiling, r, r1, r2, t_earliest, t_start, t_mission, t_avail, p_fts,
    t_diag, t_fail, mttr, fr

routine init
  r = random()    $ Random value between 0 and 1
  r1 = random()
  r2 = random()
return


function nil OK
  $ Nil-function returns 1-prob
return nil

$ Failure to repair make up systems. Failures after repairs are also included.
$ Two make up system repairs are modelled. The second repair is modelled by calling
$ RepairFail function, which is defined in the common section.
$ The failure probability that this function calculates covers both repairs.
function real FAIL
  $ Three failure modes of make up system 1 (or 2) are evaluated in the following:
  $ failure to repair, failure to start and failure to run.
  $ For the latter two, another repair is considered.
  $ The probabilities of the failure modes are summed.

  $ Failure mode 1: repair failure
  $ -----------------------------

  $ Time available for repair.
  t_boiling = (BoilingTemp-Temperature)/HeatUpRate
  t_avail = t_boiling + (WLevel-FuelLevel)/BoilingRate

  $ The repair failure probability is calculated assuming exponential distribution
  $ for the repair time.
  prob = EXP(-t_avail/mttr1)

  $ The repair time is drawn from exponential distribution.
  r1 = r1*(1-EXP(-t_avail/mttr1))
  t_start = -LN(1-r1)*mttr1

  $ The spent fuel pool conditions are updated depending on
  $ if the system is started before or after boiling.
  if t_start < t_boiling then
  begin
    Temperature = Temperature+HeatUpRate*t_start
  end
  else
  begin
    Temperature = BoilingTemp
    WLevel = WLevel-(t_start-t_boiling)*BoilingRate
  end

  $ Failure mode 2: failure to start
  $ --------------------------------

  $ Failure to start probability of make up 1,
  $ or make up 2 if make up 1 start execution failed.
  p_fts = P_PUMP_FTS
  if MU1EFAIL then p_fts = P_ALL_FTS

  $ MTTR for another repair after the failure to start is determined.
  $ It depends on if make up system start execution has occurred.
  mttr = mttr2
  if MU1EFAIL or MU2EFAIL then
  begin
    if MU1EFAIL then
    begin
      if r2 < CP_DG_FTS then mttr = MTTR_DG_FTS else mttr = MTTR_pump
    end
    else
    begin
      mttr = MTTR_pump
    end
```

```
  end

  $ Probability of failure to start and failure of consecutive repair is added.
  prob = prob+(1-prob)*p_fts*RepairFail(Temperature, WLevel, mttr, t_start)

  $ Failure mode 3: failure to run
  $ ------------------------------

  $ If MU1 was repaired only pump failure is considered.
  $ If MU2 was repaired both DG and pump failures are considered.
  if MU1EFAIL then fr = FR_DG+FR_PUMP else fr = FR_PUMP

  $ The mission time is tentatively calculated as the time to reach normal water level.
  t_mission = (InitWLevel-WLevel)/LevelIncRate

  $ Given the repair time of the spent fuel pool cooling system,
  $ the earliest allowed failure time is calculated.
  $ The EarliestTime function is defined in the common section.
  t_earliest = EarliestTime(Temperature,t_repair-t_start-t_mu1-t_mu2)

  $ If the earliest allowed failure time based on the repair of the spent fuel pool cooling
  $ system is larger than the time to reach the normal water level, the mission time is
  $ determined based on that.
  if t_mission < t_earliest then t_mission = t_earliest

  $ The failure time of the diesel generator is determined.
  t_fail = t_mission*r

  $ The spent fuel pool conditions are updated based on the failure time.
  $ The Cooldown function is defined in the common section.
  Temperature = Cooldown(Temperature,t_fail2)
  WLevel = WLevel+LevelIncRate*t_fail2
  if more(WLevel,InitWLevel) then WLevel = InitWLevel

  $ MTTR for another repair after the failure to start is determined.
  $ It depends on if make up system start execution has occurred.
  mttr = mttr2
  if MU1EFAIL or MU2EFAIL then mttr = MTTR_DG_FTR

  $ Probability of failure to run and failure of consecutive repair is added.
  prob = prob+(1-prob)*(1-exp(-fr*t_mission))*RepairFail(Temperature, WLevel, mttr, t_start+t_fail)

