NKS-432
ISBN 978-87-7893-522-9

Prolonged Available Time and Safe States

Tero Tyrväinen[1], Ilkka Karanta[1], Terhi Kling[1]

Xuhong He[2], Frida Olofsson[2] Ola Bäckström[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]Lloyd's Register Consulting – Energy AB, Sweden

[3]IFE (Institute for Energy Technology), Norway

[4]Risk Pilot AB, Sweden

February 2020

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.

Key words

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

NKS-432
ISBN 978-87-7893-522-9
Electronic report, February 2020

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 2019 NKS-R PROSAFE activity

(Contract: AFT/NKS-R(19)128/3)

Tero Tyrväinen[1], Ilkka Karanta[1], Terhi Kling[1]
Xuhong He[2], Frida Olofsson[2] Ola Bäckström[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]Lloyd's Register Consulting – Energy AB
[3]IFE (Institute for Energy Technology)
[4]Risk Pilot AB

Table of contents

Acronyms

Acronym	Description
AFW	Auxiliary Feed Water
ASEP	Accident Sequence Evaluation Program
ATHEANA	A Technique for Human Event Analysis
ATWC	Anticipated Transient Without Control rods
ATWS	Anticipated Transient Without Scram
BE	Basic Event
BWR	Boiling Water Reactor
CBDT	Cause Based Decision Tree
CCF	Common Cause Failure
CDF	Core Damage Frequency
DG	Diesel Generator
DSA	Deterministic Safety Assessment
ECC	Emergency Core Cooling
EDG	Emergency Diesel Generator
EOC	Error Of Commission
EOP	Emergency Operating Procedure
EPRI	Electric Power Research Institute
ERO	Emergency Response Organization
ET	Event Tree
ETF	Extended Time Factor
FC	Fractional Contribution
FLEX	Diverse and Flexible Coping Strategies
FT	Fault Tree
FTR	Fail To Run
HCR	Human Cognitive Reliability
HEP	Human Error Probability
HFE	Human Failure Event
HMI	Human Machine Interface
HPLV	Human Performance Limiting Value
HRA	Human Reliability Analysis
HTA	Hierarchical Task Analysis
HVAC	Heating, Ventilation and Air Conditioning
I&AB	Initiators and All Barriers
I&C	Instrumentation and Control
IE	Initiating Event
IPE	Individual Plant Examination
LERF	Large Early Release Frequency
LOCA	Loss Of Coolant Accident
LPSD	Low Power and ShutDown
MCR	Main Control Room
MCS	Minimal Cut Set
NARA	Nuclear Action Reliability Assessment
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
RPV	Reactor Pressure Vessel
PPE	Personal Protective Equipment
PROSAFE	PROlonged available time and SAFE states
PRA	Probabilistic Risk Assessment
PSA	Probabilistic Safety Assessment
PSF	Performance Shaping Factor

PTR	Prolonged Time Recovery factor
PWR	Pressurized Water Reactor
RCS	Reactor Coolant System
SAMG	Severe Accident Management Guidelines
SHARP	Systematic Human Action Reliability Procedure
SPAR-H	Standardized Plant Analysis Risk-Human Reliability Analysis
SC	Success Criteria
SSC	Systems, Structures and Components
SSES	Safe and Stable End State
THERP	Technique for Human Error-Rate Prediction
TRC	Time Reliability Curve
TSC	Technical Support Centre
TTA	Tabular Task Analysis

1. Introduction

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. It is also stated that termination of the analysis at a fixed mission time may prevent meaningful results from being obtained. This leads to the question what a safe and stable state is and how it shall be defined, considering the increased scope of modern safety assessments.

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. 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. A common practice is to apply more or less categorically 24 hours mission times, and in some cases, e.g., in level 2 PSA, longer time windows need to be considered (48 or 72 hours).

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), and consideration of non-reactor nuclear facilities (e.g. spent fuel pools) and decommissioning phase reactors such a simplified approach may need justification. 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 results it is needed to study possibilities to treat mission times more realistically. It is important to notice that mission time is also related to several other issues in modelling. For longer time windows, it becomes evident to consider possibilities for recovery and repair. However, for these issues there is not yet a consensus.

The goal of the project "Prolonged available time and safe states" (the NPSAG project 53-003 PROSAFE) is to study how the safe, stable state should be defined, and whether it is necessary to adjust success criteria and mission times in PSA. It is expected that in some accident scenarios, there is a need to consider longer time windows. Current practice is that with 24 hour time windows, repairs and their effects need not to be considered. Longer time windows bring in the need to model and analyse more recovery actions and component repairs, and to revise human reliability analyses (HRA), since such scenarios offer large time margins for human actions. Static event tree and fault tree modelling techniques may also need to be complemented by dynamic methods, and further development of PSA tools may be needed. In addition, the reliability data and uncertainties in longer time windows are worth considering.

1.1. Purpose

PROSAFE (PROlonged available time and SAFE states) is a Nordic collaboration project.
The objective of the project is to improve the quality of safety assessment methods with respect to safe and stable state definition, assessment of long time windows, including human reliability analysis in long time window scenarios, crediting repair and modelling different time windows.

1.2. Scope of project

PROSAFE is dedicated to current Nordic conditions, meaning that the method development is adapted to type of reactors and sites that exist in Finland and Sweden. Method development takes also into account regulatory requirements and typical PSA applications. In this way, the

scope of PROSAFE can be defined to cover an assessment of fuel damage and radioactive release risk related to reactors and spent fuel pool, i.e., level 1 and level 2 PSA.

The method development is driven by pilot studies with the purpose to identify areas of risk importance and to evaluate the feasibility of the proposed methods.

1.3. Project organization

PROSAFE studies is carried out in five work packages:

- WP1 Information Collection;
- WP2 Safe and Stable State;
- WP3 Methods;
- WP4 Pilot studies;
- WP5 Meetings, dissemination and management.

Table 1 describes activities performed within each work package during 2019.

Table 1. Activities performed in PROSAFE during 2019

WP1	• Information collection and literature study. • Questionnaire to all Stakeholders
WP2	• Activity moved to WP3, see note.
WP3	• Development of definitions and abbreviations, including definition of Safe and Stable State. • Development of a requirements specification for modelling of long time windows. • Identification of human actions related to long time windows, • Investigation on important performance shaping factors and task analysis methods. • Investigation of fault tree and event tree methods for modelling of repair, dynamic mission times, time windows and dynamic success criteria. • Investigation on failure data for long mission times.
WP4	• Method elaboration and hypothesis testing in PSA models of Nordic utilities. • Development of a fictive spent fuel pool design for the example PSA.
WP5	• Project Management. • Two Stakeholder meetings and one Seminar • Two papers to ESREL 2020 and PSAM15 conference.

Note: The answers of the questionnaire showed that the stakeholders did not see definition of Safe and Stable State as a prioritized area. It was agreed with the Stakeholders that only a definition of Safe and Stable State for use within WP3 should be developed. Hence, the WP2 activity was moved into WP3.

1.4. Project interfaces

The project has had significant interaction with Nordic utilities and regulatory authorities. These include stakeholder meetings where the project financiers provided input on the scope and direction of the project and a seminar where results achieved during 2019 and plans for 2020 were presented. In WP1, an extensive survey was carried out among the stakeholders and the results were presented and discussed at a separate workshop.

Four utilities provided PSA models to be used for information collection and hypothesis testing in the early stages of WP3, and two of the utility models will be used in WP4 as pilot studies for the method development.

The project results were communicated at the 2019 NPSAG Summer Seminar in Helsinki (Authén et al., 2019a). In addition, papers on progress and tentative results of PROSAFE have been accepted to be presented at ESREL2020 and PSAM15 conferences (Authén et al., 2019b).

1.5. Report contents

This is a status report on the 2019 progress of the work packages of the PROSAFE project. Section 2 presents discussions and results of WP1, which was completed in 2019. Sections 3 – 4 presents performed work within WP2, WP3 and WP4, and Section 5 presents findings and conclusions based on the 2019 scope of work.

2. Information Collection

Information on topics important for the project were collected utilizing two main methods of inquiry: a literature review and a questionnaire to the stakeholders of the project. Results from these two activities are presented in the following subsections.

2.1. Literature review

2.1.1 Safe, stable state

Several guidance documents provide some sort of a definition for safe stable state, safe state or controlled state. Table 2 presents definitions from different sources. The definitions are typically very short and open for interpretation. Some of the definitions are significantly different from each other. The definition of ASME/ANS RA-S-2009 is based solely on reactor coolant system conditions. Other definitions include criteria on safety functions. The definition in STUK Y/1/2018 is most specific requiring reactor shutdown, low pressure and removal of decay heat. IAEA documents include criteria on core sub-criticality in the definitions.

Table 2. Definitions for safe, 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.
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).
Jacquemain et al., 2018	A plant is considered in a **safe stable state** when all components of the degraded core are in a coolable configuration, either still in place and/or relocated in-vessel and/or ex-vessel, and any stored spent fuel is also in a coolable configuration. The degraded core, if retained in-vessel, is considered to have reached a coolable configuration when there is no further hydrogen production from water-metal (clad and structural materials) interaction, the release rate of fission products is exceedingly low and there is no risk of re-criticality or of corium rupturing the vessel. Similarly, the degraded core, if ex-vessel, is considered to have reached a coolable configuration when there is no further incondensable gas generation from molten core concrete interaction, release of fission products from core-concrete interactions is exceedingly small, there is no risk of re-criticality and the ex-vessel core debris is retained in the containment without breaching the containment integrity. The spent fuel inventory is considered in a coolable configuration if all the spent fuel rods, degraded or not, are confined in the pool without the risk of a runaway oxidation reaction, there is no significant production of hydrogen and no risk of criticality.
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.

Each end point of level 1 PSA should be either a safe, stable state (or at least controlled state) or core/fuel damage state (IAEA-TECDOC-1804). However, the authors have not found any quantitative criteria for safe, stable state from literature, except concerning reactor sub-criticality (effective multiplication factor less than 0.995 in STUK Y/1/2018). Success criteria analyses often consider a fixed time window, typically 24 hours, and it is studied whether core damage occurs during that time window or not given specific conditions (NUREG-1953; Butler et al., 2010). The basis for success criteria seems to be avoidance of core damage within the

fixed time window rather than reaching a safe, stable state. For example, NUREG/CR-7177 studies definitions of core damage surrogates for success criteria analysis. The conditions at end points of the analyses are examined to check if the plant is in a stable state or safe stable state, but it is not specified what it exactly means, and the time point where safe stable state is reached is not determined.

Ma & Buell (2016) have studied safe and stable state in event tree modelling with quite similar scope as the PROSAFE project. They have considered the definitions from ASME/ANS RA-S-2009 and NUREG-2122, and have not specified any quantitative acceptance criteria for safe state. They point out the importance of checking the trends of plant parameters, such as core temperature, i.e. are the parameter values stable or changing at the end of a thermal-hydraulic analysis. If the parameter values are steady, the plant state can be assumed safe and stable. If the parameter values are changing, the mission time of the thermal-hydraulic analysis should be increased. In such a case, Ma & Buell recommend a mission time of 72 hours if it is practically possible.

In some PSAs, controlled states are used as end states instead of safe states. ASAMPSA_E (2015) points out the issue that safety analyses should be performed to the point where a controlled plant state is reached. ASAMPSA_E does not provide a definition, but states that it should be "defined by clear criteria for plant parameters and availability of essential safety functions." It states also that "challenges to such a controlled state should require additional, independent events in PSAs modelling."

ANS/ASME-58.22-2014 argues that for low power and shutdown (LPSD) PSA, there may be a need to evaluate successful end states of the at-power PSA to examine potential failures during repair and through start-up, e.g. feed and bleed cooling, high pressure recirculation, low pressure recirculation, and states with reactivity controlled but without the control rods inserted. They however conclude that these scenarios are low in frequency and often are neglected.

For severe accidents, the definitions of safe, stable state are more complicated. They also address the conditions related to reactor core debris and its coolability, and the release rate of fission products. The definition in STUK Y/1/2018 concerns also conditions of the containment. Jacquemain et al. (2018) specify also criteria that there should not be significant hydrogen production or core-concrete interaction anymore.

Jacquemain et al. (2018) state that some severe accident management guidelines specify acceptance criteria for a controlled, stable state after a severe accident. The variables used in the criteria include core exit temperature, hydrogen content, the pressure of the containment, radiation levels and the water level of the spent fuel pool. The criteria are however not presented in (Jacquemain et al., 2018).

2.1.2 Success criteria

The definitions of success criteria from different sources are often similar, e.g. as stated in ASME/ANS RA-Sa-2009: *"Criteria 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."* Table 3 presents definitions from different sources.

NUREG-2122 states that PSA uses several different types of success criteria, e.g. for different safety functions, for system functions needed to support the safety functions, and for the

components within these systems. The success criteria specify how the systems and components must function, when they must begin to function, and how long they must function.

The success criteria are typically developed by thermo-hydraulic analyses that represent the design and operation of the plant being evaluated, and where deterministic acceptance criteria are defined for the different safety functions.

Normally, success criteria in the PSA are defined relative to the initial requirements when an initiating event has occurred, and rarely take into account the possibility of increased safety margins, and thus less stringent requirements, some time after the initiating event. The time period, i.e. the mission time, during which the specified criteria need to be fulfilled is in most cases set to 24 hours (PSA level 1) or 48 hours (PSA level 2), even though the required time may be shorter. ASME/ANS RA-Sa-2009 requires for all Capability Categories that the effect of variable success criteria (for system functions) due to time dependence shall be incorporated into the system modelling.

ASME/ANS RA-Sa-2009 requires for Capability Category II that acceptance criteria are chosen such that the determination of core damage is as realistic as possible, and with enough margin to code-calculated values to allow for limitations in the code. Examples of core damage surrogates are given as:

- Collapsed liquid level less than 1⁄3 core height or code-predicted peak core temperature > 2500 °F (~1370 °C, BWR), or
- Collapsed liquid level below top of active fuel for a prolonged period, or code-predicted core peak node temperature > 2200 °F (~1200 °C) using a code with detailed core modelling, or
- code-predicted core peak node temperature > 1800 °F (~980 °C) using a code with simplified (e.g., single-node core model, lumped parameter) core modelling, or
- code-predicted core exit temperature > 1200 °F (~650 °C) for 30 min using a code with simplified core modelling (PWR)

NUREG/CR-7177 also studies definitions of core damage surrogates for success criteria calculations with thermo-hydraulic analysis and defines a peak cladding temperature of 2200°F (~1200 °C) as an appropriate surrogate for core damage at at-power analysis. For shutdown conditions they recommend a combination of surrogates, e.g. a reactor pressure vessel water level of one-third of the fuel height as a precursor to fuel damage and a peak cladding temperature of 1200 °C as a precursor to core damage.

ANS/ASME-58.22-2014 states that changes of success criteria during a plant operating state (POS) requires a change in the POS interval and an additional POS to be defined.

Ma & Buell (2016) have addressed the definition of success criteria in their study of safe and stable state, by using the definition of ASME/ANS RA-Sa-2009. They point out the close relation between safe and stable state, mission time and success criteria, and that a success criterion shall include a specified mission time a safety function needs to operate in order for the reactor to reach a safe and stable state. They present an iterative process for developing success criteria that a) "represent the minimum number of systems/components and human

actions that are required to ensure the safety function" and b) results in a safe stable state verified by thermo-hydraulic analysis results.

In the aftermath of the Fukushima accident it was recognised that present state-of-the-art PSA contain several insufficiencies, e.g. concerning the consideration of long scenario analysis times and mission times but also concerning that success criteria should be clearly defined for reaching a long term stable end state (ASAMPSA_E, 2015). Consideration of partial core damage was also identified to result in the need for development of specific success criteria.

Table 3. Definitions of Success Criteria.

Source	**Definition**
ASME/ANS RA-S-2009	**Success Criteria:** Criteria 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. The term accident **success criteria** is a technical element in the ASME/ANS PRA Standard whose objectives are to define the plant-specific measures of success and failure that support the other technical elements of the PRA. The minimum combination of systems and components needed to carry out the safety functions given an initiating event.
IAEA-TECDOC-1511	**Success criteria** regarding the plant response to initiating events are used to specify whether safety related functions meet the requirements to prevent damage to the core or mitigate significant releases of radioactivity. These safety-related functions in terms of a PSA may be functions of operating systems, front line safety systems, I&C, support systems, structures, components, and operator actions. For operator actions success criteria are characterized by statements that certain actions are successfully carried out within a defined time window.
NUREG-2122	The minimum combination of systems and components needed to carry out the safety functions given an initiating event.

2.1.3 Mission time

ASME/ANS RA-S-2008 defines mission time as "the time period that a system or component is required to operate in order to successfully perform its function." For many safety functions, the mission time must be the time it takes to bring the plant to a safe, stable state (IAEA-TECDOC-1804). The mission time is however often just set conservatively to 24 hours based on earlier experience without detailed analysis. This approach has been criticised, e.g. in ASAMPSA_E (2015). A more realistic approach is to use suitable deterministic computer code to determine how long it takes to bring the plant to safe state. The mission time analysis is closely connected to success criteria analysis, and e.g. same thermo-hydraulic calculations may be utilised in both analyses.

In a typical PSA, the mission time is 24 hours for most safety functions. The Fukushima accident however demonstrated that it can be relevant and more realistic to consider longer mission times (Burgazzi et al., 2014). For example, in cases of long term station blackout or loss of ultimate heat sink, mission times of 48 hours or 72 hours could come into question.

Shorter mission times than 24 hours have also been considered. Risk assessment of operational events handbook (USNRC, 2017b) provides an example that in the case of loss of coolant accident (LOCA), the mission time of low pressure injection could be 1 hour, after which recirculation needs to function 23 hours.

Risk assessment of operational events handbook (USNRC, 2017b) states that the mission time of emergency diesel generators has been determined based on the mean recovery time of the offsite power in some PSAs. In the case of loss of offsite power, there are examples of shorter (e.g. 2 hours) and longer mission times (e.g. 72 hours) (WGRISK, 2017). 72 hours have been used for containment systems and spent fuel pool analysis.

If a safe, stable state has not been achieved at the end of the mission time, IAEA-TECDOC-1804 recommends one of the following alternatives:

- Assigning an appropriate plant damage state for the sequence,
- Extending the mission time to the point where a safe, stable state is reached,
- Modelling of additional system recovery or operator interactions that bring the plant to a safe, stable state.

As the current best practise, Ma & Buell (2016) recommend 72 hours as the maximum mission time, because the accuracy of the analysis is expected to decrease with longer time windows, and the likelihood that non-modelled mitigation/recovery actions terminate the accident increases. They recommend sensitivity analyses for such scenarios.

If different mission times need to be modelled for the same event in different scenarios, an option is to use different basic events for different mission times in the PSA model. Recovery rules or fault tree configurations management techniques can be used to select the correct basic event for the analysed accident sequence. Use of multiple basic events to represent different mission times can however be somewhat inconvenient e.g. in risk importance measure computation, but it seems that current PSA tools do not offer better options to handle the issue. A possibility to facilitate the modelling could be to develop functionality to select the mission time of a basic event based on the accident sequence.

2.1.4 Crediting recoveries and repairs

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

- 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 handwheel 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.

There are two main issues in crediting recoveries and repairs in the PSA model:

- How to assess the probability that recovery or repair is successful in a given time window (or more generally, probability distribution of the time that recovery or repair of the system takes).

- How to model recovery or repair of the safety system in the PSA model.

PSA models typically include a number of recovery actions. For example, the recovery of offsite power is a recovery event that has often been modelled in PSA. Recovery of emergency diesel generators has also been modelled in many PSAs (USNRC, 2017b). Concerning offsite power, multiple possible recovery times are often modelled (WGRISK, 2017).

Because recovery actions can involve complicated actions that are usually governed by procedures, most are typically evaluated using HRA methods. A general exception is the treatment of offsite power recovery where the required recovery actions are often not within the jurisdiction of the plant personnel. Thus, offsite power recovery data is collected for use in PSAs (NUREG/CR-6823).

The repair of components is typically not modelled in PSA because one or more of the following apply to most minimal cut sets and accident sequences (USNRC, 2017b): (1) the time available to repair most components is generally too limited (i.e., core damage would occur before the repair is completed), (2) repair is an action that is not always governed by procedures and thus difficult to model, (3) the availability of spare parts is not always certain, and (4) abnormal procedures generally direct operators to rather use alternative equipment.

Modelling and analysis of recoveries and repairs

There are three main approaches to analyse recoveries and repairs: the judgmental approach, the statistical approach and the systems approach. In the judgmental approach, an expert or a group of experts assess and give estimates on various quantities of interest. In the statistical approach, the model is derived from available data, with the internal logic of the recovery or repair being of secondary concern. In the systems approach, the recovery or repair is considered to consist of more than one constituent parts (activities), and the model consists of models for the activities and the dependences between them. Also hybrids of two or all three approaches may be used.

There are several types of risk associated with recoveries and repairs, such as performance risk (the repaired/recovered system does not fill its performance requirements), side effect risk (the repair/recovery action compromises some SSCs of the plant), cost risk and occupational health risk, but the main emphasis in PSA has been on schedule risk. This is the risk that the recovery or repair may be completed too late from the accident progression point of view.

In the judgmental approach, various methods to elicit probabilities and other quantities from experts have been developed, and various issues to take into account in the process have been identified (e.g. Ortiz et al., 1991; Cooke, 1991; Meyer & Booker, 2001; Ayyub, 2001; O'Hagan et al., 2006). Humans are notoriously prone to various errors of judgment, and these have to be taken into account in formulating the questions posed to the experts. Also, other issues have to be taken into account, for example that experts are not asked to supply too many estimates. Nevertheless, the judgmental approach is often used when enough data is not available and when a systems model of the repair/recovery cannot or will not be built.

In the statistical approach, the main method used to model the uncertain completion time of an action is to fit a probability distribution to the data. There are many probability distributions

that can be used, for example the exponential, normal, Weibull, gamma and lognormal distribution (see, e.g. Bury, 1999). The lognormal distribution is often used in the modelling of the duration of human activities, because analysis of data has shown that maintenance times tend to be lognormally distributed (O'Connor & Kleyner, 2012, p. 410). Nevertheless, the choice of distribution depends on what kind of activity is being modelled and how well each distribution fits the data available.

Recoveries and repairs are results of human actions. These actions may consist of several interdependent activities, and they may be carried out by more than one person. Thus, there is some justification to consider them as operations (or projects). There are two systems approaches to the risk analysis of recoveries and repairs: one based on operation or project risk analysis, and one based on human reliability analysis.

One approach to the modelling and analysis of recoveries and repairs as contributors to risk is provided by project risk analysis, although its use in the nuclear safety field seems to have been minor so far (perhaps partly because repairs and recoveries have received relatively little attention). In this approach (Williams, 2002), a recovery or repair is viewed as consisting of a set of activities (also called tasks) that have precedence constraints between them and that are performed with some resources (humans, spare parts, materials etc.). The set of activities may be obtained by constructing a work breakdown structure (Norman et al., 2008). In the analysis of schedule risk, the most common quantitative methods are the critical path method (CPM), project evaluation and review technique (PERT), and Monte Carlo simulation of activity networks (Munier, 2014). Performance risks have received much less attention than schedule risks, but in principle they can be accounted for by e.g. fault trees.

Risk assessment of operational events handbook (USNRC, 2017b) summarizes the following factors from the PRA standard supporting requirements (ASME RA-Sa-2009) which should be considered in the analysis of recovery actions as well as repairs:

- plausibility and feasibility of the action in the analysed scenarios,
- availability of procedures, operator training, cues and manpower,
- scenario-specific performance shaping factors in the HRA,
- dependencies between human failure events in scenarios, accident sequences or minimal cut sets.

The handbook also contains a more detailed list of questions to be considered when modelling recoveries and repairs. In addition, it presents some examples of failure events and potential recovery/repair actions. The list provided by the handbook is not complete, because e.g. the availability of spare parts is not considered.

Risk assessment of operational events handbook (USNRC, 2017b) states that HRA techniques for estimating the likelihood of successful repair should not be used. This is because the possible repair scenarios, which are affected by a variety of human actions and hardware-related issues, would not be known without knowing the specific causes of the problem. There are however exceptions, such as the replacement of fuses, which can be performed rather quickly since spare fuses are available. In that case, the failure probability for the repair can be estimated by HRA or statistical analysis based on available repair data.

Existing HRA methods may be subjected to criticism also on the ground that they usually have a too simplistic view on repair time and factors that affect it. Some methods also may be inapplicable due to various reasons: for example, sufficient data might not exist to estimate the parameters of a repair time probability distribution.

Kichline (2018) points out that current HRA methods were not developed to quantify the human error probabilities (HEPs) associated with the transportation, placement, connection, or local control of portable equipment. Existing HRA methods may model certain types of actions and some performance shaping factors similar to those associated with the use of portable equipment. However, the HEPs were not developed for the context of FLEX (flexible coping strategies) actions (e.g., the HEP for a human task in the technique for human error-rate prediction (THERP) might be very different from the HEP of the same task in the scenario that results in the use of FLEX equipment).

Recovery/repair data used in probability estimation should reflect accident conditions (NUREG/CR-6823). Data from non-accident conditions should not be used, because there is no similar pressure for the performance of the action. NUREG/CR-6823 provides guidance for probability estimation based on operating data.

Recoveries and repairs in PSA model

Recoveries and repairs of safety relevant SSCs, whether successful or not, may significantly change accident progression. Therefore, they need to be considered in the plant PSA model if the mission time is sufficiently long so that recoveries and repairs may credibly take place.

Recoveries/repairs of failure to run events may need to be modelled separately from failure on demand events (USNRC, 2017b). If a component works some time before it fails, the time available for recovery/repair can be extended significantly, because the time to core damage is delayed. Failure times are therefore highly relevant when considering recoveries and repairs, and modelling of failure times can affect recovery/repair modelling significantly. However, in PSAs, failure to run events are typically conservatively assumed to occur at the time of the demand.

Another issue is that repair time can depend significantly on the specific failure causes and how the component exactly fails. Accurate repair modelling may therefore require division of a failure basic event into multiple events. For example, failures could be divided into those that can be repaired in a short time and those that require long repair times on the average. This might require re-evaluation of the failure data. The division could be done either explicitly in the PSA model or in background calculations providing inputs for the PSA model.

Recoveries and repairs can be modelled in PSA at the event tree level, fault tree level, sequence level and minimal cut set level (USNRC, 2017b). Recoveries from initiating events and main safety functions are typically modelled at the event tree level as additional event tree branches. Recoveries and repairs of individual components and subsystems are usually modelled at the fault tree level. A typical example of fault tree modelling is that the component failure basic event and the failure to recover/repair basic event are set under an AND gate. Scenario-specific basic events can be used for the same recovery/repair event if the probability of the recovery/repair varies depending the scenario. Techniques to handle such cases include recovery rules and use of multiple configurations of the same fault tree. Different fault tree configurations can, for instance, be applied to different accident sequences. Recovery rules can be used to manipulate minimal cut sets (USNRC, 2017b).

When the failure of the safety function has a major impact on accident progression, modelling recovery or repair at the event tree level is called for. In the simplest case, the recovery/repair of the component/subsystem/structure may be represented as a section in the event tree. The success criterion of the recovery/repair is that it is completed within some given time frame. If accident progression differs significantly depending on when the recovery/repair occurs, modelling of several time limits can be considered and several branches may be added to the tree in the recovery/repair section. This type of modelling may however make event trees very complicated, and therefore, the conventional event tree/fault tree based modelling approach is not the most suitable method for detailed recovery modelling.

Risk assessment of operational events handbook (USNRC, 2017b) states that the recovery and repair modelling should credit only one component in a system if there are multiple failed components. If there are failures in two systems, the possibility to recover/repair both requires case-specific consideration. If one failure can be recovered quickly from the control room, e.g. by simple trip reset, there may be time for another recovery or repair. In the case of multiple recoveries/repairs or recovery/repair combined with other human error events, it is important to analyse the dependencies.

If a component has a large failure probability, it may be relevant to consider second failure after recovery or repair.

Recovery of emergency core cooling systems is sometimes modelled in level 2 PSA (ASAMPSA2, 2013). The recovery may also induce additional risk, if the recovery can occur in a critical time window to produce large amounts of hydrogen. Therefore, instead of modelling only success and failure of recovery, modelling of different recovery times may be needed to make the analysis realistic. Recovery time modelling in simulation-based containment event trees has been studied in (Tyrväinen & Karanta, 2019).

2.1.5 Human reliability analysis methods

How to account for available time is an important issue in HRA, especially for the post-initiator human failure events (HFEs) (Category C). Historically the main focus for Category C HRA has been on supporting Level 1 PSA, that is, to estimate the likelihood of the main control room (MCR) operators failing to implement the emergency operating procedures (EOPs) in a number of accident scenarios that might end up in damaging the reactor core. The typical available times for nuclear power plant level 1 human actions are among 30 minutes to 1 or 2 hours. The existing HRA methods are developed to cope with this situation.

It seems that HRA of field workers other than operators (such as maintenance personnel) has not received much attention in HRA literature. Even though pre-initiator (Category A) HFEs are related to the maintenance personnel, they are typically latent errors that the personnel make during normal situations at the plant. Nevertheless, the success or failure of these NPP workers in repair and many recovery activities may affect accident progression significantly in long time window scenarios.

Human reliability as a function of time

Human error probability of a typical Category C HFE includes both diagnosis (e.g. detection, decision making) error probability and execution error probability (IAEA 50-P-10, 1996).

NUREG-1921 (NUREG-1921, 2012) provides a timeline illustration diagram (Figure 1), and shows the definitions of start time, time delay, available time, cognition time, execution time and required time.

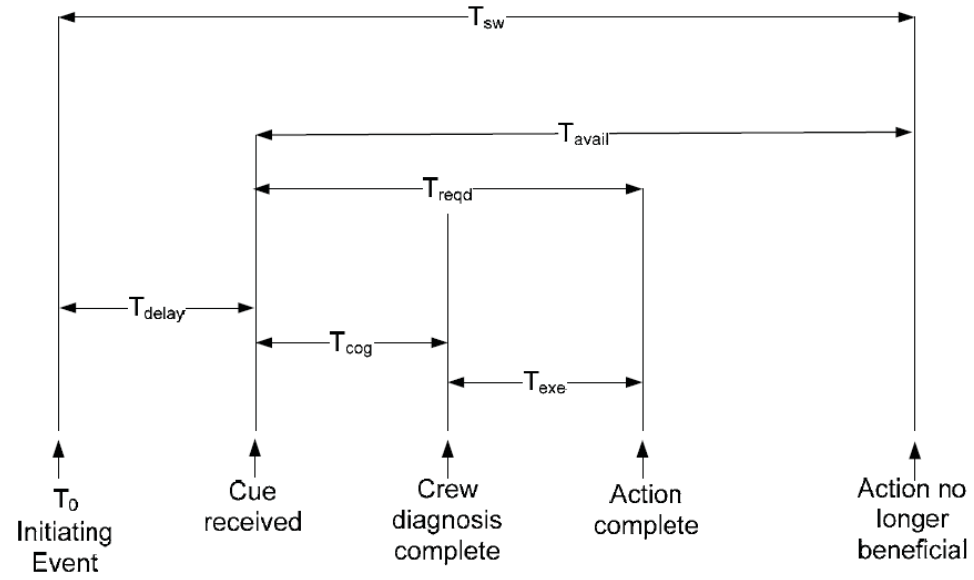

Figure 1. Timeline illustration diagram (NUREG-1921).

