NKS-419
ISBN 978-87-7893-508-3

Site risk analysis for nuclear installations

Jan-Erik Holmberg[1]
Stefan Authén[1]
Kim Björkman[3]
Ola Bäckström[2]
Xuhong He[2]
Salvatore Massaiu[4]
Tero Tyrväinen[3]

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

February 2019

Abstract

Currently, multi-unit risks have not typically been adequately accounted for in risk assessments, since the licensing is based on unit-specific probabilistic safety assessment (PSA) with focus on a reactor accident. NKS-R project SITRON (SITe Risk Of Nuclear installations) has searched for practical approaches for Nordic utilities to assess the site level risk. Starting point of SITRON work has been the fact that the Nordic utilities already have good unit-specific PSAs. Therefore, the question is what additional efforts are needed to obtain a site level risk assessment. Practically, it means two tasks: 1) to identify relevant inter-unit dependences, and 2) to quantify the site level risk. Inter-unit dependences consist of multi-unit initiating events, shared systems, structures and components, dependences in human actions, inter-unit common cause failures, and plant operating state combinations. SITRON provides guidance how to perform the identification of dependences and how to select relevant dependences for quantification (screening). Quantification of site risk can be performed quite straightforwardly, given that the quality of the single-unit PSAs is sufficient. SITRON project has also included a survey on the role of Emergency Response Organisation (ERO), often referred to as the Technical Support Centre (TSC) in accident management. Based on responses from four plants in Finland and Sweden, SITRON has investigated different implementations of EROs with respect to possible impact on operational decisions in severe accident and multi-unit scenarios. The human role in severe accidents differs markedly: new decision makers (ERO and TSC rather than main control room); different instructions (guidelines rather than procedures); different decisions (involving trade-offs, novel actions, and strategies contrary to conventional knowledge); inter-unit influences; unreliability of instrumentation; and long time windows for actions.

Key words

Probabilistic safety assessment, nuclear power plant, site risk, multi-unit risk, technical support centre

NKS-419
ISBN 978-87-7893-508-3
Electronic report, February 2019
NKS Secretariat
P.O. Box 49
DK - 4000 Roskilde, Denmark
Phone +45 4677 4041
www.nks.org
e-mail nks@nks.org

Site risk analysis for nuclear installations

Final Report from the NKS-R SITRON activity

(Contract: AFT/NKS-R(18)125/3)

Jan-Erik Holmberg, Stefan Authén[1]
Ola Bäckström, Xuhong He[2]
Kim Björkman, Tero Tyrväinen[3]
Salvatore Massaiu[4]

[1]Risk Pilot AB
[2]Lloyds Register Consulting – Energy AB
[3]VTT Technical Research Centre of Finland Ltd
[4]IFE (Institute for Energy Technology)

Table of contents

Project reports / Appendices

Each of the works package reports (except pilot study reports) produced during the project are provided as attachments to this report:

Appendix A – WP1 Risk Metrics (Holmberg 2017)
Appendix B – WP2 Method development (Bäckström et al. 2019)
Appendix C – WP3 Site PSA model management (Tyrväinen & Björkman 2019)
Appendix D – WP5 Technical support centre (Massaiu 2019)

Acronyms

BWR	Boiling water reactor
CD	Core damage
CDF	Core damage frequency
CSNI	Committee on the Safety of Nuclear Installations (OECD/NEA)
FDF	Fuel damage frequency
HEP	Human error probability
HFE	Human failure event
IAEA	International Atomic Energy Agency
IE	Initiating event
LERF	Large early release frequency
LRF	Large release frequency
MUCDF	Multi-unit core damage frequency
MUIE	Multi-unit initiating event
MULERF	Multi-unit large early release frequency
MUPDS	Multi-unit plant damage state
NEA	OECD Nuclear Energy Agency
NPP	Nuclear power plant
NRC	U.S. Nuclear Regulatory Commission
OECD	Organisation for Economic Co-operation and Development
PDS	Plant damage state
PSA	Probabilistic safety assessment
RC	Release category
RCF	Release category frequency
SAFIR	Finnish Research Programme on Nuclear Power Plant Safety
SAP	Safety Assessment Principles (UK)
SCDF	Site core damage frequency
SSM	Strålsäkerhetsmyndigheten, Swedish Radiation Safety Authority
SUIE	Single-unit initiating event
SUPDS	Single-unit plant damage state
STUK	Säteilyturvakeskus, Radiation and Nuclear Safety Authority
SUCDF	Single-unit core damage frequency
VTT	Technical Research Centre of Finland
WGRISK	OECD/NEA CSNI Working Group on Risk Assessment
YVL	Ydinvoimalaitos (nuclear power plant), STUK's regulatory guide series for nuclear facilities

1. Introduction

After the Fukushima Daiichi accident in March 2011 general interest in site level Probabilistic Safety Assessment (PSA) has increased. Major part of the nuclear power sites house more than one reactor unit and other nuclear facilities such as spent fuel pool storage. Currently, multi-unit risks have not typically been adequately accounted for in risk assessments since the licensing is based on unit-specific PSA with focus on a single reactor accident.