  FD = true
return prob
```

Common section

```
real Temperature,  $ Spent fuel pool temperature
     WLevel,       $ Spent fuel pool water level

     t_mission2,   $ Mission time for FLEX diesel generator
     t_repair,     $ Repair time of the spent fuel pool cooling system
     t_start1,     $ Start time of make up 1
     t_start2,     $ Start time of make up 2
     t_fail2,      $ Failure time of FLEX diesel generator
     mttr1,        $ MTTR for first make up system repair
     mttr2,        $ MTTR for second make up system repair
     sfpcmrt,      $ MTTR for spent fuel pool cooling
     boiltime,     $ Time from SFPC failure to boiling
     t_mu1,        $ MU1 use time (manual action + operation)
     t_mu2,        $ MU2 use time (manual action + operation)

     $ Model parameters
     NormalTemp = 35,        $ Normal temperature of the spent fuel pool
     InitWLevel = 10,        $ Normal water level of the spent fuel pool
     BoilingTemp = 100,      $ Boiling temperature
     FuelLevel = 4,          $ The height of the upper part of the fuel (m)
     CoolingFactor = 0.03,   $ Temperature decrease factor during cooling
     LevelIncRate = 0.25,    $ Water level increase factor during cooling
     HeatUpRate = 2.71,      $ Temperature increase factor before boiling
     BoilingRate = 0.0834,   $ Water level decrease factor during boiling
     CoolantTemp = 20,       $ Temperature of the coolant for all systems

     MTTR_pump = 20,
```

```
    MTTR_DG_FTS = 11,
    MTTR_DG_FTR = 15,

    FR_DG = 1.65E-3,      $ Failure rate of diesel generator
    FR_PUMP = 5E-6,       $ Failure rate of pump
    P_DG_FTS = 4.52E-3,   $ Failure to start probability of diesel generator
    P_PUMP_FTS = 3.95E-2, $ Failure to start probability of pump
    P_ALL_FTS = 4.38E-2,  $ Failure to start probability of pump and DG
    P_EXE1 = 5E-4,        $ Execution failure probability of make up 1 start
    P_EXE2 = 5E-3,        $ Execution failure probability of make up 2 start
    CP_DG_FTS = 0.103,    $ Conditional FTS prob of DG given that the system fails to start

    rr2                $ Random variable for timing determination


boolean FD,         $ Whether fuel damage occurs or not
       MU1EFAIL,    $ Make up 1 start execution failed?
       MU2EFAIL,    $ Make up 2 start execution failed?
       LOOP         $ Loss of offsite power scenario?

$ Distributions for make up system start diagnosis durations
LOGNOR MU1D = (2, 7.02),   $ Make up 1
      MU2D = (2, 8.29)     $ Make up 2

$ The temperature after specified time is calculated when a cooling system is in operation.
$ IT = initial spent fuel pool temperature.
$ t = duration of the cooling.
function real Cooldown (real IT, t)
  real Temp, Time, D

  Temp = IT
  D = 0.1    $ Time step
  Time = 0

  $ Temperature decrease is calculated in discrete time steps
  while Time < t do
  begin
    Temp = Temp-CoolingFactor*(Temp-CoolantTemp)*D
    Time = Time+D
  end
return Temp


$ The earliest allowed failure time given the spent fuel pool cooling system repair time is calculated.
$ The failure can occur before the repair if the temperature is below 100, because there is still some
$ time before the boiling starts.
$ IT = initial spent fuel pool temperature.
$ RT = repair time of the spent fuel pool cooling system.
function real EarliestTime (real IT, RT)
  real Temp, Time, D

  Temp = IT
  D = 0.1    $ Time step
  Time = 0

  $ The earliest allowed failure time is reached when the temperature is such that boiling could not start
  $ before the spent fuel pool cooling system repair.
  while Temp > BoilingTemp-(RT-Time)*HeatUpRate do
  begin
    Temp = Temp-CoolingFactor*(Temp-CoolantTemp)*D
    Time = Time+D
  end
return Time


$ Failure probability of a repair is calculated.
$ Failure to start or run after the repair are also included in the probability.
function real RepairFail(real Temp, Level, mrt, t_mu1r)
  $ Local variables
  real t_boil, t_ava, t_st, t_miss, t_earl, p, p_fts, fr

  $ Failure mode 1: repair failure
  $ ------------------------------

  $ Time available for repair.
  t_boil = (BoilingTemp-Temp)/HeatUpRate
```

```
  t_ava = t_boil + (Level-FuelLevel)/BoilingRate

  $ The repair failure probability is calculated assuming exponential distribution
  $ for the repair time.
  p = EXP(-t_ava/mrt)

  $ The repair time is drawn from exponential distribution.
  rr2 = rr2*(1-p)
  t_st = -LN(1-rr2)*mrt