The terms associated with each timing element are defined mathematically.

- T0 = start time = start of the event
- Tdelay = time delay = duration of time it takes for an operator to acknowledge the cue
- Tsw = 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.
- Tavail = time available = time available for action = (Tsw - Tdelay)
- Tcog = cognition time consisting of detection, diagnosis, and decision making
- Texe = execution time including travel, collection of tools, donning personnel protection equipment (PPE), and manipulation of components
- Treqd = time required = response time to accomplish the action = (Tcog + Texe)

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 recovery action to the time required to perform the action (Tcog+Texe) and is calculated as follows:

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

For the diagnosis part, the available time has always been an important factor. Some HRA methods consider time as the dominant factor in diagnosis HEP estimation, e.g. human cognitive reliability (HCR)/operator reliability experiments (ORE) (Parry, 1992) or time

reliability curve (TRC) in THERP (NUREG/CR-1278, 1983). Some HRA methods consider time as one of the performance shaping factors (PSFs), e.g. SPAR-H (NUREG/CR-6883, 2005).

In general the time reliability curves used in HRA assume that the probability of a human failure event (its cognitive part and execution part) will be lower when the available time is longer. Figure 2 presents the TRC used in THERP for diagnosis HEPs. The nominal median HEP is 1E-4 for diagnosis of the first initiating event 60 minutes after the event cues (signals) appear in the main control room. The HEP will be lower when the time is longer.

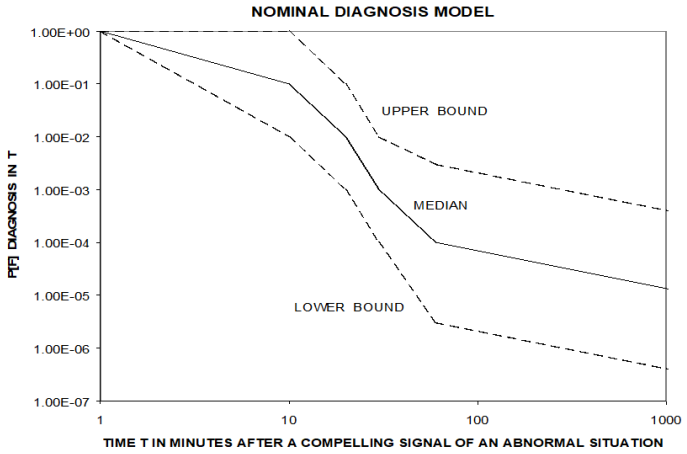

Figure 2. Time reliability curve used in THERP for diagnosis human error probabilities (NUREG/CR-1278).

In SPAR-H the available time is one of the eight PSFs in the HEP estimation. Table 4 shows the multipliers for the available time PSF for LPSD tasks. With the expansive time, the multiplier can be 0.1 to 0.01 for the diagnosis (nominal diagnosis HEP is 1E-2) and 0.01 for the action (nominal action HEP is 1E-3) part of LPSD tasks.

Table 4. Available time performance shaping factor for low power and shutdown (NUREG/CR-6883).

Case	**Available time**	**PSF Multiplier**	**Notes**
LPSD: Available time for diagnosis	Inadequate time	P(failure) = 1.0	* Analyst's choice, depending on complexity of diagnosis, including multiple factors such as available help and likelihood of additional cues. ** Analyst's choice, depending on complexity, PPE, work environment and ease of checking and recovery.
	Barely adequate time (approximately 2/3 x nominal)	10	
	Nominal time	1	
	Extra time (between 1 and 2 x nominal)	0.1	
	Expansive time (> 2x nominal)	0.1 to 0.01*	
LPSD: Available time for action	Inadequate time	P(failure) = 1.0	
	Time available is approximately equal to time required	10	

	Nominal time	1	
	Time available is ≥ 5x the time required	0.1	
	Time available is ≥ 50x the time required	0.01**	

There are important issues connected with the use of TRC methods in HRA. The first is the risk that some HRA methods, e.g. HCR/ORE or TRC of THERP, might produce unrealistically low diagnosis HEPs when time is considered as the dominant factor in the estimation/calculation of HEPs for human failure events (HFEs) with longer time frames. To avoid unrealistic estimation of low HEP, NRC (NUREG-1792, 2005) suggests that some limiting HEPs should be defined, considering the uncertainties. In UK, the human performance limiting value (HPLV) is typically set as 1E-5. However, for optimal conditions and scenarios with excessive time scales (> 12 hours) the HPLV can be justified as 1E-7.

The cause based decision tree (CBDT) method was intended to address actions with longer time frames that were outside the valid range of extrapolation for the monotonically decreasing HCR/ORE TRC. CBDT considers a relatively large set of potential PSFs and operator influences (e.g., quality of training, procedures, the human-machine interface, recovery potential) and uses a series of decision trees to establish the HEP. However, CBDT appears to be a method for treating post-initiator control room actions only (guidance and data for quantifying local actions is not provided) through a time-independent quantification approach. In that approach, time is considered qualitatively in addressing the potential for self-recovery of an error or recovery by another crew member. As a result, any analytical (i.e., not based on plant specific human error data) non time-related HRA method could be used for treating longer time frames in the way CBDT does.

A second issue with TRC methods is that they use time as the main (or only) determinant for the HEP, in which case it works as a proxy cause for the combined effect of all underlying causes of human error or non-response. Concern is raised about using the HCR/ORE and THERP TRC blindly across many different scenarios and contexts without consideration of other factors that may be more dominant error causes, thus arriving at optimistic estimates (NUREG-1842, p. A-2). This is especially serious when plant/context specific data are not collected and generic TRCs are used. The TRC in THERP is based on expert judgment derived from some early simulator data collections by General Physics and Oak Ridge. The TRC of the HCR/ORE was developed by EPRI in a simulator data collection program called ORE to examine the validity of the original HCR curves (Jung & Park, 2019). The results of ORE experiments did not support the use of the four factors originally included in the HCR TRCs (i.e., training, human-system interface, experience, stress). The factors were dropped from the HCR/ORE approach (NUREG-1842, p. 3-50) leaving time (available time and crew response time) as the only determinant for the HEP. It is thus an important assumption of the HCR/ORE method that the influence of important plant-specific factors will be implicitly included in the simulator-based, time-to-respond data that is collected at the plant and/or in the plant-specific estimates obtained from operators (NUREG-1842, p. 3-51).

Longer time windows

Most reference sources for HEPs are typically about main control room operating crews' tasks performed in a relatively short period of time (e.g., THERP considers less than two hours after the initiating event, NUREG/CR-1278, Figure 17-2, page 17-15). The Savannah River State human error data base development for non-reactor nuclear facilities (Benhardt et al., 1994) calculated the failure probability of longer time window tasks. These were called "long-term accident recovery" actions and were defined as "the failure to diagnose a situation and to correctly identify a recovery action when hours to days are available for the recovery". Using THERP fault tree modelling three failure probability values were proposed based on the available time for accident recovery and other conditions such as training, quality of procedures, and stress. As no installation-specific data were available for long time windows tasks, the recommended HEPs are the result of a THERP analysis in which median HEPs are converted into mean HEPs (based on the lognormal distribution for the HEPs) and rounded to 1, 3, or 5 times the appropriate power of ten. The HEPs were thus recommended for the non-reactor facilities (e.g., plutonium storage, waste tanks, solid waste disposal or defence waste processing). These probabilities are presented in Table 5.

Table 5. Recommended human error probabilities for long time windows actions at Savannah River State non-reactor facilities (Benhardt et al., 1994).

Nominal mean value	3.0E-3	EF = 10	Use: 24 to 48 hours for recovery, simple recovery actions
High mean value	1.0E-1	EF = 3	Use: Less than 24 hours for recovery
Low mean value	3.0E-5	EF = 10	Use: Three to seven days for recovery, simple recovery actions

The nominal mean value provided is 3.0E-3. This assumes that (a) recovery actions are to be completed within 24 to 48 hours following the initiating event, (b) stress is moderately high for the operators on shift during the initiating event but decreases to optimal levels for subsequent shifts, (c) there is low dependence on the previous shift, (d) procedures with checklist are followed, and (e) the second shift personnel might recover any errors made by the previous shift. The high mean value failure probability is 1.0E-1. It differs by the nominal case by assuming extremely high stress levels due to recovery actions to be completed within a short time frame of approximately 2 to 24 hours and by eliminating the two recoveries modelled in the nominal THERP tree. The low mean value failure probability considers an extended time window of three to seven days and thus optimal stress levels and recovery possibility, and is estimated at 3.0E-5.

Prolonged available time issue is also related to level 2 PSA since HRA needs to include a more comprehensive and realistic assessment of influences of long-term post-core damage events (ASAMPSA_E, 2015). Long-term post-core damage sequences, with time windows for severe accident management guideline actions spanning from several hours up to 72 hours, invoke new issues regarding the timing of operator actions. For example, in the Fukushima Dai-ichi NPP accident, the opening of containment vent valves was unexpectedly delayed by several hours by: 1) waiting for a nearby town to be evacuated, 2) hardware failures, and 3) harsh environment conditions that developed during the waiting time. For these prolonged scenarios, potential time delays need to be accounted for in a realistic manner. The lack of contingency procedures and pre-staged equipment impacted operator actions, so that operators had to

operate outside the procedural space or formal training. Relevant PSFs, such as fatigue (e.g., operators in the Fukushima Dai-ichi NPP event had long shifts with minimal food and rest) and "stress" in a very real sense.

Another potentially important aspect of long-term scenarios is the impact of shift changeover on the reliability of measure. Shift changeovers may lead to a loss of information or situational awareness, thus inducing additional sources of human error. In a longer time scenario, the plant crisis organization would be in place. The potential impacts of multiple decision makers on the performance should be considered realistically.

HRA in a longer time window might be related to knowledge-based decisions and actions for mitigating an accident. Therefore, it should be considered how to systematically analyse knowledge-based decisions and actions in a longer time window. This is considered as one of the needs in level 2 HRA for those post-core damage HFEs.

When there are longer available times, the potential new human actions should also be considered, e.g. recovery and repair actions. The credit and considerations of recovery and repair actions are discussed in Section 2.1.4.

It is noted that ASME PRA standard requires to account for any dependency between the HFE for operator recovery and any other HFEs in the sequence, scenario, or cut set to which the recovery is applied (ASME/ANS RA-Sa-2009). NPSAG HRA dependencies project reports provide good summaries on how to assess the dependency level and how to consider use of minimum values for joint HEPs (He et al., 2016, 2017).

2.1.6 Risk and reliability analysis methods

In this section, mathematical methods and models applicable to risk and reliability analysis for accident scenarios with long mission times are considered. In practice, they are methods that enable crediting repairs and recoveries, and also facilitate modelling situations where the order of events can vary and the order matters. Dynamic PSA methods fit these requirements.

Static fault tree and minimal cut set based techniques have significant limitations in modelling time related aspects. In level 1 PSA, the static and simplified approach has mostly been considered sufficient, but when modelling longer time windows, the limitations of the approach become more evident. In level 2 PSA, there has been more variety in the use of methods because of the dynamic behaviour of severe reactor accidents. Some level 2 PSAs rely on static event trees and fault trees, whereas some other level 2 PSAs use more advanced event tree techniques (ASAMPSA2, 2011; Tyrväinen et al., 2016; Guigueno et al., 2016).

In principle, PSAs could be made more realistic by using dynamic methods (Aldemir, 2013), e.g. dynamic and simulation-based event trees (Metzroth, 2011; Karanki et al., 2015; Queral et al., 2018; Tyrväinen et al., 2016; Tyrväinen & Karanta, 2019). On the other hand, the static approach has significant benefits, such as minimal cut sets, reasonable computation times, transparency of the model and easiness of the modelling. In addition, change of the method would be laborious. In the short run, it could be more realistic to consider incorporation of dynamic analyses to the static models, e.g. by more accurate computation of minimal cut set frequencies by dynamic methods (Bäckström et al., 2018), use of time-dependent basic events (USNRC, 2017) or crediting convolution (USNRC, 2017; Smith, 2016). Convolution could be used e.g. in the combined analysis of emergency diesel generator failure times and offsite power recovery time (USNRC, 2017). Complementary dynamic analyses could also be used to improve PSA models in some specific scenarios (Mandelli et al., 2019).

Markov models are a dynamic method to model state transitions of systems and components (Bucci et al., 2008). Markov models are particularly useful in modelling repairs and recovery actions. Markov models are likely not practical for plant-wide modelling, but can be effective and accurate in the analysis of individual systems. Hassija et al. (2014) present a good example on the application of Markov models to a long time window scenario with time-dependent success criterion.

Initiators and All Barriers (I&AB) is a dynamic methodology developed by EDF (Industrial Risks Management Department, France) and which is implemented in RiskSpectrum® PSA. It enables taking repair into account in a practical way in a full scope PSA application at the same time as you can actually define sequence specific time intervals referring to the available time to repair failed components until the undesirable end state occurs. Implementation of I&AB in RiskSpectrum® PSA is further described in (Bäckström et al., 2018). The PSA model is solved in the same way as for a static PSA, resulting in a minimal cut sets list to be quantified. These cut sets are then quantified using the I&AB method. This method is an analytic conservative approximation of the continuous time Markov chains for the cut set. It captures the most important dynamic behaviour of a failure mode (that is, the first-order dependence between failures of barrier components), while offering an approximate analytical method.

2.1.7 Reliability data

Basic events in PSA are normally divided into unavailability (because the equipment is undergoing testing or maintenance), failure to start or change state, and failure to run (after successfully starting) or maintain state to the end of the required mission time (NUREG-6823, 2002).

The basic event representing fail to run (FTR) is typically modelled with the reliability model 'mission time' which calculates the failure probability based on the failure rate and the mission time.

$$Q(t) = q + (1-q)\left(1 - e^{-\lambda T_m}\right) = 1 - (1-q)e^{-\lambda T_m} \quad (2)$$

where $Q(t)$ is the failure probability of the component; q is mission time independent failure probability for the component; λ is failure rate; T_m is the mission time.

This reliability model is used for most components, which have a mission time. Failures are assumed Poisson distributed which implies that the failure rate λ does not change during the mission time. The model also assumes that the component cannot be repaired within the mission time period (non-repairable).

In reality, failure rates of some components are not constant. The assumption of constant failure rate might particularly be unrealistic in long mission time scenarios.

For emergency diesel generators (EDGs), the available data are in general applicable only for short mission times since the operating experience is mainly based on the performed periodical tests, when the diesels functioning duration is generally short.

Grant et al. (1999) used reported EDG failures from tests performed at plants that reported under RG-1.108 requirements during the study period (1987-1993). These tests required the EDGs to run for 24 hours. There were 27 FTR events observed in the cyclic surveillance test data. The duration of the EDG run times prior to the failure of the EDG were reported in 19 of the licensee event reports. Based on analysis of these data the study concluded that three distinct

failure rates existed. The failure rate during the first half an hour was 2.5E-2 per hour. The failure rate decreased significantly to 1.8E-3 per hour for the period between 0.5 hours and 14 hours. For periods greater than 14 hours, the failure rate again decreased to 2.5E-4 per hour. Figure 3 illustrates the estimation of the three different failure rates.

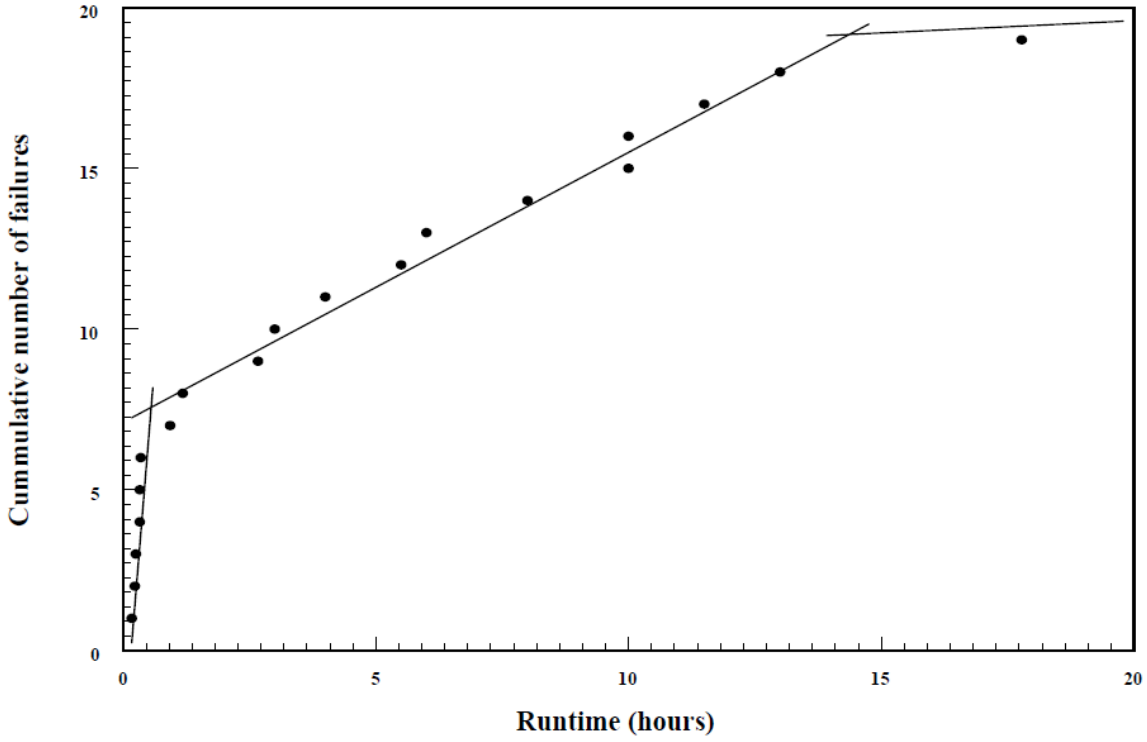

Figure 3. Cumulative number of EDG FTR events observed during the cyclic surveillance tests as a function of the time of the failure (Grant et al., 1999).

They commented that the early, middle, and late failures seem to correspond in part to different failure mechanisms. The change in the failure rate per hour was linked to a change in the mechanism of the EDG train failures. That is, the cooling subsystem dominated the early failures, accounting for about one-third of all the failures that occurred during the first half an hour; the electrical and fuel subsystems combined account for half of the failures in the period between 0.5 hours and 14 hours; and beyond 14 hours the only failure observed occurred in the electrical subsystem.

In comparison to the EDG failure data applied in US PSA or individual plant examination (IPE) study, approximately 80% of the PSA/IPEs reviewed by Grant used a single hourly failure rate for the entire mission time. The average failure rate for these PSA/IPEs is 5.9E-3 per hour. The remaining PSA/IPEs differentiated between less than one hour and greater than one hour failure rates. The average failure rate based on the less than an hour PSA/IPE data is 1.1E-2 per hour. The greater-than-one-hour average failure rate based on the PSA/IPE data is 2.3E-3 per hour.

The plant-specific estimates of failure to run probability were calculated for the respective mission times postulated in the PSA/IPE. The mission times postulated in PSA/IPE accidents were 6, 8, and 24 hours. Susquehanna assumed a 72-hour mission time, but details on how this was factored into the EDG failure probability estimate are not available. The RG-1.108 values for Susquehanna are calculated for a 24 hour mission time. Even though the IPE stated a 72-hour mission time, RG-1.108 data is restricted to less than a 24-hour run time. Extrapolating

the FTR probability to 72 hours was not done since the failure data was based solely on the cyclic surveillance tests of 24-hour endurance run. The Palo Verde IPE utilized a 7-hour mission time as their success criteria. The RG-1.108 values for Palo Verde are based on an 8-hour mission time.

In T-book for Nordic countries, one mean failure rate is provided for the diesel generator spurious stop. The critical failures included in the spurious stop have been the following: leakage in various forms, spurious trip for long start-up time or high voltage due to erroneous or incorrectly adjusted relays. The mean failure rate is around 1E-3/h level for Nordic plants. If this failure rate was used for scenarios of a longer mission time, the EDG failure probability would be quite high.

It is necessary to look at the whole EDG train boundaries for the prolonged mission time, as the root causes must be addressed as a part of the analysis. The boundary of the EDG train includes

- the diesel engine,
- electrical generator,
- generator exciter,
- output breaker,
- load shedding and sequencing controls,
- EDG room heating/ventilating subsystems,
- the exhaust path,
- lubricating oil,
- fuel oil subsystem (including all storage tanks permanently connected to the engine supply),
- the starting compressed air subsystem.

The fuel capacity of the day fuel tank and the large external storage tank need to be considered. The large external storage tanks have a capacity for several days of system operation. The day tank typically has capacity to operate the engine for 4 to 6 hours (Grant et al., 1999).

A more recent study is INL/EXT-14-31133 where a performance evaluation of EDGs using Equipment Performance and Information Exchange data from 1998 through 2012 and maintenance unavailability performance data using Mitigating Systems Performance Index Basis Document data from 2002 through 2012. The failure types studied are failure to start, failure to load and run and failure to run >1 hour. The results indicate that the failure rate during the first hour is more than three times greater than the failure rate after the first hour.

2.1.8 Epistemic uncertainty

Uncertainties are generally divided into two types: aleatory and epistemic. For the PROSAFE project mainly the epistemic uncertainty is of interest, since the aleatory uncertainty (stochastic uncertainty) describes the randomness that is the basis of events and phenomena.

Epistemic uncertainty refers to uncertainties related to a lack of knowledge, information or methods, also called “State-of-knowledge uncertainty” (NUREG-1855). This type of uncertainty can be identified, valued and reduced and is therefore relevant for all areas of the PROSAFE literature study. Three different definitions of epistemic uncertainty are presented in Table 6.

Epistemic uncertainty is normally divided into three groups:

- Parametric uncertainty

- Model uncertainty
- Completeness uncertainty

For the areas of the literature study, parametric uncertainty mainly relates to uncertainties in reliability data, parameter values in thermo-hydraulic success criteria calculations and human reliability calculations. Model and completeness uncertainties exists more or less in all tasks, though with emphasis on model uncertainty.

The need to address model and/or completeness uncertainties concerning e.g. stable end state, success criteria and mission time was identified in (ASAMPSA_E, 2015) but also recognised to be significantly harder to quantify than parametric uncertainty. Although it was stated to require alternative logic models, it was found necessary to include in the PSA.

Related to the areas of the PROSAFE literature study, the following high level or supporting requirements can be found in the ASME/ANS RA-S-2008:

- HLR-SC-B: The thermal/hydraulic, structural, and other supporting engineering bases shall be capable of providing success criteria and event timing sufficient for quantification of [core damage frequency] CDF and [large early release frequency] LERF, determination of the relative impact of success criteria on SSC and human actions, and the impact of uncertainty on this determination.
- HR-D6: PROVIDE an assessment of the uncertainty in the HEPs in a manner consistent with the quantification approach. USE mean values when providing point estimates of HEPs.
- HR-G8: Characterize the uncertainty in the estimates of the HEPs in a manner consistent with the quantification approach, and PROVIDE mean values for use in the quantification of the PRA results.
- HLR-QU-E: Uncertainties in the PRA results shall be characterized. Sources of model uncertainty and related assumptions shall be identified, and their potential impact on the results understood.
- HLR-LE-F: The quantification results shall be reviewed, and significant contributors to LERF, such as plant damage states, containment challenges, and failure modes, shall be identified. Sources of model uncertainty and related assumptions shall be identified, and their potential impact on the results understood.

NUREG-1855 gives guidance on how to address the different epistemic uncertainties in PSA applications, it does however not give guidance on how to treat uncertainties within specific areas, e.g. safe and stable end state or acceptance criteria. Though the presented methodology should in large be applicable also for plant PSA.

A possible approach for evaluating uncertainties in assumptions related to the success criteria definition is described in NUREG/CR-7177, where the effect of variations in MELCOR modelling assumptions on figures-of-merit for level 1 PSA is investigated and also the choice of core damage surrogates. It was found that some particular modelling assumptions can have significant impact, e.g. break size and location, number of ruptured steam generator tubes, reactor power level at the time of trip, timing of early operator actions, time of battery depletion,

behaviour of turbine-driven systems after battery depletion; and stochastic failure in the open or partially open position of relief valves.

NUREG/CR-7177 also presents a MELCOR uncertainty analysis for a loss of feedwater scenario and compare the results with a corresponding uncertainty analysis performed with MAAP code, without finding any significant differences in terms of the fraction of accident simulations predicted to result in core damage. Definitions for epistemic uncertainty are presented in Table 6.

Table 6. Definitions for epistemic uncertainty.

Source	**Definition**
ASME/ANS RA-S-2008	*"the uncertainty attributable to incomplete knowledge about a phenomenon that affects our ability to model it.* ***Epistemic uncertainty*** *is reflected in ranges of values for parameters, a range of viable models, the level of model detail, multiple expert interpretations, and statistical confidence. In principle, epistemic uncertainty can be reduced by the accumulation of additional information. (Epistemic uncertainty is sometimes also called 'modeling uncertainty.')"* Source of **model uncertainty**: *"a source that is related to an issue in which there is no consensus approach or model and where the choice of approach or model is known to have an effect on the PRA model (e.g., introduction of a new basic event, changes to basic event probabilities, change in success criterion, introduction of a new initiating event)."*
NUREG-1855	*"****Model uncertainty*** *is related to an issue for which no consensus approach or model exists and where the choice of approach or model is known to have an effect on the PRA model (e.g., introduction of a new basic event, changes to basic event probabilities, change in success criterion, and introduction of a new initiating event). A model uncertainty results from a lack of knowledge of how structures, systems and components (SSCs) behave under the conditions arising during the development of an accident."*
NUREG-2122	*"Variability in an estimate because of the randomness of the data or the lack of knowledge."* *"****Parameter uncertainty*** *is the uncertainty in the values of the parameters of a model represented by a probabilistic distribution. Examples of parameters that could be uncertain include initiating event frequencies, component failure rates and probabilities, and human error probabilities that are used in the quantification of the accident sequence frequencies."* *"****Completeness uncertainty*** *is caused by the limitations in the scope of the model, such as whether all applicable physical phenomena have been adequately represented, and all accident scenarios that could significantly affect the determination of risk have been identified."*

2.2. Questionnaire

A questionnaire was prepared for the stakeholders of the project. It covers the same areas as the literature survey in the previous section. The questions are presented in Appendix of (Tyrväinen et al., 2019). Five nuclear power plant companies, two nuclear safety regulators, and one nuclear fuel and waste management company answered to the questionnaire. This section presents a summary of questionnaire results. The section is divided into subsections according to the areas of the questionnaire.

2.2.1 Safe, stable state

The respondents provide different definitions of safe and stable end state (SSES) with variations regarding content, areas of applicability (e.g. PSA, deterministic safety analysis) and level of detail. Two organizations have no definition that is applied in PSA.

SSES for PSA level 1. Most definitions of SSES for PSA level 1 agree on requiring successful reactor shutdown and secured decay heat removal. Many also require reactor subcriticality and water supply for 24 hours, which is the time window mentioned when explicitly included in the definitions (i.e., in 50% of the responses).[1] One organization also includes in the definition of safe state the requirement of a non-pressurized reactor and of a leak-tight containment in LOCA scenarios. When SSES definitions for spent fuel are provided they refer to sufficient cooling to maintain stable temperature (and subcriticality). Three organizations also mention a general definition that "safe state is an operating state that minimizes the risk of a radiological accident." One of the organizations mentions it only in relation to deterministic safety analyses.

Some organizations specifically define the concepts "controlled", "safe" and "final safe state", but also here differently. A controlled state requires reactor shutdown (and subcriticality for one organization) and decay heat removal. Safe state is achieved when the reactor is also depressurized and can be kept in controlled state as long as the safety demands of the event remain. From a safe state it is possible to return to normal operation or proceed to the final safe state. Final safe state is when the subcritical reactor's residual heat is removed with a good margin and the safety demand caused by the event no longer exists. The reactor can be depressurized and the core removed. One organization applies the definition of controlled state to the successful end states in PSA instead of the definition of safe state.

One organization specifies a definition for spent fuel so that "safe state means that operations with handling of the fuel are able to end such that the spent fuel is in fuel pools or in another position where it can be stored safely with respect to cooling and criticality."

SSES for PSA level 2. In broad terms PSA level 2 definitions assume a SSES when a major release to the atmosphere has ceased within 24 hours from the event start. The reactor is in "controlled state", which implies core/debris decay heat removal secured, core/debris temperatures stable or decreasing, no risk of re-criticality, and no significant volumes of fission products being released, and, in addition, any remaining release is minor (the pressure inside the containment is low enough if the containment is not leak-tight). Two organizations specify the parameters for the size of a small release (e.g., less than 0.1% of volatile / non-volatile fission products of the hearth inventory of a 1800 MW type reactor; reactor subcritical with reactor pressure vessel (RPV) temperature under 100 ^{o}C). Some organizations do not

[1] One organization used to distinguish between safe states ("ok" end states in the PSA event tree) recognizing that although a core is kept stable and cooled within the time frame, discharge of primary coolant to the atmosphere may still occur and/or core damage might occur later, if additional recovery actions to establish long-term cooling are not performed. This distinction is no longer applied.

necessarily consider the successful end states in PSA level 2 as stable and safe states, but as controlled states.

SSES in deterministic analysis. In deterministic analysis the definitions of "stable state" refer to an operating mode where the radiological consequences of an accident are under allowed values. The situation is under control when the transient is over. More specifically, the definitions refer to the following set of physical conditions/parameters:

- reactor shut down and non-pressurised
- fuel covered with water
- no boiling
- decay heat removal secured (e.g., RPV temperature below 100 ºC)
- reactivity control established (e.g., effective multiplication factor of less than 0.995)
- manual cool down
- shutdown margin < 5% (safe state)

For events that include severe core damage additional criteria of the SSES are:

- water-covered core/debris
- residual heat removal / long term cooling for the core/debris,
- debris temperatures stable or decreasing
- no risk of re-criticality
- no significant volumes of fission products being released.

The successful transition from a controlled state to a safe state is usually grounded on a qualitative analysis, and specific "stable states" are defined for each analysis.

Half of the organizations did not see needs for improvement concerning the definition of safe, stable state. One organization stated that more exact definition would increase realism, but it is a matter prioritization. For regulators, it would be easier to interpret results if all utilities used the same definitions. One organization stated that "there is some ambiguity how the definitions for safe state versus controlled state are used. It is also somewhat unclear how the definitions should be applied for other operational states than at-power and for non-reactor nuclear facilities."

2.2.2 Success criteria

All organizations stated that a more realistic consideration and modelling of time related dependencies of success criteria could in general be beneficial for the PSA, especially for long time windows but also within the normal 24 hours mission time, and it could improve the use of PSA applications and decision making based on PSA input.

Success criteria is in general developed based on a conservative approach, though several organizations stated that they aim for a best estimate approach. The main concern with regard to long time windows was how to take into account that success criteria may change over time.

The deterministic acceptance criteria used in developing success criteria for the different safety functions are very similar among the different organizations (e.g. maximum fuel cladding temperature < 1204 °C), except for one organization that applies a criteria of max 1000 °C for 10 min in a core node during the time course studied. Concerning spent fuel pool some organizations only applied fuel covered in water as acceptance criteria, while others also considered avoidance of boiling.

Failures of system functions are either assumed to occur immediately after initiating event or divided into a few steps related to battery capacity times (mainly considered for electrical SSCs). This is either way conservative, and with increased mission times the conservatism will also increase (relatively). Change of success criteria over time was only considered by two different organisations for one case each.

The computer codes used for calculating success criteria were considered realistic for long time windows by two organisations, though the codes had not been verified for long time windows.

Most organizations analysed other end states than core damage, mainly boiling of spent fuel pool or condensation pool, but partial core damage was only analysed by one organization and in that case for level 2 (limited core melt).

2.2.3 Mission times

Most organizations use mission time of 24 hours in level 1 PSA. One organization uses 20 hours. In level 2 PSA, the used mission times vary from 24 hours to 48 hours (including also some mission times between those values). One organization performs level 2 analysis 24 hours from the onset of the release, which varies. Longer mission times are considered for shutdown states and spent fuel pool analyses. Some organizations use shorter mission times in loss of offsite power scenarios and for batteries. One organization models some actions outside the defined time windows. A special case is an interim storage facility for spent fuel, for which mission time of 720 hours is used.

If safe, stable state is not reached at an analysis end point, some organizations extend the mission time and some do not.

Some organizations identified some possibilities to change mission times. Longer mission times could be used for seismic events. Shorter mission times could be used for diesel generators, because loss of offsite power can be shorter than 24 hours, and for some supporting systems, such as ventilation systems.

Challenges related to mission times include:

- Estimation of failure probabilities in long time window scenarios
- Changing success criteria
- Modelling different mission times increases the model complexity and the number of basic events

- Some components, such as motor operated valves, need to be actuated several times during the mission time

- Possible measures that can be taken after a long time period may not be possible to analyse with credibility

- How to deal with extremely long mission times

2.2.4 Recoveries and repairs

Most organizations model some recovery actions. The recoveries that are modelled are typically selected based on their importance for the results and available time. Most organizations did not specify which recoveries are modelled. Recoveries of core cooling and pressure relief in level 2 PSA are examples that were mentioned.

Repairs are modelled typically only in long mission time scenarios, such as level 2 PSA and spent fuel pool analyses.

Recoveries and repairs are modelled in PSA either as separate basic events or they are included in the probabilities of basic events representing execution errors. One organization specifies that they have a fault tree dedicated for repair events, which appears as an event tree section.

Dependencies between recovery and repair actions and other human actions are generally not taken into account. One organization assumes that recovery/repair is either completely dependent of the related human action or independent. However, if a recovery failure is included in an execution failure, the available time after the execution failure is analysed.

Errors of commission are not considered in any of the modelled recovery actions.

To estimate recovery and repair probabilities, HRA methods, plant data and expert judgements are used. HRA methods that are used include Enhanced Bayesian THERP (Holmberg, 2019) and modified accident sequence evaluation program (ASEP) HRA procedure (NUREG/CR-4772).

Estimation of recovery and repair probabilities is considered a challenge in long time window scenarios. Their modelling also increases model complexity. Modelling of dependencies between recoveries and repairs and other human actions could make the analysis more realistic. Examples of actions that could be modelled in the future include repair of diesel generators, and events related to residual heat removal, water supply and power supply.

2.2.5 HRA methods

The HRA methods used are SPAR-H (NUREG/CR-6883), THERP (NUREG/CR-1278, 1983), Enhanced Bayesian THERP (Holmberg, 2019) and ASEP-HRA (NUREG/CR-4772). Some organizations use a combination of two or more of these methods and some organizations use a modified version of the method.

Some organizations only consider the diagnosis part for most actions inside the main control room. One organization states that the reason for this is that the failure of execution is considered to be negligible compared to the diagnosis part. One organization assumes that simple and short executions (regardless of location) can be included in the diagnosis part. Sometimes the diagnosis and execution parts are modelled as one common basic event, and sometimes it is split up into two separate basic events. Practices of taking recovery into account

vary: some organizations take it into account in both diagnosis and execution parts, some do not at all.

In general, no specific modelling is used for human actions with long time windows, but the available time is taken into account as one of the PSFs in most HRA methods. Also, in some organizations expert judgements and modified or extrapolated values from the ASEP-method are used. One organization noted that they do not think that enough credit is given for very long time windows with the method that they are using (SPAR-H). Another organization comments that they see the need for guidance on how to estimate the effect of the available time on the human error probability.

Some organizations do not use a lower limit for the failure probability and one of them also notes that this assumption is motivated by their PSA study. Other organizations use 1E-4 as a lower limit and one organization sets the limit to 1E-6.

Most organizations do take concurrent and competing activities into consideration when the HEP is calculated, but some do not.

All organizations that responded to the question "Are any human actions with long time window modelled" do include such human actions in their PSA. Examples of such actions are actions that are required late in level 1 PSA, actions in PSA level 2 or actions/repairs related to spent fuel pools. For fuel pools the available time for some of the modelled actions are in the scale of several days or weeks.

Most organizations intend to consider different crews and shift changes. Sometimes this is included when evaluating the PSFs and sometimes a qualitative assessment is made based upon expert judgements.

The main area for development that is identified is how to credit the long available time for manual actions and what other factors to take into account. Some organizations indicate that the used methods do not completely cover these manual actions with long available time in a satisfactory manner.

2.2.6 Methods to model time-dependencies

Different time windows for the return of offsite power are modelled in several PSAs. One organization models different diesel generator failure times with separate basic events. One organization considers the order of cable failures in fire PSA, because the impact depends on the order, but implements different scenarios simply with individual basic events in the PSA model.

Current PSA methods are generally considered sufficient to produce the required results. Some organizations however do not consider current methods sufficient to model various time-dependencies. One organization mentioned that challenging time-dependent scenarios do not play an important role in overall results.

Dynamic methods have not been used in PSA analyses. Reasons include lack of tool support and amount of effort needed.

Needs to model of time-dependencies include

- Modelling of dynamic success criteria

- Modelling of failure times in common cause failures (it is conservative to assume that all occur at the same time)
- Passing timing information from level 1 to level 2
- Modelling of core reflooding in critical time window for hydrogen production
- Modelling of fast and slow impacts of fires (some safety features may be available early in the scenario, but fail later due to fire)

2.2.7 Reliability data

Most organizations have not considered increasing or decreasing failure rates during an accident. Some organizations have modelled different failure rates for diesel generators depending on the mission time. Diesel generators have in those cases been modelled with a higher failure rate for short mission times, i.e. the failure rate for diesel generators decreases for longer time windows. In the study presented in INL/EXT-14-31133, it is shown that the failure rate for diesel generators decrease with operating time.

One organization notes that modelling long mission times is a challenge since it makes failures almost inevitable, even if this is not the experience of the operator. There is a perceived discrepancy between reality and PSA in this issue.

Some organizations comment that there is a need to identify component groups and failure modes for which non-constant failure rates should be used. One suggestion is that it should be evaluated if such data could be presented in the T-book.

2.2.8 Epistemic uncertainty

There were rather few answers to the questions covering uncertainty even though it is a recognised area of concern.

A few organizations stated that uncertainties concerning definition of safe and stable end state, success criteria, mission time and reliability data were small within 24h, but also that a conservative approach had been used. One organization stated that mission times much longer than 24h used in their analyses are used due to requirements and not related to realistic time to reach a safe and stable end state, and hence not an epistemic uncertainty.

Large uncertainties were said to be found mainly concerning scope of HRA for long term scenarios with associated failure probabilities, and reliability data for active equipment with mission times longer than 24 hours. Also, the choice of recovery actions to include, and hence also the number of recovery actions, in the analyses was identified to increase uncertainty.

2.2.9 Analysis cases to study within the project

Spent fuel pool accident scenarios were proposed by several organizations. Two organizations stated that HRA should play an important role in the analysis. Long term loss of offsite power and external hazard impacting sea water intake were also mentioned. One organization proposed that a normal accident scenario (e.g. loss of coolant accident or transient) with mission time of 24 hours would be modelled more realistically taking into account dynamic success criteria and repairs. The same organization also proposed analysis of a scenario with extended mission time considering reaching the safe, stable state.

2.3. Information collection conclusions

Ideally, successful PSA sequences should lead to a safe, stable end state. 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 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 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.

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.

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.

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). TRC from THERP/ASEP (or a modified curve, or combined with a low cut off value) is still commonly used to derive the diagnosis HEPs of these HFEs. SPAR-H uses the 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.

A large number of references on dynamic PSA methods can be found from the literature. 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 is need to study suitable approaches for modelling such time-dependencies.

It has been shown in a few different studies that failure rates of some components are not constant over time. 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.

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.

The objective of the questionnaire was to map current practice and difficulties within the areas of the literature survey and to identify the stakeholders view on the prioritized areas for research and development. Based on the results of the questionnaire the following contents for the continuation of the PROSAFE 2019 were decided:

Work package 2, Safe and Stable State.
The answers of the questionnaire showed that the stakeholders do not see this as a prioritized area. However, the project can see some challenges in performing the activities of work package 3 without addressing the definition of safe and stable state, especially for e.g. analysis of spent fuel pool. Based on the above, no new activities in this area were included in the 2019 activities, but a definition of Safe and Stable State was developed within work package 3 in order to support the work there. The area will be further considered in the 2020 activities of PROSAFE.

Work package 3, Methodologies
The activity was decided to cover the following areas:

- Modelling of sequences with long time windows. This will mainly address events for the spent fuel pool but also core related events requiring mission times longer than 24 hours.
- HRA methodology for actions with long grace times.
- Consideration of repair of failed equipment.
- Time window modelling with respect to credit of repairs, dynamic success criteria and failure data.
- Failure data. The area will be shortly addressed by identification of needed development, e.g. prioritized component types.

Work package 4, Pilot Studies
The purpose of the pilot studies is to evaluate the feasibility of the proposed methods in WP3. Real case studies can point out significant issues for the method development work of WP3. For this purpose the generic model from the DIGREL project (Authen et al., 2015) will be used, and complemented with a model for the spent fuel pool. Apart from this, the Ringhals 4 model of the spent fuel pool may also be used. The Pilot studies are carried out in close cooperation with the utilities which are the owners of NPP PSAs.

3. Methods

This work package covers methods related to prolonged time window and safe states (PROSAFE) in the context of nuclear power plant safety. It is divided into two parts:

- Human Reliability Analysis (HRA) – How to account for human actions with long time window.
- Probabilistic Safety Assessment (PSA) – Methods for modelling/account for different aspects related to long time windows in the PSA.

For both HRA and PSA, PROSAFE related definitions, modelling requirements, modelling methods and approaches are described. In PSA, hypothesis tests are performed using the stakeholder PSA models.

The proposed PSA and HRA methods and approaches will be further developed and refined in the pilot studies which will be conducted in 2020.

3.1. 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 (NUREG-1921, 2012) provides a timeline illustration diagram (Figure 4), and shows the definitions of start time, time delay, available time, cognition time, execution time and required time.

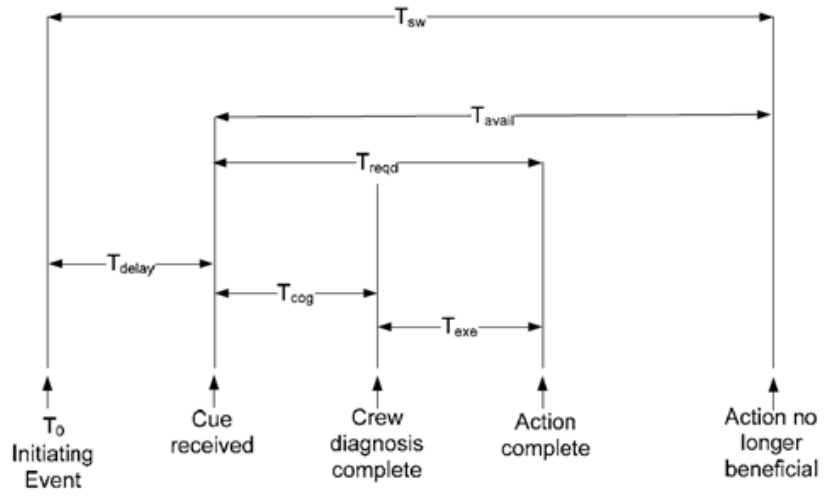

Figure 4. Timeline illustration diagram (NUREG-1921)

The terms associated with each timing element are defined mathematically.

- T0 = start time = start of the event
- Tdelay = time delay = duration of time it takes for an operator to acknowledge the cue
- Tsw = 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.
- Tavail = time available = time available for action = (Tsw - Tdelay)
- Tcog = cognition time consisting of detection, diagnosis, and decision making
- Texe = execution time including travel, collection of tools, donning personnel protection equipment (PPE), and manipulation of components
- Treqd = time required = response time to accomplish the action = (Tcog + Texe)

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 (Tcog+Texe) and is calculated as follows:

$$Time\ Margin\ (TM) = \frac{T_{avail} - T_{reqd}}{T_{reqd}} \times 100\% \qquad (3)$$

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 recovery actions to restore functions, systems or components are 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) which is credited within the specific HFE. Recovery mechanisms

(factors) are typically credited in the evaluation of the human error probability (HEP) for the HFE, and not modeled explicitly as separate basic events in the PSA model. Such recovery mechanisms include peer checking, unexpected instrument responses in response to an action, and new alarms that correct an error in response and would prevent the HFE from occurring (NUREG-CR 2199, 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. This measure is further discussed in Section 3.4.4.

In PSA, there is a clear distinction between actions to repair components or systems and actions to recover components or systems (NUREG/CR-6823, 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 handwheel 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 active 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

In WP1 of PROSAFE (Tyrväinen et al., 2019) it was noted that there was no current need to elaborate on the definition of the safe and stable end state, but there might be a need to revisit these definitions later.

Current state of the art considers some different definitions for safe and stable state for core damage where some 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 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."

SSM is similar regarding safe state of nuclear reactors:

"[…] refers to a normal and safe subcritical reactor and temperature below 100 degrees in the reactor pressure vessel."

NUREG-2122 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 modeling 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.

3.2. Requirements Specification

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 human reliability analysis (HRA) perspective. These definitions should be defined in the probabilistic safety assessment (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. Thus, it is important to have a proper 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 recovery 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.

Long-time windows specificities in Diagnosis and Execution

It is required to address both diagnosis and response execution failures for Category C HFEs.

Diagnosis includes detection, interpretation and (when necessary) decision making. Diagnosis tasks typically rely on knowledge and experience to understand existing conditions, plan and prioritize activities, and determine appropriate courses of action.

For the diagnosis part, the available time has always been an important factor for level 1 category C HFEs. If the time available far exceeds the time required and there are not multiple competing tasks, the estimated HEP is not expected to be strongly influenced by this factor. Thus, it is required to identify if other PSFs become dominant and how they influence the diagnosis. Possible error recovery of the diagnosis failure should be considered if feasible given the time window and the personnel available (e.g. additional staff and/or new shift).

For category C level 1 HRA the execution is typically considered as well defined, with a specific sequence of sub-steps to be performed in a fixed order, and typically there is no need to distinguish between the initiation and the completion of the action. In long time windows these conditions might not apply, and the following aspects should be considered:

- Multiple teams (control room crew, field operators, emergency manager, etc.)
- Several simultaneous actions
- Alternative options available
- Same/different actions at multiple units
- Continuous actions can fail underway (e.g., shovelling snow for many hours)
- Recurring actions (e.g., refuelling every 10 hours).

New HFEs (Recovery Actions and Repairs) considerations

For the important/dominant sequences, it is suggested to consider appropriate recovery actions and repair if they are feasible. These actions are not already included in the PSA (e.g., aligning another backup system not already accounted for) and can be tried out by the crews in order to restore the failure.

In long time windows scenarios the probability for recovery (i.e., “workaround” correct actions not directed by emergency, abnormal or component operating (EACO) procedures in effect but contained in some other EACO procedures not in effect) and repairs (bringing failed equipment that is required by EACO procedures in effect back to operable state) might be higher than in scenarios with limited time windows. This is because there is more time for the operators to find the relevant EACO procedure containing the recovery actions and more time for implementing/completing the EACO procedure for the repair. Typically, in short time-windows scenarios if no procedure specifying the required action exists, credit for the action is not given. Credit might be given as recovery or repair: if the operators autonomously find an applicable

EACO procedure through a walkaround (recovery) or if there is enough time to complete a repair as directed by the EACO procedures.

These definitions of recovery and repairs originate from HRA for proceduralized actions in the main control room (post-initiator level 1 HRA) for design-basis accidents and require analysis of the presence and feasibility of the actions contained in emergency, abnormal or component operating procedures. This analysis is also required for long time-windows scenarios. However, the availability of longer time windows does not guarantee recovery and repair for required actions, even when contained in procedures. This because the operators might delay decision or misinterpret the state of the plant for long time:

- Long time can mean little observable change, delayed feedback and counterintuitive dynamics.
- Alarms and cues might be ambiguous, might be shared by different failure states and/or by non-failure states.
- In unusual events the procedures do not easily accommodate the uncertainty and the dynamic characteristics of the plant environment. Procedures need often to be interpreted, bent or modified on the fly to deal with unexpected plant responses.
- Significantly different interpretations or response strategies might be available but in conflict, creating disagreement and debate among different decision makers.

The operators can thus, in addition of performing a wrong diagnosis despite the extended time, use the extra time for making sure the right diagnosis and response plans are made, and this could reduce the time available for acting.

It is then important to identify the actual plant conditions (and associated PSFs) and the operators/organizational differences in the nominal/bounding scenario and develop deviation scenarios (NUREG/CR-7017, 2012) if relevant.

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 (Johanson et al., 2015).

3.2.2 Hypothesis Testing with PSA Models

3.2.2.1 Hypothesis Testing Plan

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 is investigated through elaboration with several PSA models and will give an indication of the potential importance of a feature. These PSA models are all performed with fault tree/event tree tools.

The purpose of this hypothesis testing is to identify the important factors where a different modelling approach significantly could improve the realism. These features will be the focus for the method development part of the PROSAFE project. The result from the hypothesis testing will also include requirements on modelling approaches and methods.

The PSA models used for the hypothesis testing are actual models for different Nordic utilities and have for that reason been anonymised in this report, see Table 7.

Table 7. List of PSA models used in the hypothesis testing

Unit #	Scope of PSA
1	PSA level 1 model for an interim spent fuel storage facility
2	PSA level 1 model for a BWR reactor type
3	PSA level 1 model for a PWR reactor type and spent fuel pool
4	PSA level 1 model for a spent fuel pool facility

The focus of the hypothesis testing will initially be on spent fuel pool scenarios. Below are the selected issues that are elaborated in the models. Connected to the findings of the hypothesis testing for each topic, constraints for studied methods are formulated.

Mission Time
Change the mission time for components and investigate how that affects the result. For example, if a modelled mission time is 24 hours what is the result of changing it to 48 hours or 96 hours? Also, the impact from shorter mission times should be investigated. How sensitive is the model to such changes? Identify which types of failure modes that are most significant for the result, i.e. is it mission time events or failure on demands or other?

If the impact on the result is not as large as expected – for which reasons could that be? Are there "hidden" factors that are not accounted for in the model? Example: A diesel oil tank normally only lasts for 8 hours. Increasing the mission time straight off is not feasible. In this case a new manual action for refilling the oil tank needs to be considered.

Crediting repair
Are the failure modes that are most important for the result that could be repairable?

Identify a set of components that have a significant contribution to the result. Assume that it is possible to repair these components by assigning a repair failure probability. What is the impact on the results if the repair failure probability is 0.1 or 0.01? Note how to estimate the repair probability is discussed further in HRA part.

Look at dominating sequences in the PSA (with different mission time lengths). What type of events are dominating (failure modes). Are they repairable? Under which constraints?

The dominating MCSs in a PSA include often common cause failures (CCFs). Repair of such events is therefore an important issue to study. The probability of repair would be dependent on whether the CCFs occur simultaneously or not. The static PSA models as of today does assume that the CCFs are simultaneous. It can be elaborated with what the potential impact would be if repair of 1, 2 or all the components in the CCF group could be credited.

When the method requirements are formulated also requirements that affect time windows due to repair modelling must be considered.

Time Windows
What time windows are accounted for explicitly vs implicitly in the model? Can any time windows that have not been accounted for in the PSA be identified? What would the effect on the model/results be if they could be credited?

Examples of different types of time windows are:

1. The time window between the initiating event (IE) and the safe state.
2. The time window for a component/function is required to run, i.e. mission time.
3. A time window before a component/system must be started.
   Example: The time delay until a fuel pool starts to boil after the cooling has stopped. If cooling can be established before boiling happens, boiling can still be prevented.
4. Delays with limited capacity that allows/can buy extra time
   Example: A water tank that can be used for cooling. However, the tank only lasts for a certain amount of time before it is empty. Another good example is depletion time of batteries.
5. Dynamic mission times for redundant/diversified components.
   Example: If the first of two redundant components, both with mission time 20 hours, fails after 10 hours, the mission time for the second component is in reality reduced to 10 hours.
6. A time window with constant failure rate.
   For some components, e.g. diesel generators, the mission time may need to be divided into time intervals with different failure rates.
7. A time window with similar consequences.
   For example, consequences can depend on when the system fails, and there might be need to divide the mission time according to that. Another example can be core reflooding in critical time window, which is significantly different from other reflooding times.

Success Criteria

The system requirements may change during a sequence for example from a 2-out-of-2 requirement to 1-out-of-2. Identify in the model a system or component where two or more redundant trains are required. This should preferably be a system that is of a significant importance to the result. How much are the results affected if the requirements are relaxed? This will give an indication on the potential impact on the result if taking dynamic success criteria into account.

Normally combined system alternatives are not considered in PSA. This is a possibility when several systems are degraded but combining them would still fulfil the success criteria. One example could be to use one train in the low pressure cooling system and one train in the high pressure cooling system for core cooling. Are there such examples in the studied model, and could we test the impact when we credit such a possibility?

Manual Actions

Investigate dominating operator actions (Category C HFEs). Would the available time for action be significantly different under some constraints (for example if the HFE is included in one MCS together with mission time failures)?

In sequences where manual actions are combined with mission failures (i.e. failure to run over a given time interval), the actual available time for the manual action could potentially be longer than assumed in the static event tree/fault tree (ET/FT) model representation. In the ET/FT representation the available time is typically estimated based on the worst case, i.e. that failures occur at the time of demand. In reality the nature of a mission failure is that the component will function for a certain time before it fails. This time could potentially allow additional time for

a manual action performed in the same sequence. An example to illustrate this is the following scenario:

A cooling system consists of two redundant pumps. The initiating event is spurious stop of the pump in operation. The redundant pump starts but stops spuriously after some time. The available time to repair the first pump is the time until the undesired consequence will occur PLUS the extra time bought when the second pump is running before it fails. This extra time bought by the actual running time before failure is in general not credited in the ET/FT model.

3.2.2.2 Hypothesis testing – Unit 1, model for interim spent fuel storage facility

Description of model

The model represents the interim spent fuel storage facility of Unit 1. Probabilistic analysis focuses on loss of residual heat removal scenarios. The main consequences that are analysed are boiling in the pool and a release. Model stats are presented in Table 8.

Table 8. Model stats (with rounded numbers)

Number of basic events	500
Number of mission time events	150
Number of CCF groups	20

Mission Time

To prevent boiling in the pool, the cooling water circuit that is taken into use after loss of residual heat removal is required to function 168 hours, and the same mission time is also used for other back-up systems. No other mission times are modelled. The mission time is not a very important parameter, but has some impact nonetheless. The results are presented in Table 9.

Table 9. Mission time test

#	Test case description	Change in boiling freq.	Change in release freq.
TC1	Mission time 168 hours is reduced to 84 hours	-4%	-0.3%
TC2	Mission time 168 hours is increased to 336 hours	+8%	+1%

For the boiling risk, four mission time basic events have a fractional contribution greater than 0.5%. 34 mission time basic events have a risk increase factor greater than 2.

For release risk, none of the mission time basic events has a fractional contribution greater than 0.5%. 11 mission time basic events have a risk increase factor greater than 2.

Conclusions

Some improvement could be achieved e.g. if less conservative mission times could be used, but it is not a top priority.

Crediting repair

Repairs and recoveries are generally included in the initiating event frequencies and component failure probabilities. Factor 0.1 is used for each component to represent failures that cannot be repaired in six days, which is the time when the boiling starts. This has been assessed to be a conservative assumption. The factor however does not seem to be applied to every component. For example, a gas turbine is an important component for which repair is not credited.

For the release risk, recovery of spent fuel pool cooling is modelled in a very broad manner. Time to recover the spent fuel pool cooling is 36 days. Failure to recover is modelled only in

specific scenarios where an earthquake or oil spill causes also a core damage. Otherwise, recovery is assumed successful with certainty.

Around 24% of the boiling risk comes from internal initiating events. If any internal initiating event could be repaired with probability of 0.99 instead of default 0.9, the boiling frequency would be decreased by 21%. If repairs of the initiating events were assumed impossible, the boiling frequency would be increased by 211%.

There are also eight significant (fractional contribution over 0.5%) post-initiating event component failures, including the failure to run events mentioned in the previous section and four failure on demand events. Two of those basic events are gas turbine failures for which repairs have not been credited. If the other failures could be repaired with probability of 0.99 instead of default 0.9, the boiling frequency would decrease by 7%. If repairs of those component failures were assumed impossible, the boiling frequency would increase by 95%. If the gas turbine could be repaired with probability of 0.9, the boiling frequency would also decrease by 7%.

The model includes quite a large number of basic events with a MTTR parameter. The values are ranging from 0.2 hours to 72 hours, but for basic events with fractional contribution larger than 0.1% the values are smaller than 24 hours. To study the sensitivity, if the probabilities of all those basic events are multiplied by 0.1, the boiling frequency decreases 9%. Anyhow, since the model contains the MTTR information, it would be tempting to utilise that for more realistic repair modelling. However, if exponential distribution is used with the available MTTRs, the repair failure probabilities for available time of six days are very small for all significant basic events. It can be too optimistic to use the MTTR values that way, because they have not been estimated based on repairs performed during accident conditions. On the other hand, application of the same factor (0.1) for all basic events may lead to unbalanced results, since some failures are clearly repaired faster than others.

Another question is whether impacts of hazards could be repaired. Hazards are dominant in the results, so such repairs could have large impacts.

Many minimal cut sets include several human failures in combination with a repair failure, so it can be relevant to consider dependencies.

Conclusions
More realistic modelling of repairs could improve the analysis. The biggest challenge is to estimate the repair failure probabilities in a credible manner for different components. The dependencies between repair actions and other important human actions should be analysed and taken into account in the probability estimates. The main challenge in the modelling would then be to model those dependencies. More realistic analysis would also consider what it takes to reach a safe state after a repair, i.e. how long the repaired system needs to function after the repair, and what is the risk of another failure after repair before the fuel pool is safe and stable.

Time Windows
The mission time for failure to run events is 168 hours. After that it is assumed that a safe state has been reached. It is not a very important parameter as discussed earlier.

The spent fuel pool starts to boil in six days without cooling water injection. This time window has been evaluated by two deterministic computer codes and it is considered quite a reliable

estimate. Time to fuel uncovery is 36 days. That has been conservatively assumed to be the time window for cooling recovery to prevent release.

The mission time is long, so failure rates of some components could possibly change during it. Such changes have however not been modelled.

No other time windows have been identified from the model.

More realistic analysis would take into account dynamic mission times that depend on how long it actually takes to reach a safe state. In practise, the mission time likely depends a lot on the status of the pool, when the system is taken into use. The later the spent fuel pool cooling is recovered, the longer is the time to reach the safe state. Also, it could be that one cooling water system works some time before it fails, and then a safe state can be reached sooner with a back-up system compared to the case where the first system fails right at the beginning. Furthermore, the time the primary system functions before failure affects the time available to switch the back-up system into use or repair the primary system. However, these types of scenarios have a minor role in the current results.

Conclusions
No top priority development needs were identified related to time windows. Some improvements could possibly be achieved by more realistic analysis of mission times, failure times and available times in some scenarios.

Success Criteria
In each case, only one pump line is needed, and the need for cooling water is assumed constant during the accident scenario. Therefore, there seems to be no need for dynamic success criteria modelling.

Manual Actions
Manual actions have a dominant role in the results. The available time for manual actions is generally assumed to be six days. There are however scenarios where the real available time could be different, e.g. if the second redundancy of the heat removal system works some time before it fails. The available time has not been modelled as dependent on failure times, but such scenarios would only have a minor role in the results as discussed earlier.

Modelling of dependencies between manual actions could potentially make difference in the results, because many important minimal cut sets include multiple HFEs. Since the spent fuel pool is unlikely to be the main focus of attention to any crew, also dependencies on the situation in the main control room (and activities of other crew such as field workers) should be considered, because it is possible that crew members neglect the spent fuel pools due to workload caused by the reactors. However, we have not identified nor analysed dependencies so far.

3.2.2.3 Hypothesis testing – Unit 2, model for a BWR reactor type

Description of the model
The model represents the reactor of Unit 2 covering the risks of accidents following initiating events of most types. The model focuses on core damage or large releases of the core inventory is evaluated. For Unit 2 there is no model of the spent fuel pool.

The plant has a high level of redundancy in safety systems and several examples of diversification among the safety functions to counteract common cause failures. Repair is not credited in the model and thus it is of interest to identify repairable events or components.

Some basic model data is presented in the Table 10. The numbers are slightly rounded for confidentiality purposes.

Table 10. Model stats

Basic events	8200
CCF groups	350
CCF events	3900
Manual actions events	900
Repair events	0

The elaborations are performed with all available initiating events. The consequence studied here is the core damage.

Mission Time

The mission time is changed from 24 hours to 48 and 72 hours and the impact on the core damage is investigated. This is the range when repair should be reasonable. The impact of lowering the mission time to 12 hours is also shown in the Table 11.

Table 11. Changes of mission time from 24h

Mission time	Change of core damage frequency in relation to 24h mission time
12h	-8%
48h	28%
72h	70%

Importance values for basic events and parameters are studied to investigate the significance of mission time events and parameters. The importance of a basic event is ranked according to the fractional contribution (FC) or the risk increase factor (RIF). The importance of parameters is ranked accordingly. The FC and RIF for basic events are summed for each component. According to NEI 00-04 significant contributors can be identified as components and parameters with FC>0.5% and RIF>2. For CCF groups significant contributors are defined for RIF>20.

For sequences leading to consequence core damage the number of components with a FC>0.5% is 43 in total. Of these 43 components, 15 components are modelled as mission time events and 22 of these 43 components have a RIF>2. About 500 components have a RIF>2. The mission time parameter for 24 hours has the 5:th highest FC and a RIF of about 21.