  $ The spent fuel pool conditions are updated depending on
  $ if the system is started before or after boiling.
  if t_st < t_boil then
  begin
    Temp = Temp+HeatUpRate*t_st
  end
  else
  begin
    Temp = BoilingTemp
    Level = Level-(t_st-t_boil)*BoilingRate
  end

  $ Failure mode 2: failure to start
  $ -------------------------------

  $ Failure to start probability of the make up system.
  $ Repair of make up 1 in the transient scenario is a special case, because power supply
  $ comes from the grid and DG failure does not need to be modelled.
  p_fts = P_ALL_FTS $ failure to start probability of DG and pump
  if MU2EFAIL and (not(LOOP)) then p_fts = P_PUMP_FTS

  p = p+(1-p)*p_fts

  $ Failure mode 3: failure to run
  $ -------------------------------

  $ Failure rate is defined.
  $ If make up 1 was repaired in the transient case, only pump failure is considered.
  fr = FR_DG+FR_PUMP
  if MU2EFAIL and (not(LOOP)) then fr = FR_PUMP

  $ The mission time is tentatively calculated as the time to reach normal water level.
  t_miss = (InitWLevel-Level)/LevelIncRate

  $ Given the repair time of the spent fuel pool cooling system,
  $ the earliest allowed failure time is calculated.
  $ The EarliestTime function is defined in the common section.
  t_earl = EarliestTime(Temp,t_repair-t_st-t_mu1-t_mu2-t_mu1r)

  $ If the earliest allowed failure time based on the repair of the spent fuel pool cooling
  $ system is larger than the time to reach the normal water level, the mission time is
  $ determined based on that.
  if t_miss < t_earl then t_miss = t_earl

  $ The failure to run probability is calculated.
  p = p+(1-p)*(1-exp(-fr*t_miss))
return p
```

Bibliographic Data Sheet **NKS-444**

Title	Prolonged Available Time and Safe States
Author(s)	Tero Tyrväinen[1], Ilkka Karanta[1], Terhi Kling[1], Xuhong He[2], Frida Olofsson[2], Salvatore Massaiu[3], Erik Sparre[4], Carl Eriksson[4], Erik Cederhorn[4], Stefan Authén[4]
Affiliation(s)	[1]VTT Technical Research Centre of Finland Ltd, [2]Vysus Sweden AB/Lloyd's Register Consulting – Energy AB, [3]IFE (Institute for Energy Technology), [4]Risk Pilot AB
ISBN	978-87-7893-536-6
Date	February 2021
Project	NKS-R/PROSAFE
No. of pages	165
No. of tables	67
No. of illustrations	46
No. of references	44

Abstract
max. 2000 characters

Definitions for accident states and safe states are decisive for both deterministic and probabilistic safety assessments (DSA & PSA) of nuclear facilities. For instance, the IAEA's guides on the performance of deterministic and probabilistic safety assessments state that determination of mission times should take into account the time it takes to reach a safe, stable shutdown state. Fundamentally, it is a matter of finding an appropriate balance between the level of realism of models and practicality of the modelling approach. One cross-cutting modelling issue in this respect is the choice of mission time and related success criteria for systems, and the possibility to realistically include recovery and repair for long time windows. In DSA, it is often adopted from the previous praxis justifying what is sufficient. In PSA, the modelling approach itself forces to simplify treatment of mission time, and repairs are mostly not considered.

Use of single time window simplifies modelling, but in the light of occurred events (Fukushima Daichii), implementation of new technology in the nuclear power plants (e.g. independent core cooling), consideration of non-reactor nuclear facilities (e.g. spent fuel pools) and decommissioning phase reactors, such a simplified approach may need justification and/or to be reconsidered. In any case, the definition of a mission time is dependent on the definition of safe and stable state.

Since selection of mission time has an impact on many modelling aspects, and hence on the PSA results, it is important to study possibilities to treat mission times more realistically. For longer time windows, it becomes evident to consider e.g. time-dependent success criteria and possibilities for recovery and repair. However, for these issues there is not yet a consensus on how they should be addressed.

The PROSAFE project started 2019 with financial support from NKS, NPSAG and SAFIR, with the objective to improve the quality of safety assessment methods with respect to safe and stable state definition and assessment of long time windows, including human reliability analysis in long time window scenarios, use of dynamic success criteria, crediting repairs and modelling of different time windows.

This report presents the second and final phase of the project which was performed during 2020. Although further work is needed within several of the investigated areas, PROSAFE have provided important findings and some of the keys needed for a more realistic consideration of long time windows in future PSA:s.

Key words PSA, HRA, Mission Time, Repair, Long Time Windows, Safe State, Dynamic Success Criteria.