For CCF groups there are 16 with a FC>0.5% and five of these are mission time events. There are 49 CCF groups with RIF>20 and 12 of these are mission time events.

Events in an MCS list can be separated in to the following four main types of events:

- Initiating event
- Failure on demand
- Mission failures
- Unavailability

It can be noted that there is more than 100 MCS contributing to more than 1% of the total core damage frequency with a wide range of initiating events and failure modes. External events contribute to this to a large extent. All combinations of the above exist but the most contributing are the following:

- **Initiating event** (Frequency), **Unavailability** (Probability)
- **Initiating event** (Frequency), **Unavailability** (Probability), **Failure on demand** (Tested)
- **Initiating event** (Frequency), **Unavailability** (Probability), **Mission failure** (Mission Time)

Conclusions
Mission time events are significant contributors to the results in the Unit 2 core events study. It can be concluded that the selected mission times modelled is of great significance to the results.

Crediting repair
In the studied model repair is not currently modelled. If repair is to be considered the component must have a repairable failure mode and the repair must be considered reasonable with respect to time windows and success criteria. The events that could potentially be repaired with these conditions have a significant contribution to the MCS-list but are still not dominating the result. To make this list, no consideration has been taken to whether the failure is due to common cause failure or independent failure. This is also taking the most conservative approach; where the cases that have some uncertainty whether there is some possibility to repair is considered unrepairable. One example of events that have been excluded is all types of battery failure.

One interesting event to consider is the 4-out-of-4 CCF spurious stop of the diesel generators during the time window of 9-24 hours. This contributes with about 7% to the total core damage (or has a cumulative relaxation of the core damage with a high repair probability). The most dominating failure sequences have a success criterion of 1-out-of-4 of these diesel generators. It is of interest because of the relative high contribution and because of the CCF-properties of the event.

Adding more of identified repairable events results in further relaxation of the core damage frequency and with the 26 most contributing repairable events (components with FC>0.5%) the relaxation is about 40%. There is a somewhat even distribution of common cause failures and independent failures that is contributing to the most relevant repairable events.

The most contributing components that could potentially be repaired (not showing most components for confidentiality reasons) for the Unit 2 model are shown in Table 12. There, the events that were considered repairable have assumed the same repair failure probability (0.1 and 0.01).

Table 12. Repairable events

Component	**Description**	**Cumulative relaxation of core damage frequency due to repair (P_{fail}=0.1)**	**Cumulative relaxation of core damage frequency due to repair (P_{fail}=0.01)**
Diesel generator	Spurious stop, CCF (4oo4), time window 9-24h	6%	7%
Repairable component 2	Failure	10%	11%
Repairable component 3	CCF	13%	14%
Repairable component 4	CCF	16%	18%

Component	Description	Cumulative relaxation of core damage frequency due to repair (P_{fail}=0.1)	Cumulative relaxation of core damage frequency due to repair (P_{fail}=0.01)
Repairable component 5	Failure	19%	20%
Repairable component 6	Failure	21%	23%
Repairable component 7	Failure	22%	25%
Repairable component 8	Failure	24%	27%
Repairable component 9	CCF	26%	29%
Repairable component 10	CCF	28%	30%
Repairable component 11	Spurious stop	29%	31%
Repairable component 12	Spurious stop	29%	31%
…	…	…	…
Repairable component 26	Failures, CCF, spurious stop	36%	40%

It can be noted that the most dominating sequences are not repairable, many containing, for example, failure of batteries (often by CCF). Further analysis might show that these sequences are repairable but here the conservative approach is applied.

Conclusions
Repair has not been considered in the modelling of the core damage events in the time windows currently considered. Although there is significant, but not dominating, contribution from repairable events, it is a quite large workload to model repair for every system and component. It would also require a more thorough investigation of repairable events.

For core damage sequences the repairable events resulting from common cause failure must be taken into consideration. This is closely related to the modelling of different time windows and whether the CCF occur simultaneously in time.

Time Windows
The following can be noted on the modelling of different types of time windows in the Unit 2 model (bullets 1-7 refer to the types of time window that are defined in the beginning of Section 3.2.2.1):

1. The time between the initiating event and the safe state is modelled as a constant time that is derived from deterministic criteria. Hence this time window is modelled with no dependency to the specific sequence of events. It is required that a safe state is either reached within this time window or that the reactor with certainty will reach a safe state after 24 hours. However, the mission time of the required safety functions is always limited to 24 hours.
2. Static mission times are in general modelled for component mission failures, where mission times of 24 hours, 16 hours, 7.5 hours and 30 minutes are used. For short-term functions (e.g. depressurization, isolation, scram) a mission time of 1 hour is assumed. This means that the mission time is in most cases not dependent on the timing of other events in the sequence. One exception is the mission time for emergency diesel generators which is dependent on the success of re-establishing external power supply.
3. The Unit 2 model considers, dependent on the initiating event, the time window before the core cooling needs to be established and also the time window for establishing residual heat removal. These time windows mainly affect the modelling of power supply and are related to modelled time windows for emergency diesel generators, return of offsite power and depletion time of batteries. There are also some other relevant examples, e.g. in sequences with main feedwater pumps running with main steam lines isolated the time until the condenser is depleted of water and required start of auxiliary feedwater is considered. A different, but related, aspect of the Unit 2 model is that it roughly considers the time after

IE when a component/function may, or needs to be, started, with regard to the possibility to credit battery backup, return of offsite power, and time dependent failure rates of diesel generators. E.g. for control functions and functions which may be initiated later than 8 hours after initiating event, low voltage supply is modelled from fault trees created specifically for the time window 8 – 24 hours.

4. Delays with limited capacity that allow/can buy extra time are considered for a few cases. The main case concerns depletion time of batteries which is considered with two time windows, 8 hours and 24 hours. Also, in sequences with isolated main steam lines the possibility to run main feedwater pumps until the water in the condenser is depleted is considered.
5. Dynamic mission times for redundant/diversified components are in general not considered. It is assumed that failures are instant. This means that if for example a pump fails after some time in operation after the initiating event, the redundant pump will still have to function for the full mission time, refer also to the similar case in bullet 3.
6. Time windows with different failure rates are considered for emergency diesel generators, where a higher failure rate is assumed for the first hour of operation.
7. It is in general not considered that failures in different points in time may lead to different consequences and/or success criteria, e.g. failure of core cooling is assumed to occur when the need for cooling is greatest (initially). One exception is found for spurious stop of emergency diesel generators and the following start of mobile diesel generators, where a prolonged available time to start the mobile diesels is credited due to that core cooling initially was established. There are also different success criteria for forced depressurization depending on when the auxiliary feedwater (AFW) system fails, e.g. failure of AFW level control function is assumed to occur after 12 hours in mean, which gives that the reactor pressure vessel (RPV) pressure already have been significantly reduced and hence a milder success criterion is applied for the forced depressurization.

The existing time window modelling in the Unit 2 model is performed by use of standard fault tree approaches, e.g. duplicated basic events differentiated by mission time and/or failure rate, exchange basic events and duplicated fault tree structures. The approach obviously increases the size of the PSA model, especially the number of fault trees and basic events for the electrical systems and the cable and cabinet modelling, but the model is still manageable. The only case of time window modelling that are performed by use of event trees is found for the modelling of success criteria of forced depressurization at late failure of AFW, when function event alternatives are used.

It is somewhat difficult to assess the effect of each type of performed time window modelling in Unit 2 PSA, since that would require results from a set of models with only one type of time window modelled in each. However, an indication can be given by studying importance measures for individual events. Some examples are given below based on results for Unit 2 power operation level 1, all initiators, analysis:

- **Time window for start of core cooling, 30 minutes for e.g. transients:**
  Return of offsite power within 30 minutes reduces the CDF approximately with a factor of 1.1.
- **Time window for mobile diesel generator at failure to run of emergency diesel generator**
  1 hour longer available time for manual action compared to sequences with failure to start of emergency diesel generator. Reduces the CDF approximately with a factor of 1.4.

- **Time window for emergency diesel generator failure rate, failure to run;**
  3.5 times lower failure rate for hours 2-24 compared to the first hour. Reduces the CDF approximately with a factor 1.3.

Conclusions
It was concluded in the tests regarding mission time that the assumed mission times assigned to mission failures are significant for the results. The time between the initiating event and the safe state does determine the mission times in the sequence. Therefore, a more realistic approach of modelling the time window between initiating event and safe state is very likely to be of importance to the result. Modelling dynamic mission times can also be concluded to be of importance as it could reduce the component mission times significantly.

It can also be concluded that existing time window modelling found in the Unit 2 model have significant impact on the results, and it is probable that an extended consideration of time windows in general in the model would increase the level of realism in the Unit 2 PSA. Development of time windows of types 1, 2, 5, 6 and 7 is assessed to have the largest potential for the Unit 2 model.

The studies on the Unit 2 model regarding time windows have identified the following needs and requirements on the method development:

- The analysis of time windows related to dependencies between initiating events and safe state, order and timing of event failures and the use of time-dependent failure rates should be extended.
- Consideration of limited mission time for backup functions, e.g. emergency core cooling (ECC) at failure to run of AFW or failure of AFW control functions, may have a significant impact.

The use of FT/ET approach is manageable in most cases, but will lead to significant increase in size and complexity of the PSA model. For the case of considering dynamic mission times for individual components the FT/ET approach is not considered feasible.

Success Criteria
The main part of the dominating CDF sequences in the Unit 2 PSA concerns safety functions where only one redundant train is required, e.g. 1-out-of-4 AFW trains and 1-out-of-4 residual heat removal (RHR) trains, where, naturally, the issue of dynamic success criteria is of no concern. There do however exist a few cases where the success criteria (SC), for a long term function, succeeds 1 train. The following cases where identified:

- RHR 322, SC 2/4 at low RPV pressure
- RHR 322, SC 3/4 at ATWS/ATWC,
- AFW 327, SC 2/4 at LOCAs and ATWS,
- AFW 327, SC 4/4 at ATWC.

The impact of possible dynamic success criteria has been evaluated for each case by changing the criteria k/N to k-1/N and study the impact on CDF for specific initiating events where the function has a large risk contribution. As can be seen from the results presented in Table 13, the only significant impact was given for the case where the success criterion of AFW (system 327) was changed from 4-out-of-4 to 3-out-of-4 in ATWC sequences for initiator TF. Also note that the performed test cases assume a lower SC for the complete mission time of 24 hours,

while in reality a reduced SC will only be relevant for a portion of the 24 hours mission time. Of course, the combined effect of implementing dynamic success criteria for both AFW and RHR in all sequences above would be greater, but a limited overall impact should still be expected for the Unit 2 PSA.

Table 13. Maximum change in CDF at change of success criteria from k/N to k-1/N.

	Success Criteria & Sequence				
IE	**2/4 322 at low RPV pressure**	**3/4 322 at ATWS/ATWC**	**2/4 327 at LOCA**	**3/4 327 at ATWS**	**4/4 327 at ATWC**
TF	-0.3%	0.0%		-0.6%	-5.1%
L_S0.321S.1	-0.7%				
L_S1.321S.1			0.0%		

Conclusions
Implementation of dynamic success criteria should not be performed in general but could be relevant to consider for specific safety functions and sequences.

The process of modelling dynamic SC to such limited extent, i.e. from k/N to k-1/N during 24 hours mission time, is manageable with a fault tree/event tree software (e.g. by use of safety functions with different time windows) and does not require additional methodology development.

Manual Actions
Most manual actions included in the dominating sequences of the Unit 2 at power level 1 PSA have short available time and appears in combination with one or two four-fold CCFs, e.g. of emergency diesel generators, valves or pumps in AFW or ECC, etc. In cases where the CCFs contains mission time failures, this indicates that these sequences contains conservatisms concerning available time for the manual action and the potential for increased realism may be large. There are some cases in Unit 2 PSA where this issue already has been addressed, mainly in sequences following initiators concerning severe weather conditions, e.g. FLEX sequences (see section on time windows above), Table 14 presents additional manual actions in sequences with mission time failures, which could benefit from increased realism concerning time available and repair of failed equipment.

Table 14. RDF of manual actions in sequences with mission time failures.

Manual Action	**RDF**
Manual RPV depressurization at failure to operate of AFW	1.19
Re-connection to external grid at failure to run of EDG	1.15
Start of mobile DG at failure to run of EDG	1.13
Stop of pumps in pump room H at failure of pump room cooling	1.08

As an example, the case of manual forced depressurization at failure of AFW can be mentioned. The manual action is needed in order for the low pressure ECC to succeed, and may be required at any time within the 24 hour mission time, depending on the time of failure of the AFW. The time available for the action, 34 min, is conservatively decided from the limiting case with initial failure of AFW. However, in the dominating CDF sequences involving manual depressurization, the AFW fails due to failure in control functions (regulating valves) or failure to run of AFW pumps which can occur at any time during the 24 hours mission time, i.e. the time available for the manual action is most likely significantly longer than 34 min due to earlier performed RPV level control and residual heat removal. For this specific case a related question is also at what time of AFW failure is depressurization no longer needed for success of the

ECC, i.e. how long must the AFW run before the RPV pressure falls below the ECC pressure specification.

3.2.2.4 Hypothesis testing – Unit 3, model for a PWR reactor type

Description of the model

The model represents a nuclear power plant including the spent fuel pit. The following elaborations are limited to sequences related to the spent fuel pit.

The consequences studied in the model are potential steaming by evaporation in the spent fuel pit (PST) and potential fuel damage (PFD).

The spent fuel cooling function has a low grade of atomization. The primary cooling system has two redundant trains and two diversified systems can be utilized in case of failure of the primary system. Repair is not credited for any initiating events, systems or components. Redundant trains and diversified systems have to be activated manually.

Some basic data regarding modelling of cooling of the spent fuel pool pit is presented in Table 15. The systems considered are the cooling system and all its support systems. The numbers are slightly rounded for confidentiality purposes.

Table 15. Model stats

Number of basic events	1400
Number of mission time events	680
Number of events with mission time 24 hours	660
Number of events with mission time 20 hours	6
Number of events with mission time 4 hours	6
Number of events with mission time 1 hours	3
Number of events modelling repair	0
Number of CCF groups	80

The elaborations are performed on internal events, area events and external events during power operation. Analysed consequences are potential steaming by evaporation in the spent fuel pit (PST) and potential fuel damage (PFD).

Mission Time

The main mission time that is used for components is 24 hours. A few components have been modelled with other mission times. For diesel generators and gas turbines mission time 20 hours and 4 hours are modelled. These different mission times are used for sequences with total loss of offsite power respective sequences where offsite power returns within 4 hours. Mission time 1 hour is used to represent transportation of mobile pumps that can be placed near a water resource. The function itself using mobile pumps for cooling does have mission time 24 hours.

The impact from changing mission times in scenarios leading to consequences PST and PFD is presented in Table 16.

Table 16. Mission time tests

#	Test Case Description	Result PST	Result PFD
TC1	Mission time 24 hours is reduced to 12 hours	-43%	-11%
TC2	Mission time 24 hours is increased to 48 hours	104%	28%
TC3	Mission time 24 hours is increased to 168 hours	1466%	383%

Importance values for basic events and parameters are studied to investigate the significance of mission time events and parameters. The importance of a basic event is ranked according to the fractional contribution (FC) or the risk increase factor (RIF). The importance of parameters is ranked accordingly. The FC and RIF for basic events are summed for each component. According to NEI 00-04 significant contributors can be identified as components and parameters with FC>0.5% and RIF>2. For CCF groups significant contributors are defined for RIF>20.

For scenarios with consequence PST in power operation in total 37 components have a summed FC of 0.5% or greater. Out of these components, 12 are modelled as mission time events. 271 components have a RIF of 2 or greater and 95 out of these components are modelled as mission time events. The mission time parameter 24 hours has the second greatest FC and highest RIF of all parameters in the spent fuel pool model.

For CCF groups in the analysis of consequence PST 12 CCF groups have a FC>0.5% where half of these are mission failures and half are failures on demand. The dominating CCF group with a FC over 70% models mission failures. This same CCF group also has a significantly higher RIF than other CCF groups. In total 13 CCF groups have a RIF>20 out of which 7 are failures on demand and 6 are mission failures.

For scenarios with consequence PFD in power operation in total 69 components have a summed FC of 0.5% or greater. Out of these components, 25 are modelled as mission time events. 339 components have a RIF of 2 or greater and 102 out of these components are modelled as mission time events. The mission time parameters 24 hours, 20 hours and 4 hours have a FC>0.5%. The mission time parameter 1 hour has a lower FC. All mission time parameters have a RIF>2.

For CCF groups in the analysis of consequence PFD 17 CCF groups have a FC>0.5% where six of these are mission failures. In total 22 CCF groups have a RIF>20 out of which eight are mission failures.

Events in an MCS list can be separated in to the following four main types of events:

- Initiating event
- Failure on demand
- Mission failures
- Unavailability

For consequence PST the type of MCS that contributes with more than 1% to the total consequence frequency are combinations of the following type of events. Within the parenthesis it is denoted which event model is used.

Power operation:

- **Initiating event** (Frequency), **Mission failure** (Mission Time)
- **Initiating event** (Frequency), **Unavailability** (Probability), **Mission failure** (Mission Time)
- **Initiating event** (Frequency), **Mission failure** (Mission Time), **Failure on demand** (Tested)

Outage:

- **Initiating event** (Frequency), **Unavailability** (Probability), **Failure on demand** (Tested)

- **Initiating event** (Frequency), **Mission failure** (Mission Time)
- **Initiating event** (Frequency), **Unavailability** (Probability)

For consequence PFD the type of MCS that contributes with more than 1% to the total consequence frequency are combinations of the following type of events. Within the parenthesis it is denoted which event model is used.

Power operation:

- **Initiating event** (Frequency), **Unavailability** (Probability), **Mission failure** (Mission Time)
- **Initiating event** (Frequency), **Unavailability** (Probability), **Failure on demand** (Tested)
- **Initiating event** (Frequency)

Outage:

- **Initiating event** (Frequency), **Unavailability** (Probability), **Failure on demand** (Tested), **Mission failure** (Mission Time)
- **Initiating event** (Frequency), **Unavailability** (Probability), **Failure on demand** (Tested)
- **Initiating event** (Frequency), **Unavailability** (Probability), **Mission failure** (Mission Time)

Conclusions

Mission time events are significant contributors to the results in the Unit 3 spent fuel pool study. It can be concluded that the selected mission times modelled is of great significance to the results.

The conclusion from this model evaluation is hence that following needs and requirements on the method development has been defined:

- The method should manage mission times in a less conservative manner than the traditional static PSA representation.

Crediting repair

Repair is not credited for any initiating events, systems or components. In Unit 3 the spent fuel pool study the available times for manual actions are long. Time to boil (PST) is 79h during power operation and time to potential fuel damage (PFD) is much longer (at least in the scale of several days). There should be a good chance to repair within this time window. At the same time, if loss of residual heat removal (caused by failure in a train in operation), redundant pumps and heat exchanger in stand-by can be started (1 of 2 trains is enough to avoid boiling in spent fuel pool). These actions are modelled in the Unit 3 model (BE for diagnosis and decision and separate BE for the different operator actions). The available time should, with a good margin, be long enough for both trying repair and activating redundant trains and systems for residual heat removal although the personnel for the different activities probably are common. However, note that there should be a strong dependency between the current operator actions (regarding starting standby pump/heat exchangers) and the repair (diagnosis, decision and action/execution).

Conclusions

Repair could be modelled for sequences in the spent fuel pool since time windows are very long. However, it is very important to consider dependencies between current HFEs regarding e.g. decision making and actions to start standby systems and potential repair actions.

Time Windows

The following can be noted on the modelling of different types of time windows in the Unit 3 model (bullets 1-7 refer to the type of time window that are defined in the beginning of Section 3.2.2.1):

1. The time between all initiating events and the safe state is modelled as a constant time of 24 hours that is derived from the PSA level 1 modelling. Hence this time window is modelled with no dependency to the specific sequence of events. This time window of 24 hours is not necessary as to be seen as the time when the safe state has been reached. It is assumed that if the undesired consequence can be avoided for this time period, the likelihood that it will occur after this time is considered negligible.
2. Static mission times are modelled for component mission failures. This means that the mission time is not dependent to the timing of other events in the sequence.
3. A time window before a component/system must be started is not explicitly considered. All events occurring after the initiating event in the MCS are assumed to be simultaneous and the order of the events is not considered. The time window before a component must start is to a limited extent considered inexplicitly when estimating manual action failure probabilities.
4. Delays with limited capacity that allow/can buy extra time are not credited. It has for example not been examined how much time the cooling water tank could buy if it would still be possible to pump in that water to the fuel pool with failures that lead to loss of heat sink. The diversified cooling systems that are modelled also have water tanks with a finite amount of water. However, these tanks contain sufficient amount of water to supply the spent fuel pools during the modelled time window of 24 hours.
5. Dynamic mission times for redundant/diversified components are not considered. It is assumed that failures are instant. This means that if for example a pump fails after some time in operation after the initiating event, the redundant pump will still have to function for the full mission time, refer also to the similar case in bullet 3.
6. Time windows with different failure rates are not considered in the model for any components.
7. It is not considered that failures in different points in time may lead to different consequences and/or success criteria, e.g. failure of components are assumed to be instant which leads to the worst consequence.

Conclusions

No testing has been performed on the importance of the simplifications made regarding time windows apart for the tests for mission time.

It was concluded in the tests regarding mission time that the assumed mission times assigned to mission failures are significant for the results. The time between the initiating event and the safe state does determine the mission times in the sequence. Therefore, a more realistic approach of modelling the time window between initiating event and safe state is very likely to be of importance to the result. Modelling dynamic mission times can also be concluded to be of importance as it could reduce the component mission times significantly.

It can be concluded that time windows of type 1,2, 3 and 5 are of great importance to the results when the modelled scenarios contain long time windows as they have an impact on mission times.

Time windows of type 4, 6 and 7 have not been elaborated on and the importance of these could be evaluated further. It can however be concluded that these potentially could have a significant impact on the results as possibilities to credit these types of time windows have been identified in the Unit 3 model.

The studies on the Unit 3 model regarding time windows have identified the following needs and requirements on the method development:

- Time windows related to dependencies between initiating events, safe state and order and timing of event failures should preferably be analysed in a more realistic way.
- Limited delays that can allow extra time, time-dependent failure rates and success-criteria depending on failure times of other safety functions could be of importance and would be good to evaluate with a method that allows the analyst to credit these.

Success Criteria
There are no requirements for two redundant trains in the Unit 3 spent fuel pool model. No tests have been performed on changing success criteria in the Unit 3 model.

Manual Actions
The available time for manual actions is generally short for most categories of initiating events (internal events).

The category of initiating events caused by external events can be expected to be characterized by long time windows. But in the Unit 3 PSA study the analysis of external events is simplified and is only considering screening values for human failures (where no time windows are considered in used HEPs).

In the analysis considering spent fuel pool the available time is long and manual actions are dominating the results. The available time from an initiating event, that causes total loss of residual heat removal in the spent fuel pool, before a manual action must be taken is more than 79 hours (time to boil is 12 hours during shutdown and 79 hours during power). Time to potential fuel damage (PFD) is not specified but is assumed to be much longer. In these sequences HEP values are estimated with range of 1E-2 to 1E-4. Repair is not considered, neither is recovery of the human failure event considered.

In general, the analysis of human actions has not been updated for a long time (except manual action connected to events in spent fuel pool.

3.2.2.5 Hypothesis testing – Unit 4, model for a spent fuel pool facility

Description of model
The model represents a spent fuel pool facility where the risk is evaluated both regarding the process of the transport containers and fuel elements handling, as well as for the long-term storage in spent fuel pools. The studied end-states and sequences depend on where in the facility the spent fuel is situated. The main consequences studied in the model are small releases (A1), large releases (A3) and boiling in the storage pool (KF).

The facility has a low grade of atomization and redundancies. Available time for recoveries and repairs is generally long in many of the studied sequences. Repairs are considered for selected components that have shown to be important to avoid too conservative results. Repair is also considered for some initiating events. Repairs are modelled explicitly in the fault and event trees with a probability of failure to repair.

Some basic model data is presented in Table 17. The numbers are slightly rounded for confidentiality purposes.

Table 17. Model stats

Number of basic events	1000
Number of mission time events	400
Number of events with mission time 720 hours	230
Number of events with mission time 72 hours	3
Number of events with mission time 12 hours	150
Number of events with mission time 1 hours	30
Number of events modelling repair	20
Number of CCF groups	20

The elaborations are performed on internal events. Area events and external events are discussed briefly with regard to some of the topics. Analysed consequences are radioactive release and boiling in the fuel storage pool.

Mission Time

The model has two main requirements on mission times for components, depending on which function is modelled. These are 12 hours and 720 hours respectively. Components with mission time 12 hours are related to the ordinary functions that provide cooling for the transportation containers in certain steps of the transportation process. These are scenarios leading to the consequence large release (A3). Mission times 720 hours are used for the emergency cooling of transportation containers, emergency cooling of fuel transported in the fuel hoist and cooling of fuel storage pools.

For batteries required for diesel start-ups a 1-hour mission time is modelled.

The main consequences studied in the model are small release (A1), large release (A3) and boiling in the storage pool (KF). For small releases, which mostly is caused by dropped fuel elements, no events are modelled with mission time. Hence this consequence is not impacted by changes of mission times. Elaborations are performed with increased mission times as well as decreased mission times. The impact from changing mission times in scenarios leading to consequences A3 and KF is presented in Table 18.

Table 18. Mission time tests

#	**Test Case Description**	**Result KF**	**Result A3**
TC1	Mission time 720 hours is reduced to 72 hours	-77%	-3%
TC2	Mission time 720 hours is reduced to 360 hours	-42%	-2%
TC3	Mission time 720 hours is increased to 1440 hours	85%	4%
TC4	Mission time 12 hours is reduced to 6 hours	0%	-6%
TC5	Mission time 12 hours is increased to 24 hours	0%	13%
TC6	Mission time 12 hours is increased to 120 hours	0%	172%

Importance values for basic events and parameters are studied to investigate the significance of mission time events and parameters. The importance of a basic event is ranked according to the

fractional contribution (FC) or the risk increase factor (RIF). The importance of parameters is ranked accordingly. The FC and RIF for basic events are summed for each component. According to NEI 00-04 significant contributors can be identified as components and parameters with FC>0.5% and RIF>2. For CCF groups significant contributors are defined for RIF>20.

For scenarios with consequence A3 all four defined mission time parameters are used (720 hours, 72 hours, 12 hours and 1 hour). In total 32 components have a summed FC of 0.5% or greater. Out of these components, 11 are modelled as mission time events. 64 components have a RIF of 2 or greater and about half out of these, 35 components, are modelled with mission time. All mission time parameters except 1 hour mission time have a FC greater than 0.5%. All mission time parameters have RIF greater than 2, and the mission time parameter 12 hours has the third greatest RIF of all parameters in the model.

For scenarios with consequence KF, the parameter with the greatest fractional contribution is the mission time parameter of 720 hours (30 days). No other mission time parameters are used for these scenarios. This parameter also has the greatest FC and RIF out of all parameters. In total 52 components have a summed FC of 0.5% or greater. Most of these, 40 components, are modelled as mission time events. 188 components have a RIF of 2 or greater and over half of these, 98 components, are modelled with mission time. For these scenarios, all with mission time 30 days, the chosen mission time is evidently of great significance, if not dominating, to the final results.

For CCF groups in the analysis of consequence A3 only one CCF group has a FC>0.5%. This CCF group models failures on demand. Six CCF groups have a RIF greater than 20, and four out of these model mission failures. There are only 8 CCF groups that are modelled in the analysis of consequence KF. Out of these four groups have a FC>0.5 and two groups have RIF of 20 or greater. All the identified significant CCF groups are mission failures.

Events in an MCS list can be separated in to the following four main types of events:

- Initiating event
- Failure on demand
- Mission failures
- Unavailability

For consequence A3 the type of MCS that contributes with more than 1% to the total consequence frequency are combinations of the following types of events. Within the parenthesis it is denoted which event model is used.

- **Initiating event** (Frequency), **Unavailability** (Probability)
- **Initiating event** (Frequency), **Unavailability** (Probability), **Failure on demand** (Tested)
- **Initiating event** (Frequency), **Unavailability** (Probability), **Mission failure** (Mission Time)
- **Initiating event** (Frequency), **Unavailability** (Probability), **Failure on demand** (Tested), **Mission failure** (Mission Time)

For consequence KF the type of MCS that contributes with more than 1% to the total consequence frequency are combinations of the following types of events. Within the parenthesis it is denoted which event model is used.

- **Initiating event** (Frequency), **Unavailability** (Probability), **Mission failure** (Mission Time)
- **Initiating event** (Frequency), **Unavailability** (Probability), **Failure on demand** (Tested)

Conclusions
It is evident that the values of mission times modelled are of significance to the results, especially when addressing longer mission times. Furthermore, mission time events are common in the dominating MCS for consequence KF and are therefore of importance for the results. Investigations (made by Unit 4) have also identified the need to further investigate the mission time aspect on the results.

The conclusion from this model evaluation is hence that following needs and requirements on the method development has been defined:

- The method should manage mission times in a less conservative manner than a static PSA.

Crediting repair
In the studied model repairs are already considered for a few components, as without crediting repair of some components the result would be greatly conservative. Repairs are only considered in sequences leading to consequence KF. The available time for the credited repairs is in the scale of several days.

Repair is credited by including basic events in the fault tree model representing the probability of failure to repair. The estimated failure probabilities lie within a span from 1E-5 to 1E-2. Some sensitivity studies where the failure probabilities for repair are altered have been performed in the Unit 4 model to investigate the significance of repair. It should be noted that the current study only credits some possibilities to repair and it is potentially possible to credit repair for more components. The different test cases and the impact on the frequency are presented in Table 19.

Table 19. Repair tests

#	Test Case Description	Impact on result KF
TC1	No credit of repair	5300%
TC2	All repair failure probabilities are doubled	197%
TC3	All repair failure probabilities are reduced to half	-86%

From the list of typical dominating MCS in the previous chapter it can firstly be noted that repair already is credited for some of the dominating MCS. Secondly events that generally are repairable such as mission time events and failures of periodically tested components are common in the dominating MCS.

Repair of components affected by area events such as fire and flooding has also been proved to be of great importance as the facility have a low level of redundancy and separation. Repairs for fire and flooding events have to some extent been modelled conservatively as it is of great significance to the result.

Repair has only been considered for a few selected components in the Unit 4 study as the result would have been too conservative. Hence repair can potentially be credited for additional components. In the study it has also been identified cases where crediting a potential repair could decrease the mission time for other components significantly, but this has not been included in the study as of now.

It is not considered in the study whether several repairs are required within the same time period. Neither is repair of CCF events addressed separately. CCF events are not dominating the results for consequence KF. Sequences that involve two-fold (or higher) CCFs contribute with less than 2% to the total frequency.

Conclusions
Repair has to some extent been considered in the Unit 4 PSA model as it was concluded in this PSA study already that repair is one of the central issues in sequences leading to consequence KF. In these sequences the available time is long (several days) and it is reasonable that there is a good chance to repair within this time window. It can be concluded that without considering repair the results would be undesirably conservative.

The sensitivity studies on the Unit 4 model has identified the following needs and requirements on the method development:

- It must be possible to credit repair of initiating events/components.

Time Windows
The following can be noted on the modelling of different types of time windows in the Unit 4 model (bullets 1-7 refer to the type of time window that are defined in the beginning of Section 3.2.2.1):

1. The time between the initiating event and the safe state is modelled as a constant time that is derived from deterministic criteria. Hence this time window is modelled with no dependency to the specific sequence of events. This time window of 24 hours is not necessary as to be seen as the time when the safe state has been reached. It is assumed that if the undesired consequence can be avoided for this time period, the likelihood that it will occur after this time is considered negligible.
2. Static mission times are modelled for component mission failures. This means that the mission time is not dependent on the timing of other events in the sequence.
3. A time window before a component/system must be started is not explicitly considered. All events occurring after the initiating event in the MCS are assumed to be simultaneous and the order of the events is not considered. The time window before a component must start is to some extent considered inexplicitly when estimating repair failure probabilities for components where repair has been credited.
4. Delays with limited capacity that allow/can buy extra time is not credited. It has for example not been examined how much time the cooling water tank could buy if it would still be possible to pump in that water to the fuel pool with failures that lead to loss of heat sink. A diversified system which provides possibilities to pump in cooling water with external pumps has not been credited in the analysis. This system could potentially extend the allowed time for repair of the primary cooling system.
5. Dynamic mission times for redundant/diversified components are not considered. It is assumed that failures are instant. This means that if for example a pump fails after some

time in operation after the initiating event, the redundant pump will still have to function for the full mission time, refer also to the similar case in bullet 3.

6. Time windows with different failure rates are not considered in the model for any components. In some sequences in the Unit 4 model the cooling pumps are required to run for 30 days.
7. It is not considered that failures in different points in time may lead to different consequences and/or success criteria, e.g., failure of cooling of spent fuel transportation container is assumed to occur when the need for cooling is greatest (initially).

Conclusions

No testing has been performed on the importance of the simplifications made regarding time windows apart for the tests for mission time, see the previous section on mission time.

It was concluded in the tests regarding mission time that the assumed mission times assigned to mission failures are significant for the results. The time between the initiating event and the safe state does determine the mission times in the sequence. Therefore, a more realistic approach of modelling the time window between initiating event and safe state is very likely to be of importance to the result. Modelling dynamic mission times can also be concluded to be of importance as it could reduce the component mission times significantly.

It can be concluded that time windows of type 1, 2, 3 and 5 are of great importance to the results when the modelled scenarios contain long time windows as they have an impact on mission times.

Time windows of type 4, 6 and 7 have not been elaborated on and the importance of these could be evaluated further. It can however be concluded that these potentially could have a significant impact on the results as possibilities to credit these types of time windows have been identified in the Unit 4 model.

The studies on the Unit 4 model regarding time windows have identified the following needs and requirements on the method development:

- Time windows related to dependencies between initiating events, safe state and order and timing of event failures should preferably be analysed in a more realistic way.
- Limited delays that can allow extra time, time-dependent failure rates and success-criteria depending on failure times of other safety functions could be of importance and would be good to evaluate with a method that allows the analyst to credit these.

Success Criteria

There are no requirements for two redundant trains in the Unit 4 model. No tests have been performed on changing success criteria in the Unit 4 model.

Manual Actions

For sequences leading to consequence KF the dominating manual actions are repair actions in the Unit 4 model. Sequences with repair events combined with mission time events contribute with more than 40% to the total frequency for consequence KF. Studying these sequences in detail it can be concluded that the mission failures will allow extra time for the repair. The available time for repair could potentially be prolonged up to five times.

For sequences leading to consequence A3 no repair is modelled but other manual actions are significant to the results. Sequences with manual actions combined with mission time events contribute with more than 22% to the total frequency for consequence A3.

Manual actions in combination with CCF events are not among the dominating sequences and have not been studied further.

Conclusions
It has not been explicitly tested how great impact a more realistic approach of sequences containing manual actions in combination with mission failures would yield. However, it can be concluded that these sequences contribute significantly to the results and also that the mission failures indeed in most cases would allow extra available time for the manual actions.

The studies on the Unit 4 model regarding time windows have identified the following needs and requirements on the method development:

- The method should consider available time for manual actions in a more realistic way. Specifically, in sequences containing manual actions combined with mission failures the available time for manual actions can potentially be too conservative in static ET/FT modelling.

3.2.2.6 Conclusions from hypothesis testing

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 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 (Tyrväinen et al., 2019). Also, some general requirements regarding feasibility etc. are formulated in this chapter.

3.2.3.1 General requirements

The chosen methods must be feasible for use in the sense of workload and integration with already used methods and software (RiskSpectrum and FinPSA). This means that the methods should be compatible with the existing fault tree and event tree modelling, either implemented in the FT/ET model or with an add-on tool.

3.2.3.2 Repair modelling requirements

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.

Cases where repair modelling needs to be applied include at least:

- Repair of an initiating event, e.g. to restore spent fuel pool cooling
- Repair of a component after a single failure to recover a failed safety function
- Repair of a component after a CCF to recover a failed safety function
- Repair of multiple components after a CCF to recover a failed safety function

Other potential repair modelling cases include:

- Repair of a component after multiple single failures to recover a failed safety function
- Repair of multiple components after multiple single failures to recover a failed safety function
- Repair of a component to recover a degraded safety function, e.g. a safety function with 2-out-of-4 criterion operating with only one train
- Repair of a component in a system still operating by other components, i.e. repair can be done before complete failure of the system

Other issues that may need to be considered:

– Modelling of another failure after a repair. Failure rate can also be different after repair.
– Impact of non-simultaneous CCFs on repair modelling.

3.2.3.3 Time window modelling requirements

There is generally a need to treat mission times and other time windows in less conservative manner. 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.

There may also be a need to credit limited delays that can allow extra time e.g. for manual actions.

3.2.3.4 Dynamic success criteria modelling requirements

A dynamic success criterion is a success criterion that changes during the mission time. For example, two cooling water pumps may be needed in the beginning of an accident for sufficient cooling, but later as the amount of residual heat decreases only one pump may be sufficient. Dynamic success criteria have been rarely modelled in PSA. Typically, conservative static success criteria are used, e.g. that two pumps are required for the whole mission time regardless of the decrease in residual heat. 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.

At this point, it is unclear

- whether dynamically varying time windows related to dynamic success criteria need to be modelled, e.g. that the time point when a success criterion changes varies based on some conditions, e.g. related to accident progression.
- what types of repairs need to be modelled in combination with dynamic success criteria.
- whether non-simultaneous CCFs need to be modelled in combination with dynamic success criteria.
- whether cases where a success criterion changes more than once need to be modelled.
- whether combined dynamic success criteria of multiple systems, e.g. two different water cooling systems, need to be modelled.

3.3. Methods, HRA

3.3.1 Qualitative HRA for Long Time Window Modelling

The qualitative part of the HRA process is as important as the quantitative part, if not even more important. For Category C HFEs with long time window, it could have large uncertainties in the quantitative HEP results as the scenarios and PSFs could have large variances in longer time window. Thus, it is important to have a proper qualitative HRA.

It is suggested to perform the following steps as qualitative HRA

1. HFE identification and definition
2. HFE data collection
3. Task analysis, including timeline analysis and teamwork diagram
4. PSF assessment

3.3.1.1 HFE identification and definition

The identification and definition of the Category C HFEs with long time window, is the same as the other Category C HFEs. The set of operator responses required to control and safely shutdown the plant following an initiating event is generated by reviewing all relevant operating procedures (e.g. emergency operating procedures, abnormal operating procedures, and annunciator response procedures) to determine what actions are required as a function of the plant status represented in the development of the accident sequences.

Typical post-initiating HFEs related to PROSAFE were collected and reviewed from the stakeholder PSA/HRA studies. The review identified the following types of HFEs:

- Late Level 1 or Level 2 (post-core damage) HFEs
- Spent fuel pool/storage pool related HFEs
- Spent fuel handling HFEs
- Diverse and Flexible Coping Strategies (FLEX) HFEs

- Recovery action failures (to be further evaluated)
- Repair failures

When there are much longer available times in the scenario, potential new human actions can be considered, e.g., recovery actions, repair actions and their dependencies with existing actions. These new actions are considered for the significant scenarios. The determination of which scenarios are significant is to be performed together with the PSA engineers using the plant PSA model.

A Revised Systematic Human Action Reliability Procedure (SHARP1, EPRI TR-101711, 1992) proposed the following questions to determine the feasibility of recovery actions in the significant scenarios:

- Can the crew diagnose the need for recovery?
- Can it be accomplished in the time available?
- Can the equipment be put in functional condition by personnel?
- Can the crew gain access to the equipment?
- Are the required staff (with the right skills) available?

If it is possible to consider multiple recoveries (i.e., several recoveries to be credited in one accident sequence/cut set), the analyst should consider that one recovery may be tried (perhaps even multiple times) and then the second recovery may be tried but with less time and possibly less resources available because of the attempts on the first recovery. Hence, the failure probability of the second recovery should be based on more pessimistic characteristics (e.g., less time available, less resources) than if such a possibility is considered alone.

Similar as recovery action, it is suggested to determine the feasibility of repairs in 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?

It might be worth to discuss whether in some long time window situations errors of commissions (EOCs) are likely and might have an unignorable impact on the risk evaluation. Following the findings of the NPSAG EOC projects, EOCs are not important contributors in level 1 internal event PSA (He & Olofsson, 2019). The identification of EOCs can be focused on level 2 or external hazards PSA when significant mismatches can occur between the scenario conditions and the crew's understanding of those conditions.

3.3.1.2 HFE data collection

One of the first steps in the HRA process is to collect the necessary information/data. According to EXAM-HRA, the data is divided into the following three headings (Johanson et al., 2015):

- Plant organization & Management
- Task specific information
- Task context.

Plant organization and management could have large impacts in the HFEs with long time window. However, many of the currently available HRA methodologies need to be further developed in order to quantitatively address aspects of organizational nature. It is thus important for HRA analysts to understand possible influences that the organization as a whole can have on the specific operator action that is being analysed. This is especially important when it comes to aspects related to decision making, i.e. how and by whom a certain decision is made about starting or stopping a certain function in a given scenario and how tasks are distributed across different actors.

The task specific information should include how the work is distributed within the control room team or the shift during accident conditions. In relation to the latter aspect it is important to understand what parallel duties exist for the shift leader and the deputy shift leader; to what extent they are available for either work in parallel to mitigate the accident, or as personnel redundancy for the operators. It is also important to understand when additional resources will become available (especially during long term scenarios), like shift technical advisor, crisis management staff, picket engineer, etc.

Task Context: the modelling of human interactions must consider the context of the task in the relevant accident scenario or sequence of events. Understanding an accident sequence context is a complex, multifaceted process. The following characteristics (among others) need to be understood and reflected upon, as necessary, in the model of a specific human action or group of actions:

- plant behaviour and conditions,
- timing of events and the occurrence of cues triggering human action,
- parameter indications used by the operators and changes in those parameters as the scenario proceeds,
- time available and locations of controls and equipment necessary to implement the human actions,
- equipment available for use by the operators based on the sequence,
- environmental conditions under which the decision to act must be made and the actual response must be performed,
- degree of training, guidance, and procedure applicability,
- additional tasks of the control room team, which are not directly related to the task concerned (either external communication or additional tasks due to accident sequence).

3.3.1.3 Task analysis

In the book “A Guide to Task Analysis” (Kirwan, 1992), task analysis is described as follows: Task analysis covers a range of techniques used by ergonomists, designers, operators and assessors to describe, and in some cases evaluate, the human-machine and human-human interactions in systems. Task analysis can be defined as the study of what an operator (or team of operators) is required to do, in terms of actions and/or cognitive processes, to achieve a system goal. Task analysis methods can also document the information and control facilities used to carry out the task.

In HRA, task analysis should be performed to identify the critical steps and the driving PSFs for the identified HFE. The personnel involved, the potential operator errors and recovery

mechanism should be discussed. Task analysis can be documented either in a Hierarchical Task Analysis (HTA) or in a Tabular Task Analysis (TTA).

EXAM-HRA provides example of HTA figure and TTA table (Johanson et al., 2015). HTA describes the task from its top-level goals down to the level of individual operations. The TTA takes each particular task step or operation and considers specific aspects, such as: Who is doing the operation? What displays are being used? What feedback is given? What errors could occur? What opportunities for recovery? The table column titles will vary depending on the purpose of the task analysis. Example of a tabular task analysis (TTA) structure is shown in Table 20.

The combination of using a HTA and TTA is a very powerful tool, since HTA gives the analyst a firm basis for understanding the system, while the TTA, on the other hand, can be used first systematically to investigate the ergonomics aspects of the system and then to justify problems identified on the grounds of likely consequences or errors.

Table 20. Example of tabular task analysis (TTA) structure

Task step no.	Task Goal	Information available to the operator	Required action	Feedback	Communications	Possible errors, distractions, time available, skills/knowledge required
#	xxx	xxx	xxx	xxx	xxx	xxx

In addition to HTA and TTA, for HFEs with long time window, it is suggested to perform the timeline analysis for estimating times for all steps included in the task. A timeline analysis can help to understand the relationship between operator actions, the time required to perform the necessary actions and the time available to the operator to perform these actions.

The timeline is intended to capture the crew response, so aspects of the context, such as sufficiency of manpower, influence of distractions, workload, and prioritization of actions, are implicitly assessed in the construction of the timeline as the timeline must consider who-does-what-when.

When the available time is large, the personnel shift switch-over and its impact should be evaluated. A new shift will increase the opportunity to recovery 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.

NUREG-1921 (NUREG-1921, 2012) provides a timeline illustration diagram (Figure 5) for a specific HFE.

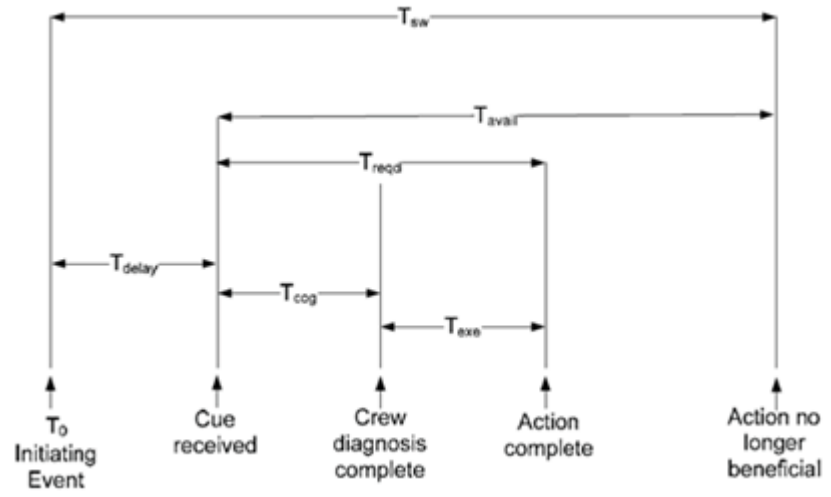

Figure 5. Timeline illustration diagram (NUREG-1921)

A timeline for a specific HFE can be illustrated in different ways, for example it can also be illustrated in a table in which the time elapsed, the estimated durations (estimated required time), and the important Crew response/Key plant events can be described.

An example timeline for an example HFE from the US NRC new developed HRA method called IDHEAS (NUREG-CR 2199, 2017) is illustrated in Table 21.

Table 21. Example timeline for the example HFE (IDHEAS, NUREG-CR 2199).

7'		Crew resp.	STA arrives after approx. 5 minutes after being called shortly after reactor trip (1 minute after reactor trip).
13'	6 mins. (after STA arrival)	Crew resp.	Enter ES-01 and begin monitoring the CSFST. Determine that the criteria for the "red path" of heat sink CSFST are met, which they will be for this scenario as determined by the PRA scenario definition and the associated T/H analysis. Under this condition, the CSFST instructs the crew to transfer to FR-H1. (CRD Node 4) The crews would be expected to enter ES-01 at latest 5 minutes after the reactor trip (i.e., at T=6'). However, the duration of interest in this part of the response concerns the monitoring of the CSFST, the determination of the Heat Sink status (that there is a Loss of Heat Sink), and the decision to transfer to FR-H1. As noted in the documentation of this node, the performance of ES-01 may compete with the CSFST monitoring although the latter is the responsibility of the STA while the crew focuses on the former.
17'	4 mins.	Crew resp.	Entry to FR-H1, "Loss of Secondary Heat Sink." Performance of initial steps in this procedure until FR-H1 Step 2. Guided by Step 2, the crew decides to establish F&B and transfers to FR-H1 Step 10, which guides the initiation of F&B. (CRD Node 5).
25'	8 mins.	Crew resp.	Implement F&B per FR-H1 Steps 10-13. (CRD Node 6).

The crew response diagram can also be illustrated in a timeline (NUREG-CR 2199, 2017), see Figure 6 below.

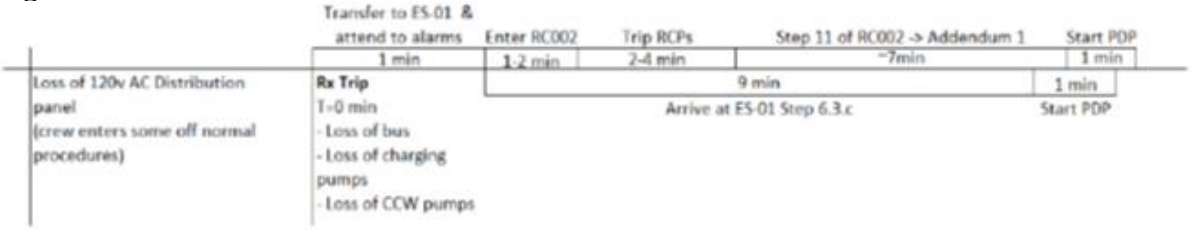

Figure 6. Timeline for loss of seawater (IDHEAS, NUREG-CR 2199)

Petro-HRA provides a typical timeline diagram which illustrates the key task steps and the responsible personnel along with the time sequences (Bye et al., 2017), see Figure 7 below. This timeline is recommended when different personnel (crews) are involved in different task steps.

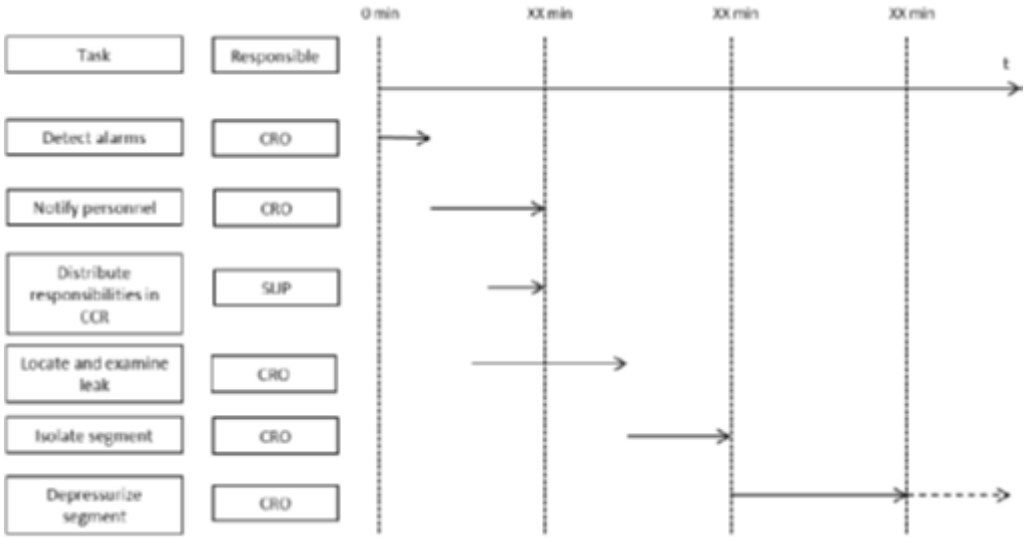

Figure 7. A typical timeline in Petro-HRA

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. An example of teamwork diagram is provided in IDHEAS-G (NUREG-2198, 2019), for the nuclear power plant crisis management teamwork, which is adapted from Le Bot et al. (Le Bot et al., 2016). In an NPP emergency, different operational states of the facility are anticipated. Figure 8 shows the teamwork diagram for the situation.

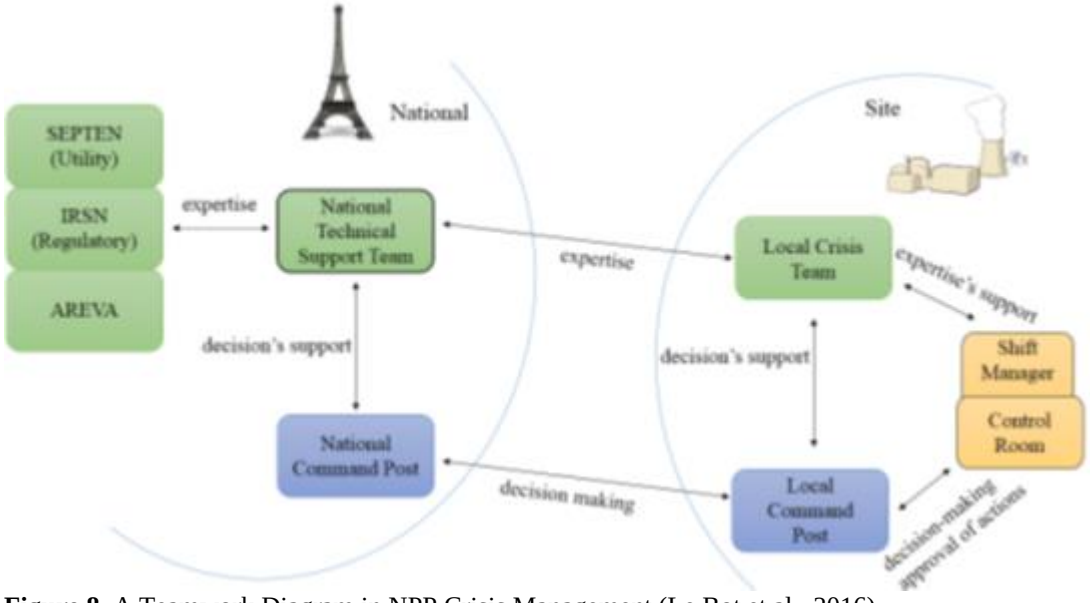

Figure 8. A Teamwork Diagram in NPP Crisis Management (Le Bot et al., 2016)

3.3.1.4 PSF assessment

During the HRA assessment it should be determined whether a PSF plays a strong, weak, negative, neutral (or not applicable), or positive influence, regardless of the HRA quantification method/tool.

PSF assessment is typically performed in the task analysis for the identified critical steps. If the SPAR-H method is selected, the PSF assessment should be performed for the tasks represented by the defined HFE as a whole.

This section tries to list the PSFs that are relevant for the HFEs with long time window. Obviously for the HFEs with long time window, the PSF of time is positive. So it is particularly important to evaluate the other relevant PSFs and their impact. It is noted that there could be large uncertainties for PSFs in long time window scenarios, thus it is important to discuss these uncertainties in the qualitative analysis.

The ASME/ANS PRA standard (ASME/ANS RA-Sa-2009) and HRA Good Practices (NUREG-1792) listed a number of plant-specific and scenario-specific performance shaping factors. The following PSFs are listed (with some modifications):

- quality [type (classroom, simulator, on the job, mental) and frequency] of the operators' training and experience on the response as the operators' knowledge and skills for the task
- quality of the procedures/instructions and how they are implemented
- availability of instrumentation needed to take corrective actions
- degree of clarity of cues/indications
- quality of the human-machine interface (equipment, controls, hardware, software, and all equipment where the operator receives information and with which carries out tasks)
- time available and time required to complete the response
- complexity of the required response (goal, scope, structure, dynamics)
- possible conflicts in the mitigation measures and priority strategies
- environment (e.g., lighting, heat, radiation) under which the operator is working
- accessibility of the equipment requiring manipulation
- necessity, adequacy, location, and availability of special tools, parts, clothing, etc.
- the perceived threat stress (the perception that own or other people's self-esteem, status, or lives could be in danger)
- attitudes to safety (safety conscious work environment, mindfulness)
- corporate support (explicit support exists for the response)
- teamwork (leadership, backup, adaptiveness, trust, and communication required for achieving common tasks)
- workload (staff available for the action and multiple and/or parallel tasks)

3.3.2 Quantitative HRA for Long Time Window Modelling

3.3.2.1 Discussions on the existing HRA Quantification Methods

HRA in PROSAFE focuses on the category C human actions in the scenarios where the time available for the actions is typically prolonged, e.g. in a range from 2 hours to a few days.

For the diagnosis part, the available time has always been an important factor. Some HRA methods consider time as the dominant factor in diagnosis HEP estimation, e.g. human

cognitive reliability (HCR)/operator reliability experiments (ORE) (Parry et al., 1992) or time reliability curve (TRC) in THERP (NUREG/CR-1278, 1983). Some HRA methods consider time as one of the PSFs, e.g. SPAR-H (NUREG/CR-6883, 2005).

In general the time reliability curves used in HRA assume that the probability of a human failure event (its cognitive part and execution part) will be lower when the available time is longer. Figure 9 presents the TRC used in THERP for diagnosis HEPs. The nominal median HEP is 1E-4 for diagnosis of the first initiating event 60 minutes after the event cues (signals) appear in the main control room. The HEP will be lower when the time is longer.

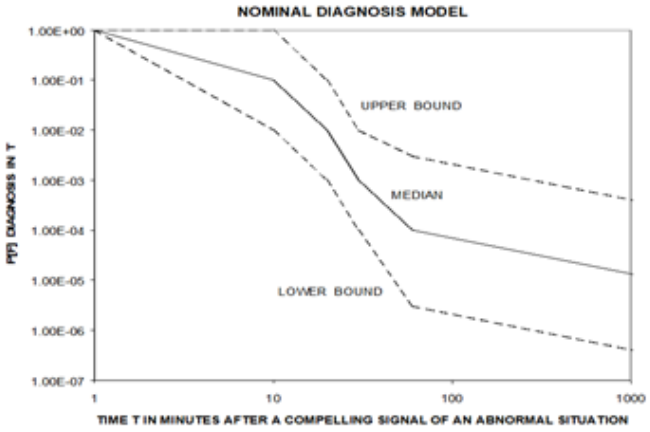

Figure 9. Time reliability curve used in THERP for diagnosis human error probabilities (NUREG/CR-1278)

The time reliability curve is mainly based on the operator data from the simulators within a relatively short time frame (within the first 1-2 hours after the initiating event). As NUREG-1792 pointed out, if the time available far exceeds the time required and there are not multiple competing tasks, the estimated HEP is not expected to be strongly influenced by this factor. This is the main reason that the TRC is not applicable for such HFEs and usually a cut-off HEP is used in practices. Typically, 1E-4 is used for diagnosis cut off probability to avoid too low probability values which are difficult to justify.

The cause based decision tree (CBDT) method was intended to address actions with longer time frames that were outside the valid range of extrapolation for the monotonically decreasing HCR/ORE TRC (Parry et al., 1992). CBDT considers a relatively large set of potential PSFs and operator influences (e.g., quality of training, procedures, the human-machine interface, recovery potential) and uses a series of decision trees to establish the HEP. However, CBDT appears to be a method for treating post-initiator control room actions only (guidance and data for quantifying local actions is not provided) through a time-independent quantification approach. In that approach, time is considered qualitatively in addressing the potential for self-recovery of an error or recovery by another crew member. As a result, any analytical (i.e., not based on plant specific human error data) non time-related HRA method could be used for treating longer time frames in the way CBDT does.

In SPAR-H the available time is one of the eight PSFs in the HEP estimation. With the expansive time, the multiplier can be 0.1 to 0.01 for the diagnosis (nominal diagnosis HEP is 1E-2) and 0.01 for the action (nominal action HEP is 1E-3) part of low power and shutdown (LPSD) tasks. Using the SPAR-H for 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 total HEP would be 2.25E-6.

If we consider the available time PSF multiplier is 0.01, however other seven PSFs are at the most pessimistic conditions (the highest multiplier is applied for other PSFs), the diagnosis HEP and the execution HEP could be as high as 1.

In recent years, SPAR-H has been applied to support HRA for Level 2 PSA (Germain et al., 2016) and multi-unit HRA (Germain et al., 2017; Park, 2019). SPAR-H quantification framework is unchanged, however further guidance is provided for selection of specific PSF values based on considerations of these scenarios. No new PSFs are introduced. Guidance is provided to improve consistency and is intended to derive more conservative results given the increased uncertainty in these situations, see Table 22.

Table 22. SPAR-H Multiplier for Level 2 HRA (Germain et al., 2016)

PSFs	PSF Levels	At power		LPSD		Level 2	
		Diagnosis	Action	Diagnosis	Action	Diagnosis	Action
Available Time	Inadequate time	P(failure)=1	P(failure)=1	P(failure)=1	P(failure)=1	P(failure)=1	P(failure)=1
	Barely adequate time	10	10	10	10	10	10
	Nominal Time	1	1	1	1	1	1
	Extra time	0.1	0.1	0.1	0.1	0.1	0.1
	Expansive time	0.01	0.01	0.1-0.01	0.01	0.1-0.01	0.01
	Insufficient information	1	1	1	1	1	1
Stress/Stressors	Extreme	5	5	5	5	5	5
	High	2	2	2	2	2	2
	Nominal	1	1	1	1	N/A	N/A
	Insufficient information	1	1	1	1	2	2
Complexity	Highly complex	5	5	5	5	5	5
	Moderately complex	2	2	2	2	2	2
	Nominal	1	1	1	1	1	1
	Obvious diagnosis	0.1	N/A	0.1	N/A	N/A	N/A
	Insufficient information	1	1	1	1	1	1
Experience/Training	Low	10	10	10	10	10	10
	Nominal	1	1	1	1	1	1
	High	0.5	0.5	0.5	0.5	N/A	N/A
	Insufficient information	1	1	1	1	1	1
Procedures	Not available	50	50	50	50	50	50
	Incomplete	20	20	20	20	20	20
	Available, but poor	5	5	5	5	5	5
	Nominal	1	1	1	1	1	1
	Diagnosis/symptom oriented	0.5	N/A	0.5	N/A	0.5	N/A
	Insufficient information	1	1	1	1	1	1
Ergonomics/HMI	Missing/misleading	50	50	50	50	50	50
	Poor	10	10	10	10	10	10
	Nomimal	1	1	1	1	1	1
	Good	0.5	0.5	0.5	0.5	N/A	N/A
	Insufficient information	1	1	1	1	1	1
Fitness for Duty	Unfit	P(failure)=1	P(failure)=1	P(failure)=1	P(failure)=1	P(failure)=1	P(failure)=1
	Degraded fitness	5	5	5	5	5	5
	Nominal	1	1	1	1	1	1
	Insufficient information	1	1	1	1	1	1
Work Processes	Poor	2	5	2	5	2	5
	Nominal	1	1	1	1	1	1
	Good	0.8	0.5	0.8	0.5	N/A	N/A
	Insufficient information	1	1	1	1	1	1

The HRA method used in Forsmark and Ringhals NPP is documented in NPSAG Report 53-002 (Holmberg, 2019). A time-dependent model is proposed for the failed diagnosis and decision making. The model is based on the use of the TRC from THERP and on the adjustment from five PSFs: procedures, training, human-machine interface (HMI), mental load, communication and coordination. This adjustment is developed with reference to the TVO's HRA method (Pyy & Himanen, 1996). The base probability curve assumes that for very long time windows (>20h), the lowest base probability value is 1E-4. The reasoning is to avoid too low probability values, which are difficult to justify. Each PSF will receive a value (selected from 1/5, 1/2, 1, 2, 5) which is the multiplier to the base probability.

It is also noted from the method that mental load cannot have a multiplier lower than 1, and communication and coordination cannot have a multiplier lower than 1/2. So in the most optimal condition, the failure probability of diagnosis is 1E-4*0.2(very good procedure)*0.2(often trained in a simulator)*0.2(practically impossible to miss the symptoms) = 8E-7.

If each of the five PSFs receives the multiplier of 5, even for the very long time windows, the failure probability of diagnosis is 1E-4*5(no procedure)*5(no training)*5(no feedback)*5(high mental load)*5(high coordination) = 3.1E-1.

In the Forsmark and Ringhals HRA method, recovery of failed diagnosis and decision making can be considered 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. 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 CBDT as its initial estimate.

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

In NARA method which is developed by UK EDF Energy (Barry et al., 2004; Raganelli, 2014), Extended Time Factors (ETFs) represent improvements to human reliability over very long timescale events (e.g. 12-24 hours) if other human factors aspects are favourable. The ETF module is based on the findings from a research project in UK. The EFTs are used as a multiplier that can lower the final HEP.

The ETF module is based on five factors related to the operator recovery over extended timescales:

- Information – e.g. prioritised alarm system, diverse communication systems, diverse monitoring of key parameters/critical functions
- Scenario characteristics – amount of time available (segmented between 2 and 24 hours), environmental conditions local at the plant (e.g. fire, storm, rubble after explosion, etc.), confusion due to misleading indicators

- Guidance – quality of procedural guidance available (e.g. EOPs, SAMGs, etc.; shift changeover protocols (for > 6 hours)
- Stress – e.g. burden of coping with fatalities or operator concern about worsening the environment or causing major capital damage by extreme recovery measures
- Teams – the degree of team training in simulators and site incidents, support by technical support centre, etc.

In UK EDF Energy method, the human performance limiting value (HPLV) is typically set as 1E-5. However, for optimal conditions and scenarios with excessive time scales (> 12 hours) the HPLV can be justified as 1E-7.

3.3.2.2 Proposed HRA Quantification Methods for Long Time Window Modelling

There are several different types of human actions related to the prolonged available times. The proposed HRA quantification method(s) is intended to be a simplified approach. This means the quantification method will not go down to detailed levels such as the different macro-cognitive functions involved in critical tasks, their failure modes and the failure probabilities. The method should however be able to find the driving PSFs for the analysed conditions and using decision trees or multipliers to derive HEPs.

An important factor in the quantification of category C HFEs with a long time window is how to consider recovery mechanism (factors) within the HFE quantification. Error recovery to the failed diagnosis and decision making is 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. To assume support from other personnel, the available time to recover a scenario should be long (several hours).

The following quantification approaches are proposed for further consideration. One or two methods will be selected to be further tested and improved in the pilot studies.

Approach 1. SPAR-H for both diagnosis and execution HEPs

1) 8 PSFs in SPAR-H are to be evaluated for both diagnosis and execution HEPs
2) Depending on the PSF levels, the result diagnosis and execution HEP values can be between 1E-6 and 1.
3) PSF multiplier selection guidance will be developed in the pilot study for the selected types of HFEs. A few multipliers might be adjusted.
4) It is worth discussing here on how to consider error recovery in SPAR-H framework, as error recovery to the failed diagnosis and decision making is more likely when there is a longer time window. SPAR-H (NUREG/CR-6883) provides two 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 and 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.

a) First option (explicit modelling of error recovery): The error recovery can be explicitly displayed as identified in the task analysis and it is possible to include them in the timeline diagram.
b) Second option (PSFs evaluation): The challenge of the second approach is the limited selections of positive PSFs levels and possible conflict with the selection of these PSF levels in existing SPAR-H method. Additional positive PSF multipliers might need to be added.
    i) Positive Procedure PSF multiplier: 0.5 for diagnosis, N/A for execution
    ii) Positive HMI PSF multiplier: 0.5 for diagnosis, 0.5 for execution
    iii) Positive work process PSF multiplier: 0.8 for diagnosis, 0.5 for execution

Approach 2. Develop a decision tree to derive a total HEP

1) As the TRC approach is not applicable for the HFEs with a long time window, a simplified decision tree is needed to consider the relevant PSFs to derive a reasonable diagnosis HEP. Similar decision tree can be used to derive a reasonable execution HEP.
2) It is proposed to use one decision tree to derive a total HEP which includes both diagnosis and execution HEPs
3) The upper HEP value is proposed as 1 (most difficult situation) and the lower HEP value is proposed as 1E-4 (most optimal situation). These two values are used as anchor points and a few intermediate values are used for decision tree sequences. A cut-off HEP, i.e. 1E-4, is suggested.
4) The decision tree needs to consider the relevant PSFs, e.g.
    a) Time margin (available time/required time)
    b) Training/experiences/practices
    c) HMI (information poor, not available, or misleading)
    d) Environmental factors
    e) Procedure (poor/ambiguous, not available, relevant steps missing)
    f) Task complexity (decision difficulty, mitigation strategy conflicts, concurrent tasks, high coordination required, etc.)
    g) Staff team: main control room (MCR) operator, field operator, technical support centre (TSC)
5) Possible prolonged time recovery (PTR) can be added to the decision tree. If the available time is much longer than the required time.
6) PTR examples: self-recovery probability = 0.5, or independent recovery probability = 0.1 from additional personnel (shift change and redundant personnel)
    a) If the operator(s) has considerable available time (e.g. double of the required time, time margin ≥ 100%) to perform the task and there is no time pressure or need to speed up to do the task in time, error recovery for self-check is assigned with a failure probability of 0.5.
        i. The basis is that the deployment team is attempting to correct its own error, a high dependence level is assumed between the errors in the critical steps and the work to correct them. Using the THERP high level dependence formula, ERE of 0.5 is a reasonable value.
    b) And if time is more than 8 hours or 12 hours and if we can assume that a new independent shift will come to help with the action, error recovery for

independent check is assigned with a HEP of 0.1. In order for the check to be credited, it must be demonstrated that the time margin ≥ 200%.

i) Error recovery for independent check HEP = 0.1 is used based on the probability for item 1 according to THERP (see table 20-22 in NUREG/CR-1278, 1983). While that item is for routine tasks in normal plant conditions, it represents failure to identity errors in connections, positions of locally operated valves, and breaker positions (MacLeod et al., 2014). If we assume there is a medium dependence level, the HEP would be around 0.23. If we assume there is a low dependence level, the HEP would be around 0.15. Thus ERE HEP of 0.1 is a reasonable value, even if there are possible dependences.

ii) If available time is more than 2 days, there could be more than 2 new independent shifts to help with the action. Even though it is possible, it is suggested not to further lower the execution HEP if one ERE for self-check HEP = 0.5 and one ERE for independent check HEP = 0.1 have already been credited. For the significant scenarios, new recovery actions (new HFEs) are suggested for function recovery.

7) One of the challenges related to the decision tree approach is the possibility to have a manageable size of the sequences. For example, if 8 PSFs are important and each PSF has 3 levels, the complete decision tree would have 3^8=6561 sequences. This is not feasible to use such a big decision tree in the analysis.
8) One possible simplified decision tree is to group multiple PSFs. An example of a simplified decision tree is showed in Figure 10.

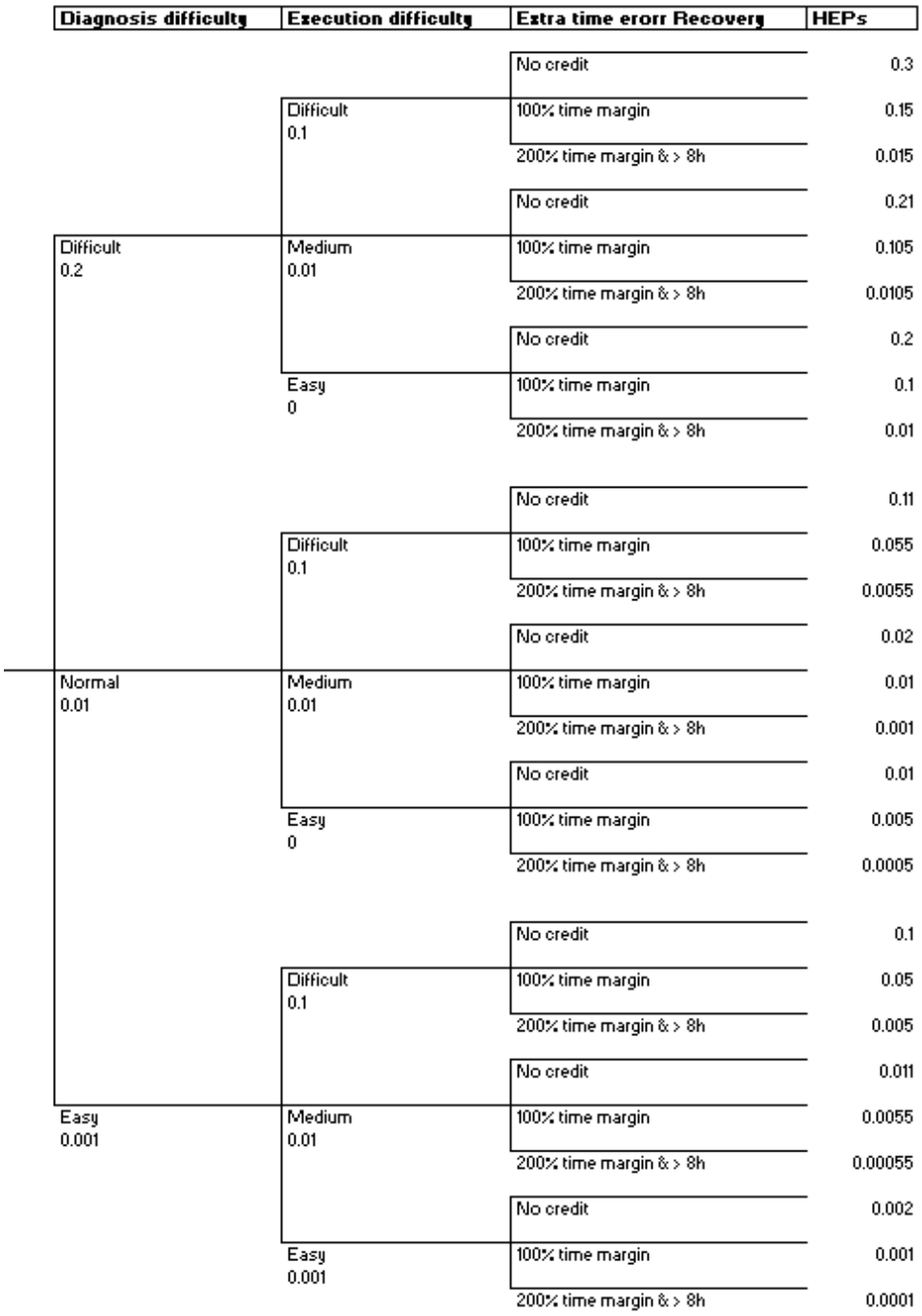

Figure 10. An example of a simplified decision tree

Approach 3. Improve the existing HRA, e.g. develop a decision tree to derive prolonged time recovery factor (PTR)

1) It would be good to have consistence in the HRA methods used in the plant PSA study. This approach means that the plants will continue to use their existing HRA methods (e.g. the Ringhals and Forsmark HRA method) for category C HFEs, but with some adjustments for PROSAFE HRA.
2) Possible areas that can be improved or adjusted (need to be further tested in the pilot study):
    a) Guidance of how to consider the required time and time available in the TRC could be explored. 'Time for identification and decision making' is used in the TRC for the base diagnosis HEP.

b) It is suggested to improve the multiplier selection criteria for the five PSFs. These PSF multipliers are used to adjust TRC for the diagnosis HEP, thus it is very important to make sure that all the relevant PSFs in PROSAFE scenarios can be considered in these five factors.
c) Considering the prolonged time window situation, it is suggested that a few PTRs are derived if the available time is much longer than the required time.
    i) PTR examples: self-recovery probability = 0.5, or independent recovery probability = 0.1 from additional personnel (shift change and redundant personnel). See more explanations in approach 2.
    ii) Experiences from CBDT or NARA ETF factors could be used as references to further refine the decision tree to derive PTRs.

3.3.2.3 Quantification of the new HFEs (Recovery actions and repairs)

For the identified new recovery actions (new HFEs) in the significant scenarios, the probabilities of failing to perform these recovery actions can be quantified by (1) using representative data that exists and is deemed appropriate for the recovery event, or (2) using the HRA method/tool(s) used for the other HFEs (EXAM-HRA, NPSAG Report 11-004-02).

For recovery actions (new HFEs), the typical important PSFs are time available and required, training practices, procedure, complexity of the action and environmental factors (SHARP1, 1992). In the current report, it is proposed to use one of the above proposed HRA approaches for the recovery actions.

The following time information need to be collected for recovery actions:

- Time for transit of plant personnel to equipment location
- Time for access (if required)
- Time to suit up (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 recovery action tasks

Please note that recovery actions to restore functions, systems or components are new basic events that would be added to the PSA. These should not to be confused with the “recovery” of an HFE which is credited within the decision trees. Recovery mechanisms are typically credited in the evaluation of the HEP for an HFE, and not modeled explicitly as separate basic events in the PSA model. Such mechanisms include peer checking, unexpected instrument responses in response to an action, and new alarms that correct an error in response and would prevent the HFE from occurring (NUREG-CR 2199, 2017).

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.

Repair actions may be modelled using task networks (Siegel & Wolf, 1969). In these, human or crew actions are modelled as a set of tasks to be accomplished, with dependences induced by precedence relations (e.g. a task cannot be started before another task has been completed). A task is characterized by a completion time distribution and task failure probability. These

tasks and the associated precedence relations comprise a task network. Monte Carlo simulation of the task network then gives the completion time distribution and the failure probability of the action. A task network-based method called Maintenance Personnel Performance Simulation (MAPPS) (Siegel et al., 1984) has been developed and it can be used to model and analyse unplanned maintenance (repair). Also other models that have been developed for the quantitative analysis of human and crew performance (Baron et al., 1990) may be applicable for repair modelling. A commercial code called Systems Analysis of Integrated Networks of Tasks (SAINT) has been available for constructing and analysing task networks since the 1970s, the current version being Micro Saint Sharp (Plott et al., 2017).

When using task networks, all potential causes of a failure mode have to be figured out, and in the worst case, a task network has to be constructed for the repair of each. Thus HRA techniques are potentially tedious to use since the method of repair is not known without knowing the specific causes (NUREG-1792). Instead repair probability may be evaluated by using actuarial data.

Repair probability estimation should consider the following elements:

- Detect the failed component and diagnose the need for repair
    - PSFs: available time, cues, instructions, experiences
    - Method: expert judgement (more in HRA side), and the dependencies with the preceding HFEs should be considered
- Repair of the failed component using actual data
    - Available time, required time (history mean time to repair)
    - Method: Probability distribution can be used considering the available time and mean time to repair (more in PSA side)
- Availability of the needed materials and personnel
    - Method: expert judgement, using the information from the plant.

3.3.2.4 FLEX actions

FLEX quantification will be investigated in 2020.

3.3.2.5 Dependencies for multiple HFEs in a Long Time Window

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.

In this section short guidelines for treatment of dependencies between category C HFEs with long time window are given. For more guidance on HRA dependencies, see NPSAG reports (He, 2016, 2017).

The rules to evaluate the dependency level among two HFEs with a long time window are in general same as the rules used for other category C HFEs. It is noted that the dependency level might be lower among HFEs with a long time window. This is because the actions take place are not close in time so there is lower possibility that a crew “mindset” or interpretation of the situation might carry over from one event to the next. Zero dependency level might be justified for the actions performed by different personnel or shift crews. In addition, when there is a long available time so that the separation time between two actions is long, e.g. more than 8 hours, different crew shifts will be involved, at least for the execution part.

When there is long available time, it is likely that recovery actions (as new HFEs) can be credited. The probability of failing to perform the recovery action(s) can be quantified by HRA method or expert judgement. The dependency between the preceding HFEs and the recovery action(s) should also be considered.

3.3.2.6 Minimum Believable Results

Up to now, there has been no consensus practice in setting or using such minimum values in the nuclear industry worldwide. In practice, it is generally recognized that the value of 1E-4 for a single human error, and 1E-5 for a set of human errors by different people, are 'credibility thresholds' in HRA.

Experience (Presley, 2016) 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 the NPSAG HRA dependencies project (He, 2017) utilities are recommended to look at 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.

- If HFEs in the important combinations are already judged to be independent, it is recommended not to apply the limiting value. A justification is needed if the joint probability is extremely low (e.g. lower than 1E-7).
- If HFEs in the important combinations are judged as dependent, it is recommended to apply limiting values, which shall not be fixed values. It is recommended to start with the limiting value 1E-5, and for the optimized conditions (e.g. a long time window), lower limiting values (1E-6 or even 1E-7) can also be applied. A good reference for optimized condition is the UK HPLV approach (Kirwan, 2008).

3.3.2.7 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.

3.4. Methods, PSA

3.4.1 Methods for Repair Modelling

The event sequences of the PSA result involve the failure events of different systems. Depending on the complexity of the specific modelling (for example the time windows and success criteria used) it may be possible to credit the reparation of specific systems.

The purpose of this section is to investigate the following issues:

- In which situations is it possible to credit the repair of a component/system?
- How could a repair be modelled?
- What are the advantages and weaknesses of the methods?

There are several reparation criteria that must be considered when modelling repair for both long and short time windows. The repair of a component is possible when some constraints in time and general possibilities are met, and these must be assessed qualitatively. The specific failure modes also need to be considered.

One aspect is that a system can be considered unrepairable for a specific time frame. This may be because it is not possible to physically access the system to be able to repair it for different reasons. There must also be enough available time left before the undesired consequence occur. That is determined by how long the system can be in one or several states that violate the success criterion. For example, if two pumps are needed to fulfil the success criterion and there is one available there will probably be more available time when compared to the scenario where none of the pumps are available. This sets restrictions on what systems/components can be repaired and during what time windows. Even if it is possible to repair a component (e.g. sufficient time window, physically available for repair, etc.), of course the repair can still fail due to reasons like an incorrect diagnosis leading to a decision to not repair, missing spare parts and other possibilities. The repair modelling must take all the repair "failure modes" into consideration.

There are several cases of interest for repair modelling. For example, the case of one component failure, several component failures and CCFs. For all cases it is of interest to observe how the repair time parameter is used in the current modelling. For single failure repair or several independent failures, a single parameter could be considered (for example if the probability of failure to repair for a basic event is to be considered). It is also possible to consider several parameters for these cases and then have more basic events under an OR-gate (or AND-gate if needed). For the case of a single component failure, multiple independent failures and the CCF-case, these parameters could describe different subtasks if a single task can be subdivided into parts. For modelling of multiple independent failures and the CCF-case, the probability to fail a repair could also differ depending on how many of the components that have failed need to be repaired. This is preferable if there are important dependencies between repairs of different components as otherwise a single parameter could account for the different aspects i.e. the subtasks.

As was discussed in WP1 (Tyrväinen et al., 2019), i.e. as shown in Risk assessment of operational events handbook (USNRC 2017b) the HRA methods are not suited for estimating the total repair probability. However, HRA methods could be applied to some repair related tasks, e.g. detection, diagnosis, decision to repair, etc. The availability of needed materials and personnel for repair should also be considered. In HRA section, how to consider repair probability is discussed.

In current PSA for Swedish power plants (T-book) repair time parameter is estimated from failure data and it is assumed that the repair time can be described with an exponential distribution and considers the parameter mean time to repair (MTTR). It is an important question to consider whether the MTTR parameter is applicable to accident conditions since the repairs have been performed under the usual plant situation. The repair time could be divided into several subtasks where each could (potentially) be described with an exponential distribution. The simplest approach to calculate the repair probability is to assume that the total time from indication of failure to repair success is described by an exponential distribution. Then the repair success probability is dependent on the MTTR and the available time. When the MTTR is low the probability to repair is high and when the available time is low the probability to repair is low as described by Figure 11. Usually it is the complement probability that is used in a PSA model (the probability to fail the repair). Figure 11 indicates that the repair probability could still be considered even when the available time is short, and it is possible to consider repair even if the available time is below 24 hours.

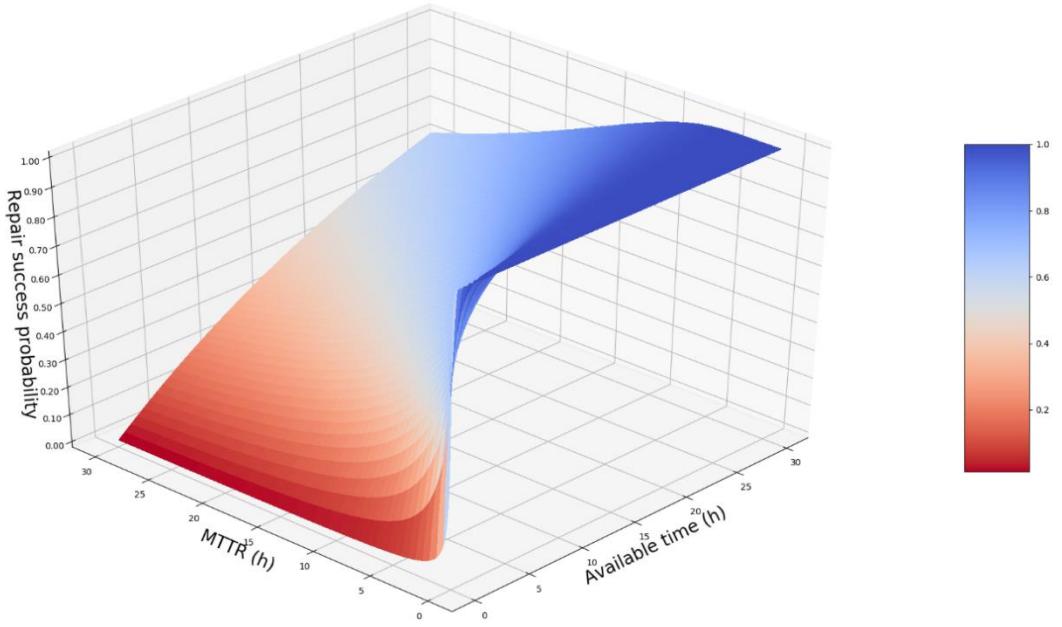

Figure 11. Repair time calculation from parameter estimation of repair time

For CCF repair modelling it is possible to use both a single parameter for the probability to repair or to use several parameters. There are many assumptions that will affect the parameter calculation and estimation. Examples of assumptions are whether the CCF occur simultaneously in time, success criterion (defining how many components need to be repaired to recover the safety function) and repair strategy (do the repair start with one or several components and are they performed by the same personnel, etc.). The simplest case is to consider the repair of one of the components and calculate the single failure repair probability. In addition, the combinatorics of repair of several components could be considered. Here it is possible to use other tools to calculate the overall repair probability from CCF for example by Markov chains.

The modelling of repair of components can be done with different methods. The available current methods include event tree modelling, fault tree modelling and manipulation of the MCS list. The three methods could take the difference of sequences into consideration. There

are pros and cons with the different methods that must be considered and what requirements these set on mission times and success criteria.

Event trees

The option of modelling repair with event trees can be the most realistic and is most suited when consideration of sequences is needed. It is also the most complex because it might increase the number of sequences. It will require the most work to adjust the model if compared to the work with fault trees, whereas event tree modelling requires consideration of the different sequences.

The modelling can be done with the inclusion of additional function events or by modifying the consequences (especially if the consequence is a transfer to a linked event tree). When the function event is added the repair, itself is modelled in the corresponding fault tree, with a basic event or a more complex fault tree structure. This will increase the number of consequences and the complexity of the event tree. The other option by modifying the consequence of the event tree will yield a modified event tree the resulting from crediting of the repair. Both cases yield a more complex structure that must be evaluated on a case-to-case basis.

A simple example is shown in Figure 12 that presents an event tree model for repair where another function event is added. There is shown two safety systems where one is repairable and the other is not and one is required to avoid core damage (to end in an OK consequence). There could potentially be other consequences C1 and C2 resulting from the sequence due to a reparation of the system or when system 2 is used.

To consider single failure repair could be done by simply adding a function event or by adding a repair tree. The same could be done for many independent failures but the number of combinations might be unfeasibly large. It will probably be difficult to model repair of CCF with event trees especially if it is handled in the linked consequence event trees because of the combinatorics. It is less complex if it is modelled under the sequence event fault tree where it is possible to calculate the probability for different CCFs or combinations of single failures. The probability to perform these repairs could also be done with the worst case of this. There the same problems that arise in fault trees arise. For complex models it is not feasible to add additional function events, but in simple models this might be feasible to consider (i.e. in spent fuel pool models).

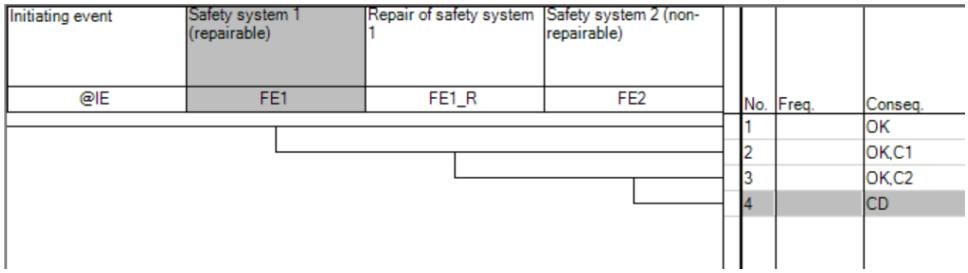

Figure 12. Event tree with one repairable system and one unrepairable**.**

Another example to show the growth of the event tree due to implementation of repair we observe an event tree with four safety systems where there is need of one of system 1 or 2 and both of 3 and 4. System 1, 3 and 4 are repairable and 2 is not. This example is shown below in Figure 13.

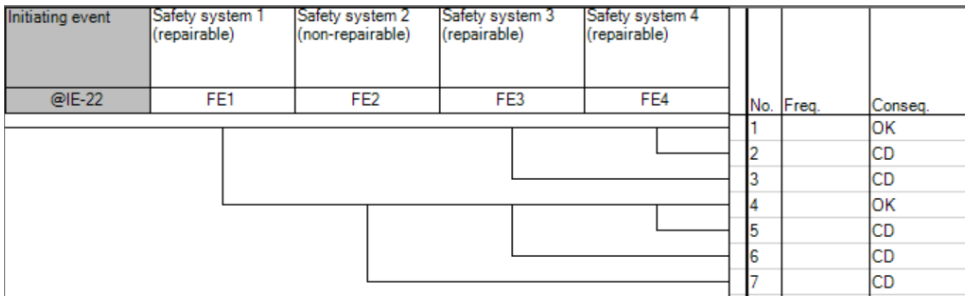

Figure 13. Event tree with three repairable systems and one unrepairable. No repair is modelled**.**

And when the repair function events are added the event tree looks as can be seen in Figure 14. The number of sequences increases from 7 to 22 and the tree grows more complex.

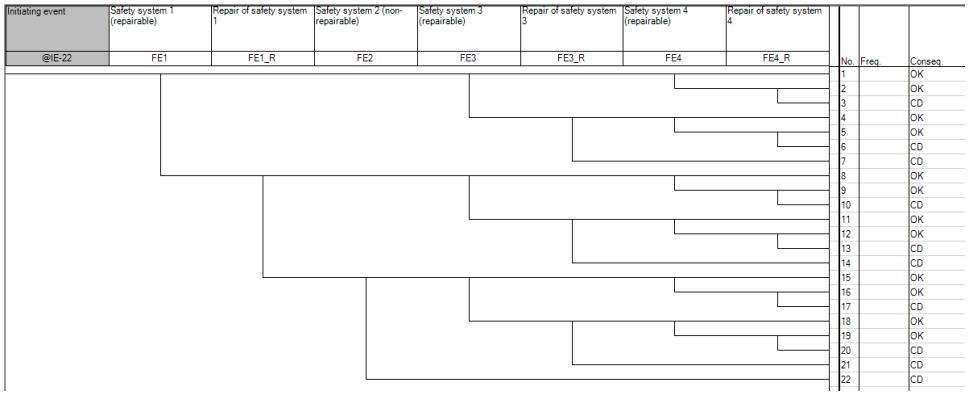

Figure 14. Event tree with three repairable systems and one unrepairable. Repairs are modelled.

It could become very difficult if the situation is more complex than the simple example here.

Fault trees

The modelling of a repair of a specific system could be done with a simple basic event probability or with a more advanced expansion of the existing fault tree structure. If the model is not very simple this should be quite time consuming depending on many factors such as type of repair, type of component and event sequence that is considered. If a subset of the specific sequences is considered this could be modelled with house events and repair rules but that quickly increases the complexity of the modelling since this requires the fault trees to have multiple configurations.

An example of a fault tree-structure with repair implemented is shown in Figure 15, without taking CCF into consideration. Here the repair basic event is divided into a decision and an execution part if there is need to consider a part of the repair with HRA-methods.

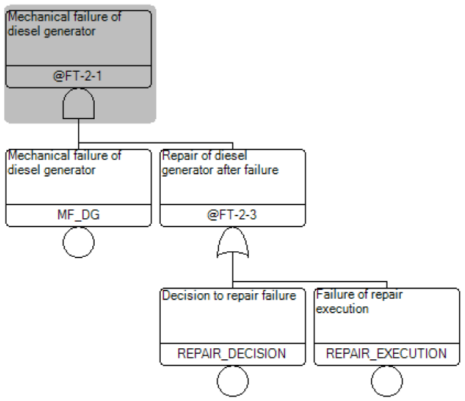

Figure 15. The simplest case of modelling repair in fault trees

Here the example is simple, but if the model is complex it will perhaps be a lot of work, even though the complexity is not as high as for event trees. If the model is complex, the workload can be reduced if only the most important systems are considered in an iterative process. For less complex models this is not a problem.

The single failure repair modelling (by adding a basic event) will consider independent failures from different components but not independent failures in the same component. The fault tree method can handle modelling of repair of CCF with some difficulties directly or indirectly. It could be done directly with a built-in/add-on tool for calculating CCF-repairs in the PSA-software. It could also be done directly by considering the cases of repairing X-out-of-Y CCFs, but this quickly becomes complex as it will have implications on time windows and perhaps success criteria considered. Indirectly it can be modelled by calculating a repair probability outside the model and adjusting the probability to fail the repair.

Manipulation of the MCS list

Repair could also be considered by manipulation of the MCSs, whether it is done manually (by multiplying the MCSs by a repair failure probability) or via a post processing tool, e.g. the post processing tool in RiskSpectrum PSA or recovery rules in FinPSA. This way of modelling the repair cannot directly consider the sequences of events but on the other hand gives an option to consider only the most dominating events that relate to the core damage frequency.

Single failure repair can easily be modelled by simply multiplying the corresponding MCSs. The case of multiple independent failures is the same as the single failure repair, but it is possible to only consider the most contributing by consideration of sequences. It is also considerably easier to model CCF with this method since the CCF-events appear directly in the MCS-list and therefore can be manipulated. The repair probability then must be considered (for all three cases) by looking at the events and sequences associated (with their possible time windows and success criteria).

Sequences

An important aspect to handle the repair is to look at the sequences. This could be done in addition to event trees, fault trees, the MCS-manipulation or perhaps as an independent modelling (if the used tool allows it). The first three options are described in respective section and independent modelling is not covered here.

3.4.2 Methods for Time Window Modelling

In a sequence of events several different types of time windows are defined. Static fault tree and minimal cut set based techniques have significant limitations in modelling these time related aspects. For example, in static PSA all events in a minimal cut set are assumed to occur simultaneously and instantly which potentially introduces large conservatisms, predominantly in sequences featuring long time windows.

The purpose of this section is to discuss the following issues:

- What is a time window and where can they be introduced in the PSA?
- What can be done with ET/FT modelling and what are the limitations with such tools?
- Under what conditions is there a need to consider certain time windows?

Some brief discussions on differences, and the advantages and drawbacks with using semi-dynamic/dynamic approaches are also included.

As we saw in Section 3.2.2.1 the following types of time windows can be identified to play a role in PSA modelling. Examples of each different type of time window are given in Section 3.2.2.1.

1. The time window between the IE and the safe state
2. The time window when a component/function is required to run, i.e. mission time
3. A time window before a component/system must be started
4. Delays with limited capacity that allows/can buy extra time
5. Dynamic mission times for redundant/diversified components
6. A time window with constant failure rate
7. A time window with similar consequences

1. The time window between the IE and the safe state

In order to address the first time window type the safe state has to be defined. The definition of safe state is also further discussed in Section 3.1. In traditional PSA the safe state is modelled with the constraint that if no undesired consequence has occurred after a certain time, the safe state is reached. This time window is commonly assumed to be 24 hours for PSA level 1 and 48 hours for PSA level 2. The same time window until the safe state is reached is normally assumed for all initiating event and sequences, which is a simplification.

In the FT/ET analysis it would be possible to define the time to the safe state for each initiating event based on deterministic calculations for one general umbrella case representing all sequences. It is also possible that this time window could be assigned as a distribution. This would still be a simplification as the development of sequences can differ greatly also for the same initiating event. A drawback with this approach is that the PSA model would quickly become rather complex.

With a semi-dynamic or dynamic approach, it would be possible to represent the time window between the initiating event and the safe state in a more realistic way for each sequence of events. The safe state can then be defined as a state rather than avoidance of the undesired consequence within a fixed time window.

2. **Mission time**

This relates also to bullet 1, as the time window between IE and safe state often determines the mission time for many components.

The mission time in a traditional static PSA is the same for a component independent of the sequence. In some cases, a component can be modelled with different (but still static) mission times in different sequences. This can be performed by using separate fault trees using different mission times, by using house events in a fault tree or exchange events. If there are only a few components that need to be modelled with a few different mission times it is reasonable to use different fault trees or just using house events in one fault trees to manage this. Introducing several different mission times for several components would introduce a lot of complexity at the same time as it would still be a simplistic representation. In this case it would hypothetically be possible to introduce either exchange events or exchange parameters to represent different mission times for the same component. The drawback with representing different mission times with different basic events that are exchanged would be that the same event would have different IDs, and hence not possible to identify as the same event in MCS results, importance analysis results, etc. The other hypothetical possibility would be to introduce exchange parameters. One set of parameters could for example be used for each initiating event. Exchange parameters would introduce some theoretical challenges as two basic events sharing the same ID would mean different thing. Note that exchange parameters are not a supported feature in RiskSpectrum or FinPSA as of today.

3. **A time window before a component/system must be started**

This type of time window is generally not considered in a static PSA. However, it may sometimes partly be considered inexplicitly for example when estimating available time for a manual action.

This issue is related to both time window types 4 and 5 as there can be several reasons why there is some available time before a component must start or function.

It is also possible to have a situation where a component fails to start in the first place, but after a certain time it is repaired, and the start is successful which leads to a different consequence than if it would not have failed at all. This issue relates to time window type 7.

These types of delays can be represented in the event tree with a function event after the occurred failure. The function event will represent the failure probability of for example repair of a component or recovery of manual actions during this time window.

4. **Delays with limited capacity that allows/can buy extra time**

This type of deterministic delays is generally not considered in a traditional PSA. However, it may sometimes partly be considered inexplicitly for example when estimating available time for a manual action.

The undesirable event is delayed by some physical process that provides a grace time. A good example is the spent fuel pool. If the cooling is lost the undesired event, for example boiling or uncovering of the fuel, is not immediate. The water will heat until it starts to boil and uncovering of the fuel will follow after another amount of time. This process is deterministic and introduces a delay that allows for recovery before the undesired event occurs.

There is also another type of time window that can allow for extra time but generally only once in a sequence. A good example would be a diversified water tank that can be pumped into the spent fuel pool. However, such a tank would only last for a certain amount of time as it would get empty. In the sequence this means that some extra time was bought before another barrier would have to cover up. Normally such a deterministic time would not be repairable, i.e. it is not possible to refill the tank with a short amount of time. In a fully dynamic model a low repair rate could be assigned to such a deterministic time. Another example apart from a diversified water tank would be batteries that could be recharged.

These kinds of delays would be possible to represent as function events in event trees. Foremost this would be a way to credit functions that would allow additional time for manual actions or repair actions. Situations where this would be a feasible to implement in the model is when system success criteria are nearly fulfilled. Extended use of this kind of modelling in event trees will though quickly become complex.

5. Dynamic mission times for redundant/diversified components.

This issue is not considered in traditional PSA. It seem to not be possible to represent these dynamic relations in a static ET/FT representation.

6. A time window with constant failure rate

Failure rates are usually assumed to be constant during the whole mission time. In some PSA studies two different time windows have been used for diesel generators with a higher failure rate during the first hour after start. This can be performed by using several fault trees using different mission times, by using house events in a fault tree or exchange events. This issue is in general easy to incorporate in an existing ET/FT model.

7. A time window with similar consequences

The time of a failure (e.g. early or late) may have an impact on the consequence. This could be represented by adding branches in the event tree or a function event and is a fairly simple exercise.

3.4.3 Methods for Dynamic Success Criteria

A dynamic success criterion is a success criterion that changes during the mission time. For example, two cooling water pumps may be needed in the beginning of an accident for sufficient cooling, but later as the amount of residual heat decreases only one pump may be sufficient. Dynamic success criteria have been rarely modelled in PSA. Typically, conservative static success criteria are used, e.g. that two pumps are required for the whole mission time regardless of the decrease in residual heat. The purpose of this section is to study how dynamic success criteria could be modelled in PSA.

Before modelling a dynamic success criterion, the success criteria and the time point(s) when the criterion changes need to be defined. The same principles can be followed as in normal success criteria analysis. For example, thermo-hydraulic simulations can be used to determine the number of cooling water pumps required at different time intervals. It is possible that there is uncertainty related to that time point, and the time point can depend on some other variables, e.g. other events that occur at the plant. In that case, one approach is to define a single time point in a conservative manner to simplify analysis. A more realistic approach, on the other hand, would take different possible timings into account. Here, we start with the simpler case and assume a single time point, i.e. that the time intervals are fixed.

In fault trees, a dynamic success criterion can be modelled by creating separate fault trees for different success criteria, e.g. one for 2-out-of-4 criterion and one for 1-out-of-4 criterion. In addition, failure to run basic events need to be divided between the time intervals, i.e. for each component, there is one basic event for the first interval and one basic event for the second interval. It has to also be modelled that components that fail during the first time interval remain failed for the second interval unless they are repaired.

Figure 16 and Figure 17 present a fictive and simple example of dynamic success criterion modelling. The success criterion is 2-out-of-4 pumps for the first 16 hours after the initiating event, and 1-out-of-4 pumps for the next 152 hours. The second fault tree includes all basic events, early and late failures, because it is possible that e.g. two components fail early in the scenario and two components fail late in the scenario. These two fault trees can either be included in separate event tree sections, or modelled in the same event tree section by a top fault tree with these two fault trees under an OR gate. If the consequences of a late failure are significantly different from an early failure, the first option is a logical choice.

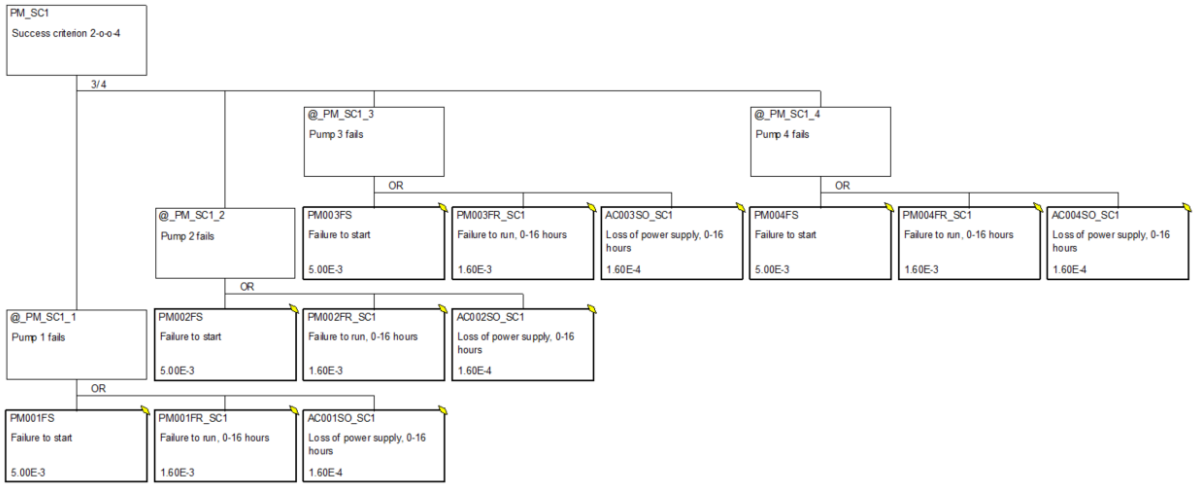

Figure 16. Fault tree for the first success criterion

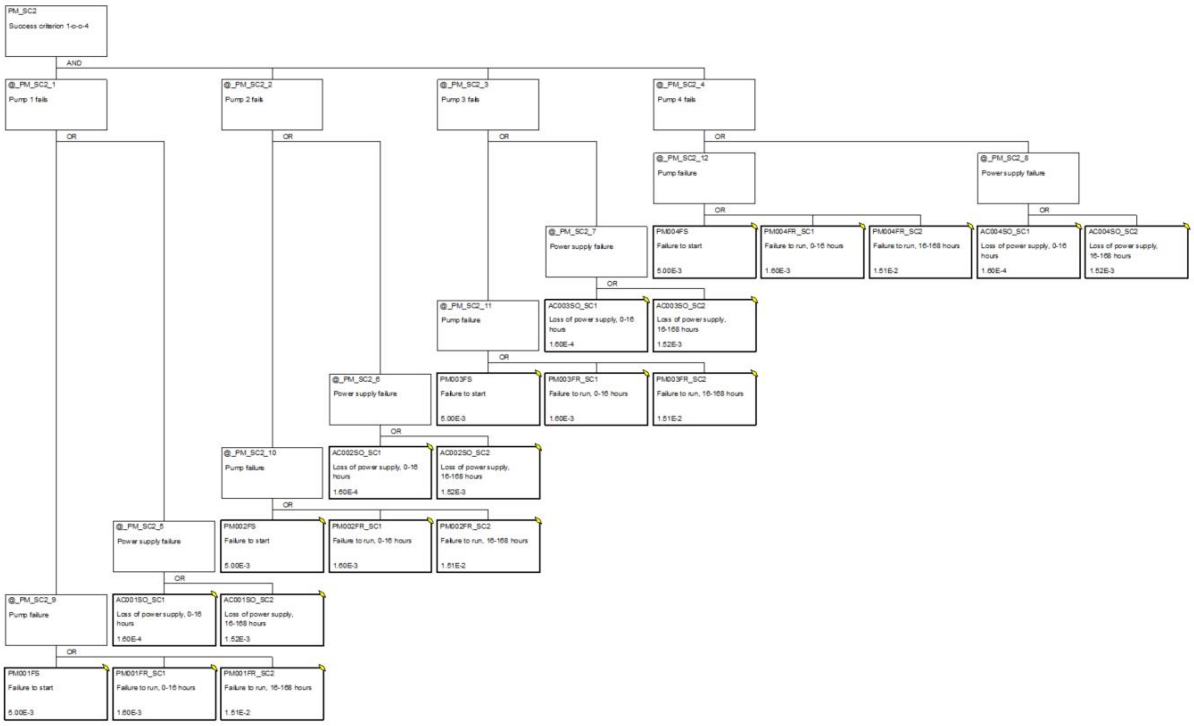

Figure 17. Fault tree for the second success criterion

In a simplified case with fixed time windows, like in the example above, the modelling of a dynamic success criterion is relatively easy. In real models, fault tree structures are larger, and by dynamic success criteria modelling they get even larger, but still the main challenge is the fault tree management, not the logical modelling. Use of some sort of house events or attributes in such fault tree management is likely useful, so that there is no need to double all the related fault tree structures compared to the modelling of a static success criterion.

Since dynamic success criteria modelling adds complexity to the PSA model, it is a good idea to evaluate first whether such modelling would have significant impact on the results. If the starting point for modelling is a fault tree with a conservative success criterion for the whole mission time, it can be used to evaluate the potential impact of more realistic modelling. The first test can be just to change the top gate of the fault tree to correspond to the success criterion that could be applied later in the scenario and see the impact on the result. If this does not make significant difference in the results, there is no need to model the dynamic success criterion. This change causes an underestimation of the risk assuming that the success criterion later in the scenario is less demanding, e.g. requires smaller number of pump lines.

One can also evaluate the impact more accurately based on the original fault tree. It is straightforward to calculate the failure probability until the time point where the success criterion changes using the original fault tree e.g. by modifying mission times for minimal cut set quantification. Then, the top gate of the fault tree can be changed to correspond to the changed success criterion, and the failure probability related to the second time interval can be estimated by modifying the mission times to correspond to the second time interval and removing failure on demand events. The sum of these two calculated probabilities is a rough approximation for the total failure probability of the safety function, and the decision about modelling can be made based on that.

If needed, PSA software tools could, of course, be developed to support the modelling better. Firstly, the dependencies between the time intervals could be handled in a more convenient manner. For example, there could be a mapping between the basic events of earlier and later time intervals so that there would not be need to include the basic events of the first interval in the fault tree of the second interval explicitly. Instead, the basic events of the first interval would automatically be added to the fault tree of the second interval when minimal cut sets would be solved. Secondly, automatic fault tree generation could be a possibility. For example, the fault trees of the different success criteria could be generated automatically based on one master fault tree according to logical rules defined by the user.

Another computation method could be just to generate the minimal cut sets for both success criteria by changing the top gate of the normal system fault tree and handle the time windows in the quantification of those minimal cut sets. This would require some PSA software development, whereas the approach presented above can be applied directly with the current tools. On the other hand, it would be more convenient if the computation was performed automatically based on one master fault tree without the need to duplicate fault trees and basic events. However, the automatic generation of the fault trees discussed above seems equally convenient and is maybe better aligned with the current capabilities of the PSA software tools as there would be no need to change the minimal cut set quantification.

There are also cases where a cooling system fails first according success criterion 2-out-of-4, the accident is managed by another system for some time, and the failed system is later taken into use with success criterion 1-out-of-4 if one redundancy remained operable or was repaired. Such case can be modelled by a similar approach with two separate fault trees. One relevant question is however how the time window of the second success criterion depends on the other safety system, i.e. how long it operates before failure. Such uncertainty on the time window may need to be taken into account in the quantification. Though, again another option is to define a single time window conservatively.

Modelling of dynamic success criteria gets more complicated when it is combined with other challenging modelling issues, such as repair modelling, varying time windows or non-simultaneous CCFs. A special case of repair modelling is a repair of a component that fails during the first time interval before more components fail during the second time interval. Such a repair could be credited by including a repair failure basic event in the fault tree, using a recovery rule to add the basic event to relevant minimal cut sets or just taking it into account in the computation of minimal cut set frequencies. The modelling also requires determination of repair time distribution and analysis of possible failure and repair times, e.g. by simulation, to calculate the repair failure probability. However, the first step is to analyse whether it is worth to credit such a repair, since its risk contribution may be small. This analysis can be performed by estimating the risk contribution of minimal cut sets to which such repair could be applied. If the risk contribution of such minimal cut sets is small, there is no need to model the repair.

Dynamic variation of time windows, e.g. the time point when the success criterion changes, can be difficult to model explicitly in fault trees. One way to approach the problem could be to take the dynamic variations into account in the computation of minimal cut set frequencies, assuming that the minimal cut sets themselves remain qualitatively the same. If distributions could be estimated for the time window variations, the computation could be performed by simulating the time windows according to the distributions.

If repairs and failure times are to be modelled with high level of realism, one option is to analyse minimal cut sets by simulating failure times and repair times. Then, for each simulation run, it can be checked whether the success criteria (early and late) are satisfied or not, and the failure probability can be calculated based on the portion of failed cases.

Hassija et al. (2014) have modelled a dynamic success criterion using a Markov model. Easy modelling of repairs is a clear benefit of this approach. There seems however to be no smooth way to represent the change of the success criterion in a Markov model, since the modelling of different success criteria required separate Markov models. It could also be challenging to integrate a Markov model to a PSA model if support system dependencies need to be modelled. On the other hand, Markov models could possibly be applied in the quantification of individual minimal cut sets, like in the I&AB method (Bäckström et al., 2018), but they do not seem to have great benefits concerning dynamic success criteria modelling.

A more realistic approach to handle varying success criteria and time windows would be dynamic event tree analysis (Karanki & Dang, 2016). In such analysis, a dynamic event tree tool would be used to generate accident sequences automatically together with a plant simulator. During a simulation run, the tool identifies stochastic branching points based on the plant conditions (e.g. when a safety function is activated and can fail), and later, the tool generates simulation runs with the events related to those branching points. For each generated accident sequence, the simulator determines whether e.g. core damage would occur or not. Separate branches can be generated for cases with different numbers of safety system trains available with different timings (e.g. 2 trains available until time point t_2 and 1 train available until time point t_1 after that), so that the success criteria analysis is part of the event tree simulations. Dynamic event trees can be used in real time risk calculation or as an extended success criteria analysis providing inputs for a static PSA model (Karanki & Dang, 2016). However, dynamic event tree analysis is currently far from practical use in full scope PSA, because the simulations that would be required are much too time-consuming. The number simulations that can be performed in success criteria analysis is typically quite limited. It can be more realistic to consider using dynamic event trees in some limited accident scenarios that involve significant dynamical behaviour.

Another potential issue related to success criteria is the possibility that core damage is avoided even if a success criterion is not met for a short time. For example, the success criterion could be that two pumps need to work, but still operation with only one pump for a short time could be sufficient as long as the second pump is repaired soon enough. To be accurate, the success criteria should then be redefined to account for the time allowed to operate with only one pump. On the other hand, this type of cases might not be very important, and it is conservative to model the strict success criterion.

3.4.4 Failure Data

It is clearly necessary to address the matter of failure data when exploring possibilities of crediting repair or dividing the analysis into different time windows. The work so far has shown that failure data need to be examined more deeply if e.g. repair or non-constant failure rates are to be used in the models. Several questions arise such as:

- Is there evidence showing that failure rates might be changing over time, and if so, how can such data be obtained?

- Is it possible to divide failure rates in such a way that it becomes clearer to what extent repair can be credited? This would probably put a requirement that the "failure to run" failure rate parameter is complemented with information about how large portion of the failures that are "catastrophic", i.e. non-repairable and consequently how large a portion of the failures that are "non-catastrophic".
- Also, in the case of common cause failures the parameters must be examined carefully in order to investigate how the conservative assumption, present in most PSAs, that all failures occur simultaneously and immediately can be improved.
- The repair time, or more precisely the *MTTR*, needs to be clearly understood since there is sometimes confusion about this parameter.

The first two questions above has been addressed within the "State of the art review" (Tyrväinen et al., 2019) where NUREG 5500, vol 5 (Grant et al., 1996) was reviewed and the following concluded:

Reported EDG failures from tests performed at plants that reported under RG-1.108 requirements during the study period (1987-1993) was used. These tests required the EDGs to run for 24 hours. There were 27 fail to run (FTR) events observed in the cyclic surveillance test data. The duration of the EDG run times prior to the failure of the EDG were reported in 19 of the licensee event reports. Based on analysis of these data the study concluded that three distinct failure rates existed. The failure rate during the first half an hour was 2.5E-2 per hour. The failure rate decreased significantly to 1.8E-3 per hour for the period between 0.5 hours and 14 hours. For periods greater than 14 hours, the failure rate again decreased to 2.5E-4 per hour. Figure 18 illustrates the estimation of the three different failure rates.

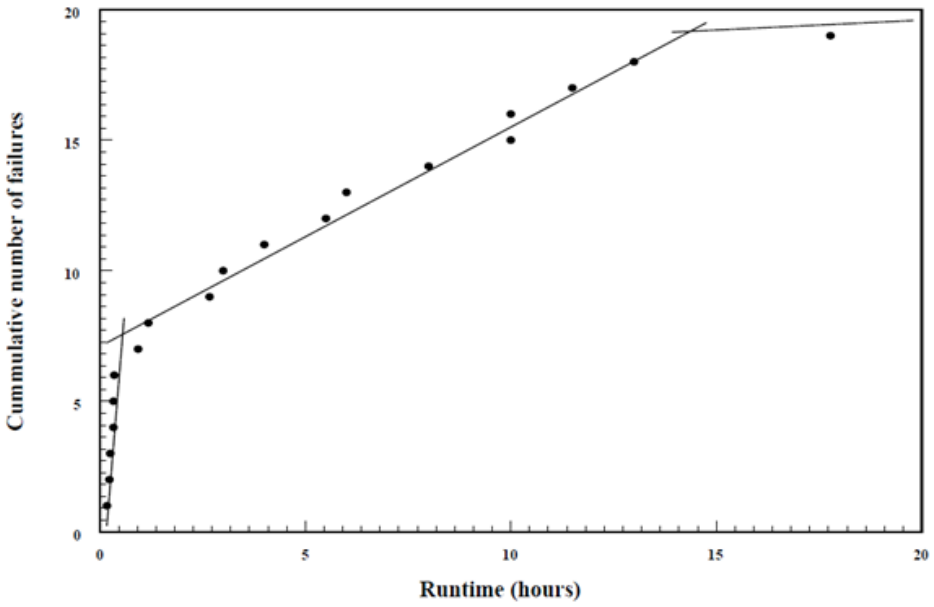

Figure 18. Cumulative number of EDG FTR events observed during the cyclic surveillance tests as a function of the time of the failure (Grant et al., 1999).

They commented that the early, middle, and late failures seem to correspond in part to different failure mechanisms. The change in the failure rate per hour was linked to a change in the

mechanism of the EDG train failures. That is, the cooling subsystem dominated the early failures, accounting for about one-third of all the failures that occurred during the first half an hour; the electrical and fuel subsystems combined account for half of the failures in the period between 0.5 hours and 14 hours; and beyond 14 hours the only failure observed occurred in the electrical subsystem.

The questions about non-constant failure rates are thus related to the question about repairable failures since the NUREG study indicates that the changing failure rate is clearly related to that the failure mechanisms change during operation.

In order to improve the data and to understand the data better, the data collection team (TUD in case of the T-book) must be involved. This is a task that not yet has been addressed within the project.

Regarding the parameter MTTR the following definitions apply (from NUREG/CR 6090, Appendix B):

MDT = MTDF + MTTR

where

MDT = Mean Down Time
MTDF = Mean time to diagnose the presence of a system fault (time to detect the fault)

and

MTTR = MTDL + MTRF + MTRO

where

MTDL = Mean time to determine fault location
MTRF = Mean time to replace a faulted component
MTRO = Mean time to return the system to operable condition

In Figure 19 the relation between the parameters is shown.

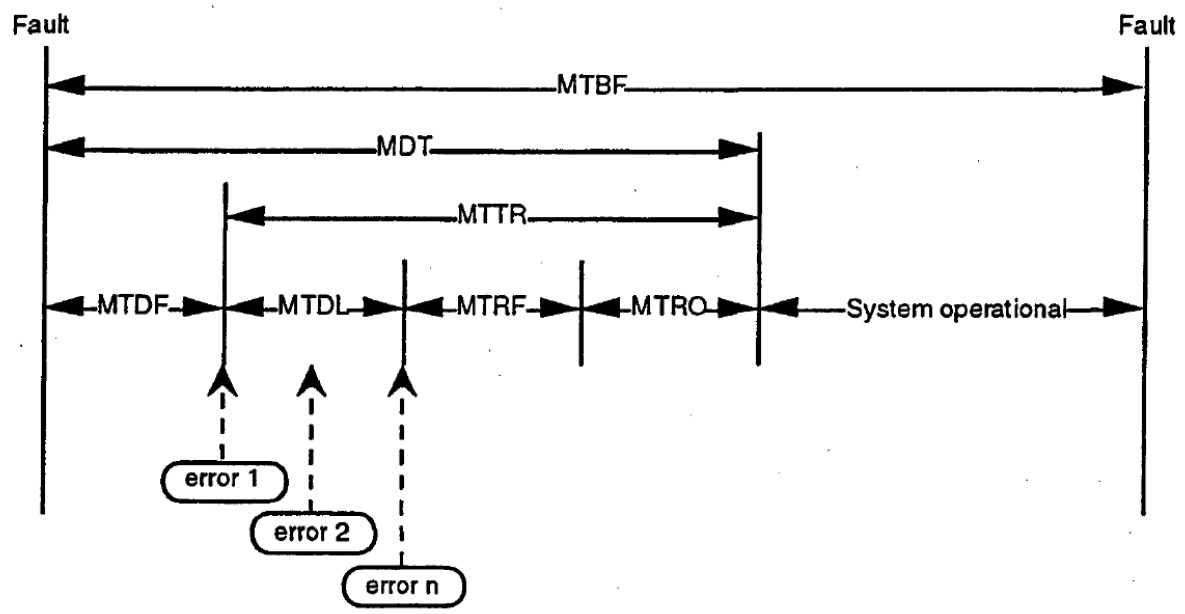

Figure 19. Relation between parameters (NUREG/CR 6090)

Selvik and Ford (2019) also discuss the abbreviation "MTTR". A principal problem (and uncertainty) is that it is generally difficult to measure the time until a failure is detected (and the exact time of occurrence), which can be caused by the fault being hidden until a sudden demand occurs.

Uncertainties are also related to the data input for calculating MTTR, for example the population (available information) being too small. Since relatively large resources are needed to gather the necessary data, there is also the risk of old data being used, with old technology as its basis since revision is costly. Also, the taxonomy of the data may not be distinct enough, which means that errors of interpretation can occur.

MTTR can also signify "mean time to *restoration",* which includes the *fault detection time*. This term is compromised by four factors; **fault detection time**, **preparation and delays** (administrative, logistic and technical delays), **active repair time** and **delays after the item is repaired** (mainly administrative). "Mean time to repair" on the other hand only contains 3 of these factors (without fault detection). This definition of "mean time to repair" is the same as in NUREG/CR-6090. As opposed to "mean time to restoration" and according to Selvik and Ford (2019), it is not always known if "the fault detection time" is included in "mean time to repair" or not. See Figure 20 below for an overview and graphic explanation.

Conclusion
From the gathered sources in this study, it stands clear that MTTR (mean time to repair) consists of at least three factors;

- Preparation and delays
- Active repair time
- Delays after item is prepared

What is not as easily determined is whether “fault detection time” is/should be included or not, and this must therefore be clarified beforehand. To be able to distinguish all the factors used in an array of data with MTTR-results may not be possible, which is why this parameter can be associated with a high level of uncertainty. The uncertainty is also coherent to the evolution of technology and shifting routines regarding old data being used and presented, as well as knowing what is included in, and meant by MTTR.

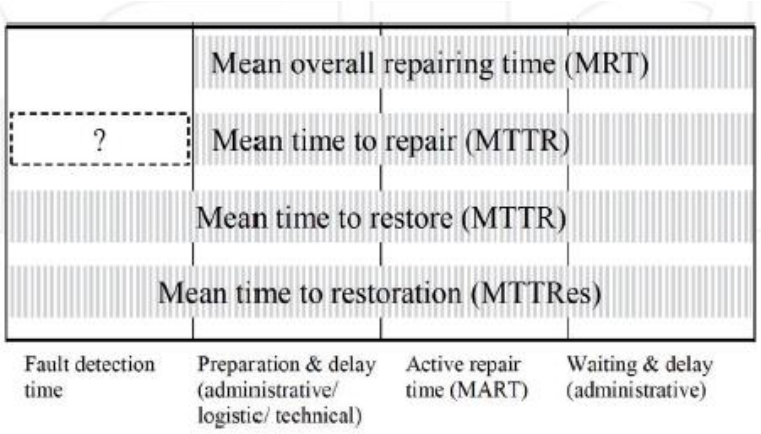

Figure 20. Relation between parameters

3.5. Methods conclusions

PROSAFE HRA focuses on the Category C HFEs. In this report, the PROSAFE HRA requirements are proposed. These requirements are mainly based on the HRA requirements in ASME/ANS PRA standard, NRC HRA good practices, considering the prolonged time window situations. The relevant PROSAFE HFEs are identified from the stakeholder PSA/HRA studies as well as literature reviews.

The qualitative part of the HRA process is emphasized as important as the quantitative part, as for Category C HFEs with a long time window, it could have large uncertainties in the quantitative HEP results as the scenarios and PSFs could have large variances in a longer time window. Proper task analysis with proper timeline diagrams is suggested.

A few quantification approaches are proposed and some of them will be further tested and improved 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 to the failed diagnosis and decision making is 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. 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. All these relevant factors should be considered in the quantification.

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 big influence on the result.

FLEX action will be further evaluated in 2020 including its important PSFs and proper quantification method.

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 mostly useful for models that are not that complex i.e. the spent fuel pool model and there it is often used already as shown in the hypothesis testing. Techniques using manipulation of the MCS-list are probably more suited for models that require more complexity.

The findings suggest some guidelines for reasonable modelling to credit repair in the PSA model. First it should be determined whether the repair modelling is reasonable by observing the impact of repairable systems by looking at time windows for repair, general limitations of repairing the systems, and the complexity of the systems and the overall model. For example, if the repair is supposed to be credited to the spent fuel pool model, we have in general long time windows and systems that are considered repairable. Then a more complex modelling technique could be used as opposed to when the time is shorter, and the system is more complex (even though repair is relevant there too).

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 has been presented. 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.

The work performed within WP3, Methods, have resulted in a number of findings, questions and conclusions. There will probably be a need to prioritize between the tasks and this work will be done in close collaboration with the stakeholders.

4. Pilot Studies

4.1. Pilot study scope

The purpose of the pilot studies is to (1) evaluate the importance of features related to long time windows, and (2) evaluate the feasibility of proposed methods. The first evaluation is performed by elaboration and hypothesis testing in actual models for different Nordic utilities, which is covered in Section 3.2.2. The second, the evaluation of proposed methods feasibility, will be performed in two pilot studies, one based on the PSA of Ringhals reactor unit 4 and one based on a generic PSA model from the DIGREL project (Authen et al., 2015).

During 2019 the DIGREL example model was expanded with a fictive spent fuel pool design in order to fit the scope and purpose of the PROSAFE project.

4.2. PROSAFE Example Model

In project DIGREL, a simplified PSA model was complemented with fault tree models for four-redundant frontline systems, support systems, power system and protection system in order to study and demonstrate the effect of design features and modelling approaches. The example PSA-model represents a fictive boiling water reactor (BWR).

For the purpose of evaluating methods identified in PROSAFE, the DIGREL model has been further developed with safety systems for cooling of the spent fuel pool and for make-up water.

The updated example model includes the following systems:

- ACP – AC power system
- ADS – Automatic depressurisation system
- CCW – Component cooling water system
- ECC – Emergency core cooling system
- EFW – Emergency feedwater system
- FCV – Filtered containment venting system
- HVA – Heating, venting and air conditioning system
- MFW – Main feedwater system
- RHR – Residual heat removal system
- RSS – Reactor scram system
- SWS – Service water system.
- SFPC – Spent fuel pool cooling system
- SFPM – Spent fuel pool make-up water systems

The system for spent fuel pool cooling (SFPC) is assumed to be similar to the spent fuel cooling system at Forsmark 3. The reason to choose this example system for residual heat removal is that, since the Forsmark 3 solution includes a four-train solution, the model will be flexible and will enable analysis of a big range of hypothesis testing e.g. regarding repair, dynamic success criteria, etc. The main consequences that are analysed in the PROSAFE spent fuel pool model are boiling in the pool and uncovered fuel (large release).

The spent fuel pit cooling system performs three functions. The primary function is to remove decay heat, generated by the spent fuel elements stored in the pits, from the spent fuel pit water. The system consists of four redundant trains with separate pumps and heat exchangers (during normal power operation the system requirements to avoid boiling is by default is assumed to be 1-out-of-4 trains, but this may change depending on the sequence and different hypothesis testing). One train (1-out-of-4) in SWS is assumed to be required for cooling of SFPC pumps and heat exchangers.

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). The initial considered initiating event is spurious stop of the pump in operation, but the model is flexible so that other initiators can be considered (if necessary for the hypothesis testing).

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

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

Figure 21 and Figure 22 show simplified flow diagrams related to the safety systems relevant to the example. It should be noted that this example must not be interpreted as a representative boiling water reactor, but rather as an example for demonstrating the reliability analysis of representative nuclear safety.

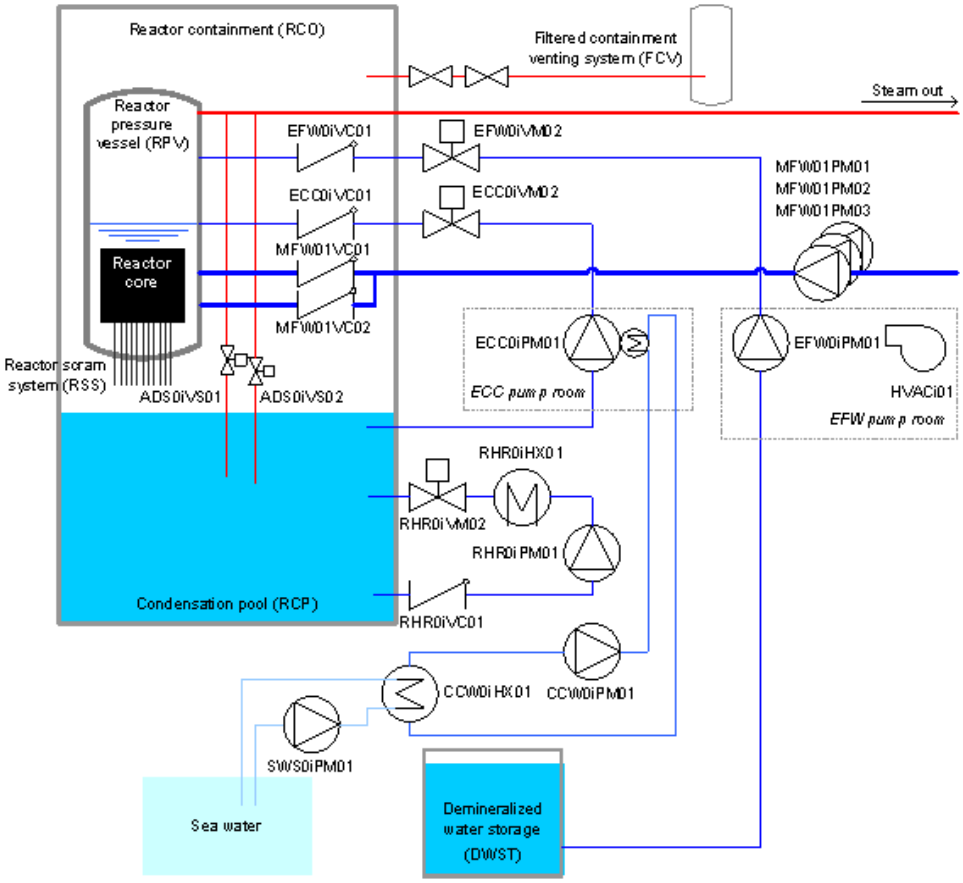

Figure 21. Flow diagram of one train of the example NPP**.**

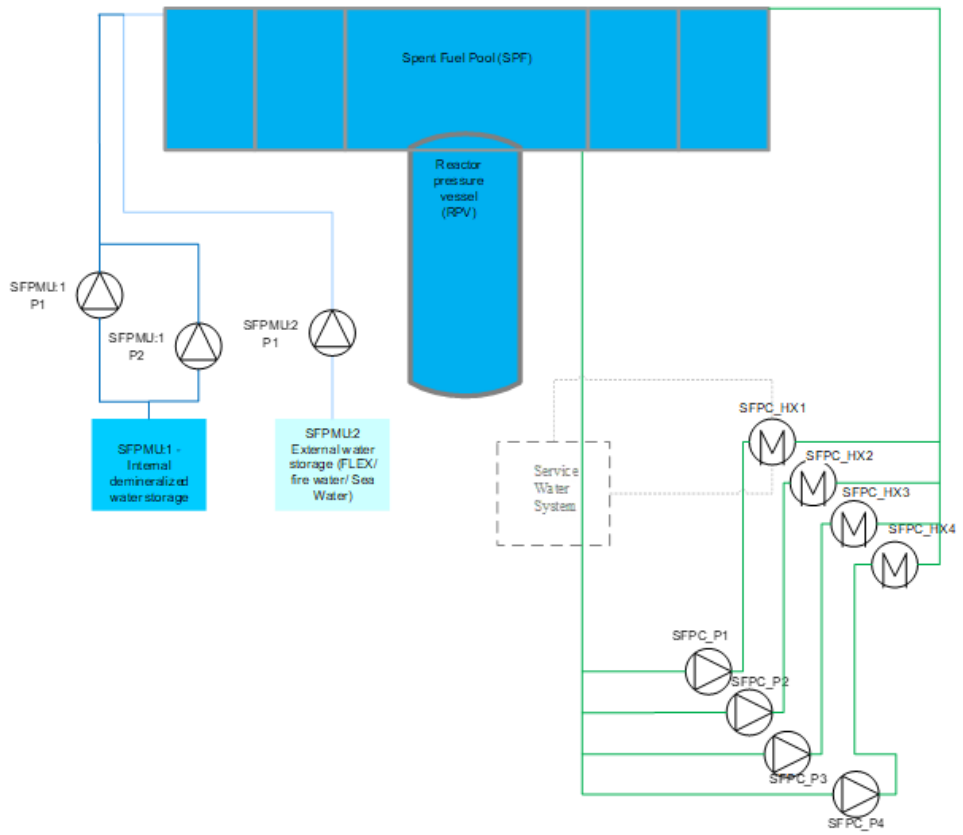

Figure 22. Flow diagram of example NPP Spent Fuel Pool Cooling System.

Table 23 presents failure mode and effects analysis for the frontline systems and the SFPM system of the example model.

Table 23. Failure modes and effects analysis of EFW, ECC and ADS.

System/component (*i* = division)	**Failure modes**	**Failure cause**	**Failure effect**
EFW (ECC)	Failure to provide coolant injection		No water to RPV
EFW division *i* (ECC division *i*)	Failure to provide coolant injection		EFW (ECC) train *i* unavailable for coolant injection
EFW*i*0PM01 (ECC*i*0PM01)	Failure to start Spurious stop	Mechanical failure Power supply I&C failure Component cooling failure Maintenance Alignment error	EFW (ECC) train *i* unavailable for coolant injection
EFW*i*0VM02 (ECC*i*0VM02)	Failure to open Spurious closure	Mechanical failure Power supply I&C failure Maintenance Alignment error	Train *i* unavailable for coolant injection
EFW*i*0VC01 (ECC*i*0VC01)	Failure to open Spurious closure	Mechanical failure	Train *i* unavailable for coolant injection
ADS	Failure to depressurize the primary circuit		ECC cannot inject water to RPV
ADS valve line *j* (8 valve lines)	Failure to open		Valve line unavailable for depressurization
ADS*i*0VS01, VS02	Failure to open	Mechanical failure Power supply I&C failure Operator error	Valve line unavailable for depressurization
SFPC_P1 (in operation)	Spurious stop	Mechanical failure Power supply	Loss of spent fuel pool cooling with train 1.
SFPC_P*i* (*i*= 2, 3, 4) (Stand-By)	Fails to start Spurious stop	Mechanical failure Power supply	Loss of spent fuel pool cooling with train *i*.
SFPC_HX*i* (*i*=1, 2, 3, 4)	Leak	Leakage	Loss of spent fuel pool cooling with train *i*.
SFPM:1 P1	Fails to start Spurious stop	Mechanical failure Power supply	No makeup water to spent fuel pool from system SFPM:1 train 1.
SFPM:1 P2	Fails to start Spurious stop	Mechanical failure Power supply	No makeup water to spent fuel pool from system SFPM:1 train 2.
SFPM:2 P1	Fails to start Spurious stop	Mechanical failure Power supply	No makeup water to spent fuel pool from system SFPM:2 train 1.

5. Conclusions

The PROSAFE project has during 2019 collected relevant information on aspects related to safe and stable state definition and assessment of long time windows in PSA, both information found in literature, current state-of-practice and the opinion of the Nordic nuclear industry on which areas that are of highest interest. The results of the information collection work package showed that definitions of safe (stable) state found in the literature and specified by the stakeholders of the PROSAFE project vary significantly. The opinion of the stakeholders was that this should not be a prioritized area for PROSAFE. Hence it was agreed that no activities would be included in the 2019 project work, but that a definition of Safe and Stable State should be developed within work package 3 in order to support the work there. The area will be further considered when planning the 2020 activities of PROSAFE.

Several literature sources identify the need for consideration of time dependencies, both within 24 hours mission time and beyond. Current PSAs generally considers 24 hours for PSA level 1 analysis and 48 hours for PSA level 2 analysis, while spent fuel pool analyses often apply longer mission times, e.g. 72 hours. Extending the mission time is recommended in the literature if plant conditions are not stable at the end of normal mission time. While traditional static PSA methods are sufficient for modelling normal accident scenarios, longer scenarios involve more dynamical behavior and time-dependencies that may be difficult to model using static methods. A large number of references on dynamic PSA methods can be found from the literature and the use of such methods could potentially make PSA more realistic.

In general when the available time is long there is no guidance in existing HRA methods on how to consider the effects of the extra time and the related issues, and while recovery actions are usually considered in PSA, repairs are usually not modelled within the mission times of 24 and 48 hours. Repair modelling is considered a challenge since it significantly increases the model complexity.

It has been shown in a few different studies that failure rates of some components are not constant over time, and time-dependencies in reliability data are often not considered in PSA. While this is seen as an important area, it was agreed that only the analysis of the effects of such data falls within the scope of PROSAFE, and that analysis of the data itself should be left out.

The findings of the information collection activity can be summarized as:

- There is a general agreement that the PSA would benefit from an advance in methodologies in order to reach a more realistic consideration and modelling of time related dependencies, e.g. approaches for dynamic modelling.
- There is agreed that methods for consideration of repair in the PSA are an important area for development.
- There is a consensus on the need of better guidance on how to estimate the effect of the long available times in the HRA.

The areas above was hence decided to be prioritized within PROSAFE and formed the basis of the methods work package which is divided into two parts, HRA methods and PSA methods.

For the HRA methods, requirements related to prolonged time window situations can be identified based on accepted standards such as ASME/ANS PRA standard and NRC HRA good practices. Relevant HFEs are identified from the stakeholder PSA/HRA studies as well as literature reviews. The qualitative part of the HRA process is found to be as important as the quantitative part and proper task analysis with proper timeline diagrams is suggested. Possible quantification approaches and relevant factors for consideration in the quantification are identified, e.g. multiple crews, parallel actions, decision from outside MCR, and error recovery to failed diagnosis and decision making.

Within the PSA methods it was concluded that for repair probabilities estimation there are dependencies that needs to be considered between different repair activities but also to other manual actions. The execution part should be analyzed with failure data but the diagnosis and decision part may need to be considered within the HRA. Crediting repair in PSA-modelling can be done by use of fault tree and/or event tree techniques if the repair situation is well defined, though there will be such a model complexity increase that direct modelling of repair events can only be recommended in PSA models of lesser complexity, e.g. spent fuel pool models. For models with already large complexity, e.g. a standard PSA level 1 or 2 for a reactor unit at-power, techniques using manipulation of the MCS-list and simple fault trees are better suited.

Modelling of 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 will require solutions that still must involve a great amount of simplifications as the models quickly would become much too complex. 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 may then be more advantageous compared to an ET/FT model and improve the realism in the results.

An exercise on modelling of dynamic success criteria using fault trees has been performed, which shows that 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.

The work performed within PROSAFE during 2019 have resulted in a number of findings, questions and conclusions that show the need of further activities, but also the need to prioritize between these activities. The following main areas in need of further investigation have been identified:

- Further investigation and improvement of HRA methods with regard to long time windows, and evaluations in pilot studies. Special attention should be given to (1) limiting human error probability, (2) dependency treatment, (3) human actions in FLEX context.
- Further investigation and improvement of PSA methods with regard to long time windows, and evaluations in pilot studies. Special attention should be given to (1)

methods and/or tools of semi-dynamic or dynamic character, (2) dependencies with regard to repair activities, (3) modelling of failure times in common cause failures.

6. 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.

7. Disclaimer

8. 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 Nuclear Society. 2009. ASME/ANS RA-S-2009 Standard for level 1/large early release frequency probabilistic risk assessment for nuclear power plant applications. New York.

American Nuclear Society. 2009. ANS/ASME-58.22-2014 Requirements for Low Power and Shutdown Probabilistic Risk Assessment. New York.

ASAMPSA2. 2011. Best-practices guidelines for L2PSA development and applications, Volume 1 - General. Euratom.

ASAMPSA2. 2013. Best-practices guidelines for level 2 PSA development and applications, Volume 2 - Best practices for the Gen II PWR, Gen II BWR L2PSAs. Extension to Gen III reactors. Euratom.

ASAMPSA_E. 2015. Lessons of the Fukushima Dai-ichi accident for PSA. Euratom.

ASME PRA standard: ASME/ANS RA-Sa-2009 Standard for Level 1/Large Early Release Frequency Probabilistic Risk Assessment for Nuclear Power Plant Applications. American Society of Mechanical Engineers 2009.

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.

Authén S., Bäckström, O., Cederhorn, E., Eriksson, C. He, X., Karanta, I., Kling, T., Massaiu, S., Olofsson, F., Sparre, E., Tyrväinen, T. 2019a. PROSAFE – Issues raised. NPSAG Summer Seminar 2019. Helsinki, Finland. May 22 2019.

Authén S., Bäckström, O., Cederhorn, E., Eriksson, C. He, X., Karanta, I., Kling, T., Massaiu, S., Olofsson, F., Sparre, E., Tyrväinen, T. 2019b. PROSAFE – A Joint Nordic Research Project on Modelling of Long Time Windows. 15th International conference on probabilistic safety assessment and management (PSAM15), Venice, Italy, 21-26 June, 2020.

Ayyub, B. 2001. Elicitation of expert opinions for uncertainty and risks. CRC Press.

Baron, S., Cruser, D., Messick Huey, B. eds., 1990. Quantitative modelling of human performance in complex, dynamic systems. National Academies Press.

Benhardt, H.C., Held, J.E., Olsen, L.M., Vail, R.E. & Eide, S.A. 1994. Savannah River Site human error data base development for nonreactor nuclear facilities. WSRC-TR-93-581, Savannah River Technology Center, Aiken, SC.

Bucci, P., Kirschenbaum, J., Mangan, L.A., Aldemir, T., Smith, C. & Wood, T. 2008. Construction of event-tree/fault-tree models from a Markov approach to dynamic system reliability. Reliability Engineering and System Safety. 93 (11): 1616-1627.

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.

Bury, K. 1999. Statistical distributions in engineering. Cambridge University Press.

Butler, J.S., Kapitz, D., Martin, R.P., Seifaee, F. & Sundaram, R.K. 2010. Analysis and justification of MAAP4.0.7 for PRA level 1 mission success criteria. Nuclear Technology. 170: 244-260.

Bye A., et. al. 2017. The Petro-HRA Guideline. IFE/HR/E-2017/001.

Bäckström, O., Bouissou, M., Gamble, R., Krcal, P., Sörman, J. & Wang, W. 2018. Introduction and Demonstration of the I&AB Quantification Method as Implemented in RiskSpectrum PSA. 14th International conference on probabilistic safety assessment and management (PSAM14), Los Angeles, CA, 16-21 September, 2018. Paper #203.

Cooke, R. 1991. Experts in uncertainty - opinion and subjective probability in science. Oxford University Press.

Guigueno, Y., Raimond, E., Duflot, N., Tanchoux, V., Rahni, N., Laurent, B. & Kioseyian, G. 2016. Severe accident risk assessment for NPPs: Software tools and methodologies for level 2 PSA development available at IRSN. 13th International conference on probabilistic safety assessment and management (PSAM13), Seoul, Korea, 2-7 October, 2016.

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.

Hassija, V., Senthil Kumar, C. & Velusamy, K. 2014. Markov analysis for time dependent success criteria of passive decay heat removal system. Annals of Nuclear Energy: 72: 298-310.

He, X. 2016. Dependencies in HRA. NPSAG REPORT 41-001:01.

He, X. 2017. Dependencies in HRA, Phase II. LRC Report 212171_R001.

He, X. 2018. Errors of Commission – Phase I. NPSAG REPORT 49-001:01.

He, X. & Olofsson F. 2019. Errors of Commission – Phase II. NPSAG REPORT 49-001:02.

Holmberg, J.-E. 2019. HRA methodology for Forsmark NPP and Ringhals NPP. NPSAG report 53-002, The Nordic PSA Group.

Idaho National Laboratory. 2014. Enhanced Component Performance Study: Emergency Diesel Generators 1998-2012. INL/EXT-14-31133

International Atomic Energy Agency. 1996. Human Reliability Analysis in Probabilistic Safety Assessment for Nuclear Power Plants: A Safety Practice. Safety Series No. 50-P-10.

International Atomic Energy Agency. 2006. Determining the quality of probabilistic safety assessment (PSA) for applications in nuclear power plants. IAEA-TECDOC-1511, Vienna.

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.

Jacquemain, D. et al. 2018. Status report on long term management and actions for a severe accident in a nuclear power plant. NEA/CSNI/R(2018)13, Nuclear Energy Agency. Draft. Limited availability.

Johanson G., et. al. 2015. EXAM-HRA A Practical guide to HRA. NPSAG Report 11-004-02.

Jung, W. & Park, J. 2019. Time-reliability correlation for the human reliability analysis of a digitalized main control room. International conference on applied human factors and ergonomics (AHFE 2019), Washington DC, July 24-28, 2019. pp. 88-94.

Karanki, D.R., Kim, T.-W. & Dang, V.N. 2015. A dynamic event tree informed approach to probabilistic accident sequence modeling: Dynamics and variabilities in medium LOCA. Reliability Engineering and System Safety. 142: 78-91.

Karanki, D.R. & Dang, V.N. 2016. Quantification of dynamic event trees - A comparison with event trees for MLOCA scenario. Reliability Engineering and System Safety. 147: 19-31.

Kichline, M. 2018. Human reliability analysis for using portable equipment [presentation]. United States Nuclear Regulatory Commission, EPRI HRA for FLEX workshop, February 28 - March 1, 2018.

Kirwan, B. & Ainsworth, L.K., Eds. 1992. A Guide To Task Analysis: The Task Analysis Working Group. London: Taylor & Francis.

Kirwan, B., Gibson, H., Kennedy, R., Edmunds, J., Cooksley, G. & Umbers, I. 2004. Nuclear Action Reliability Assessment (NARA): A Data-Based HRA Tool. PSAM 7 — ESREL'04 June 14–18, 2004, Berlin, Germany, Volume ISBN: 978-1-4471-1057-6.

Kirwan B., Umbers, I., Edmunds, J., et al. 2008. Quantifying the unimaginable – the case for human performance limiting values. PSAM9-0260.

Le Bot, P., Alengry, J. & De La Garza, C. 2016. Organising the Operation of Nuclear Reactors in Extreme Situations: Simulator Based-Test Methodology. Proceedings of the 39th Enlarged Halden Programme Group (EHPG) Meeting, Fornebu, Norway.

Ma, Z. & Buell, R. 2016. Safe and stable state in SPAR model event trees. Idaho National Laboratory, INL/LTD-16-38575, Idaho Falls.

MacLeod D. E., et al. 2014. Simplified Human Reliability Analysis Process for Emergency Mitigation Equipment (EME) Deployment, Probabilistic Safety Assessment and Management PSAM 12, June 2014, Honolulu, Hawaii.

Mandelli, D., Wang, C., Alfonsi, A., Smith, C., Youngblood, R. & Aldemir, T. 2019. Mutual integration of classical and dynamic PRA. International topical meeting on probabilistic safety assessment and analysis (PSA 2019), Charleston, SC, April 28 – May 3, 2019.

Metzroth, K.G. 2011. A comparison of dynamic and classical event tree analysis for nuclear power plant probabilistic safety/risk assessment [dissertation]. The Ohio State University, Ohio, USA.

Meyer, M. & Booker, J. 2001. Eliciting and analysing expert judgment - a practical guide. Society for Industrial and Applied Mathematics.

Munier, N. 2014. Risk management for engineering projects – procedures, methods and tools. Springer International Publishing Switzerland.

Norman, E., Brotherton, S. & Fried, R. 2008. Work breakdown structures – the foundation for project management excellence. John Wiley & Sons.

Nuclear Energy Institute. 2005. 10 CFR 50.69 SSC categorization guideline. NEI 00-04 (Rev 0).

NUREG/CR-1278. Swain, A.D. & Guttmann, H.E. 1983. Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications. Sandia National Laboratories for the U.S. Nuclear Regulatory Commission, Washington, DC.

NUREG-1921. EPRI/NRC-RES Fire Human Reliability Analysis Guidelines – Final Report. 2012.

NUREG/CR-6823. Handbook of Parameter Estimation for Probabilistic Risk Assessment. 2003.

NUREG/CR-6883. The SPAR-H Human Reliability Analysis Method. 2005.

NUREG-1792. Good Practices for Implementing Human Reliability Analysis (HRA). U.S. Nuclear Regulatory Commission. 2005.

NUREG/CR-7017. Preliminary, Qualitative Human Reliability Analysis for Spent Fuel Handling. U.S. Nuclear Regulatory Commission. 2012.

NUREG-CR 2199. An Integrated Human Event Analysis System (IDHEAS) for Nuclear Power Plant Internal Events At-Power Application. 2017.

NUREG-2198. The General Methodology of an Integrated Human Event Analysis System (IDHEAS-G). Draft version, 2019.

O'Connor, P. & Kleyner, A. 2012. Practical reliability engineering, 5th edition. John Wiley & Sons.

O'Hagan, A., Buck, C., Daneshkhah, A., Eiser, R., Garthwaite, P., Jenkinson, D., Oakley, J. & Rakow, T. 2006. Uncertain judgments - eliciting experts' probabilities. John Wiley & Sons.

Ortiz, N. R., Wheeler, T. A., Breeding, R. J., Hora, S., Meyer, M. A. & Keeney, R. L. 1991. Use of expert judgment in NUREG-1150. Nuclear Engineering and Design. 126: 313-331.

Queral, C., Gomez-Magan, J., Paris, C., Rivas-Lewicky, J., Sanchez-Perea, M., Gil, J., Mula, J., Melendez, E., Hortal, J., Izquierdo, J.M. & Fernandez, I. 2018. Dynamic event trees without success criteria for full spectrum LOCA sequences applying the integrated safety assessment (ISA) methodology. Reliability Engineering and System Safety. 171: 152-168.

Park J., et al. 2019. Treatment of human and organizational factors for multi-unit HRA: application of SPAR-H method. Annals of Nuclear Energy. 132: 656–678.

Parry, G., et al. 1992. An Approach to the Analysis of Operator Actions in PRA. EPRI TR-100259, Electric Power Research Institute, Palo Alto, CA.

Plott, B., Pearson, J. & Shaw, C. 2017. Micro Saint Sharp User Manual v3_8. Lulu.com.

Presley M., Parry, G., Julius, J., et al. 2016. Use of minimum bounds for joint human error probabilities in PRA. PSAM 13, 2~7 October, 2016, Seoul, Korea

Pyy, P. & Himanen, R. 1996. A Praxis Oriented Approach for Plant Specific Human Reliability Analysis - Finnish Experience from Olkiluoto NPP. In: Cacciabue, P.C., and Papazoglou, I.A. (eds.), Proc. of the Probabilistic Safety Assessment and Management '96 ESREL'96 — PSAMIII Conference, Crete, June 24–26, 1996. Springer Verlag, London, 1996, pp. 882–887.

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.

Raganelli, L. & Kirwan, B. 2014. Can we quantify human reliability in Level 2 PSA? PSAM 2014 - Probabilistic Safety Assessment and Management.

Raimond, E. et al. 2013. ASAMPSA2 "Best-Practices Guidelines for Level 2 PSA Development and Applications", April 2013.

Selvik, J. & Ford, E. 2017. Down Time Terms and Information Used for Assessment of Equipment Reliability and Maintenance Performance, chapter from the book "System Reliability".

Siegel, A. & Wolf, J. 1969. Man-machine simulation models: psychosocial and performance interaction. Wiley-Interscience.

Siegel, A., Bartter, W., Wolf, J., Knee, H., Haas, P. 1984. The MAintenance Personnel Performance Simulation (MAPPS) model. Proceedings of the Human Factors Society, 28th annual meeting, 247-251.

Smith, C.L., Wood, T., Knudsen, J. & Ma, Z. 2016. Overview of the SAPHIRE probabilistic risk analysis software. 13th International conference on probabilistic safety assessment and management (PSAM13), Seoul, Korea, 2-7 October, 2016.

Swain, A.D. 1987. Accident sequence evaluation program human reliability analysis procedure. NUREG/CR-4772, United States Nuclear Regulatory Commission, Washington DC.

Tyrväinen, T. & Karanta, I. 2019. Dynamic containment event tree modelling techniques and uncertainty analysis. VTT Technical Research Centre of Finland Ltd, VTT-R-06892-18, Espoo.

Tyrväinen, T., Karanta, I., Kling, T., Sparre, E., Authen, S., He, X., Olofsson, F., Bäckström, O., Massaiu, S., Eriksson, C. & Cederhorn, E. 2019. Prolonged available time and safe states - State of the art review. VTT Technical Research Centre of Finland Ltd, VTT-R-00883-19, Espoo. 37+5 pp.

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. 1977. Periodic testing of diesel generator units used as onsite electric power systems at nuclear power plants, Revision 1. Regulatory guide 1.108, Washington DC.

United States Nuclear Regulatory Commission. 1983. Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications. NUREG/CR-1278, Washington DC.

United States Nuclear Regulatory Commission. 2003. Handbook of parameter estimation for probabilistic risk assessment. NUREG/CR-6823, Washington DC.

United States Nuclear Regulatory Commission. 2005. Good Practices for Implementing Human Reliability Analysis (HRA). NUREG-1792, Washington DC.

United States Nuclear Regulatory Commission. 2005. The SPAR-H Human Reliability Analysis Method. NUREG/CR-6883, Washington DC.

United States Nuclear Regulatory Commission. 2006. Evaluation of human reliability analysis methods against good practices. NUREG-1842, Washington DC.

United States Nuclear Regulatory Commission. 2010. Confirmatory thermal-hydraulic analysis to support specific success criteria standardized plant analysis – Surry and Peach Bottom. NUREG-1953, Washington DC.

United States Nuclear Regulatory Commission. 2012. EPRI/NRC-RES Fire Human Reliability Analysis Guidelines. NUREG-1921, Washington DC.

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. 2014. Compendium of analyses to investigate select level 1 probabilistic risk assessment end-state definition and success criteria modeling issues. NUREG/CR-7177, Washington DC.

United States Nuclear Regulatory Commission. 2017a. Guidance on the treatment of uncertainties associated with PRAs in risk-informed decision making. NUREG-1855, Washington DC.

United States Nuclear Regulatory Commission. 2017b. Risk assessment of operational events, Handbook, Volume 1 - Internal events, Revision 2.02. Washington DC.

Williams, T. 2002. Modelling complex projects. John Wiley & Sons.

Working group on risk assessment, WGRISK. 2017. Probabilistic safety assessment insights relating to the loss of electrical sources. Nuclear Energy Agency, Organisation for Economic Co-operation and Development, NEA/CSNI/R(2017)5.

Bibliographic Data Sheet **NKS-432**

Title	Prolonged Available Time and Safe States
Author(s)	Tero Tyrväinen[1], Ilkka Karanta[1], Terhi Kling[1], Xuhong He[2], Frida Olofsson[2] Ola Bäckström[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]Lloyd's Register Consulting – Energy AB, [3]IFE (Institute for Energy Technology), [4]Risk Pilot AB
ISBN	978-87-7893-522-9
Date	February 2020
Project	NKS-R / PROSAFE
No. of pages	116
No. of tables	23
No. of illustrations	22
No. of references	95

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.

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