The methodology for a site level risk analysis needs to consider the dependencies between the units at a site. Site risk analysis does not only cover reactors but also other relevant sources for radioactive release such as spent fuel pools and storages. The dependencies can be caused by external hazards, which can affect multiple units at the same time; shared operational and safety systems at the site; common staff who should manage the situations; etc. Site risk analysis is not only a matter of extending current risk analyses to properly cover inter-unit dependencies in the risk assessment, but it should also provide risk insights for the site level safety management, e.g., w.r.t., severe accident management, emergency preparedness, design, operation and maintenance of shared systems.

1.1. Purpose

SITRON (SITe Risk Of Nuclear installations) is a Nordic collaboration project. The first objective of the SITRON project is to search for practical approaches for Nordic utilities to assess the site level risk. This objective concerns with safety goals, risk criteria and PSA applications for a multi-unit site. The second objective of the project is to develop methods to assess risk for multi-unit scenarios. This objective concerns with methods to identify, analyse and model dependencies between the units.

1.2. Scope of project

SITRON 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 for single units. In this way, the scope of SITRON can be defined to cover an assessment of fuel damage and radioactive release risk related to reactors and spent fuel pool at a site, i.e., level 1 and level 2 PSA.

The method development has been driven by two practical pilot studies. The both pilot studies concerns an assessment of a two-unit combination. Therefore, the developed method assumes a two-unit case, but it could be generalized to a site risk analysis with more units.

1.3. Project organization

SITRON studies have been carried out in six work packages:

- WP1 Risk metrics;
- WP2 Multi-unit PSA methods;
- WP3 PSA model management;
- WP4 Pilot studies;
- WP5 Technical support centre;
- WP6 Meetings and management.

WP1 provided an overview of internationally applied risk criteria for site risk, and proposed risk metrics for site level risk studies.

WP2 was dedicated to PSA analysis and modelling issues which are specific for a site level PSA and different from a single-unit PSA. A framework has been set for identification of dependencies, screening principles, probability estimation, modelling of dependencies and quantification.

WP3 provided guidance about site PSA documentation, database management, use of single-unit models and the analysis process.

WP4 covered two pilot studies: one for Forsmark nuclear power plant (NPP) site and another for Ringhals NPP site. Multi-unit initiating events, systems dependencies and human actions dependencies have been identified. Loss of offsite power (LOOP) initiating event has been used as an example for the scenario modelling and quantification.

WP5 studied in which manner the technical support centre's (TSC) is defined at different sites in the Nordic countries, how it is expected to operate and what its main challenges are in multi-unit scenarios, and whether/how its role is credited by human reliability analysis (HRA) in the context of PSA.

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. Two utilities provided a realistic case to be used as pilot studies for method development (WP4). In WP5, a survey on the role of technical support centre was carried out among the utilities.

The project has created interest in many international organizations and has fostered Nordic participation in several international site level PSA activities. The project results were communicated in the International Workshop on Status of Site Level PSA Developments organised by OECD/NEA Working group RISK, July 18–20, 2018 (Holmberg et al. 2018b). SITRON project is a member of the IAEA coordinated research project "Probabilistic Safety Assessment (PSA) Benchmark for Multi-Unit/Multi-Reactor Sites" (I31031), which was launched in June 2018. In addition, results of SITRON have been presented in ESREL2018 and PSAM14 conferences (Holmberg et al. 2018a, Bäckström et al. 2018a).

1.5. Report contents

This is a summary report of the work packages of SITRON project. The following sections briefly summarize the work performed under each work package as outlined in Section 1.3. Complete discussions on each work package, except the pilot study reports, are attached as appendices to this report where the appendices represent the actual documentation that has been produced for each task.

1.6. Acknowledgements

The work has been co-financed by SAFIR2018 (The Finnish Research Programme on Nuclear Power Plant Safety 2015–2018), Forsmark Kraftgrupp AB, Ringhals AB, Swedish Radiation Safety Authority (SSM), 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.

1.7. Disclaimer

2. Risk metrics

This section is summary of the WP1 report (Appendix A) and the WGRISK workshop paper (Holmberg et al. 2018b).

2.1. Definitions

A “single-unit PSA” (SUPSA) means a PSA made for a nuclear facility such as the reactor facility or unit and the interim storage for spent fuel. A single-unit PSA is assumed to cover all fuel locations within the facility. For a reactor unit, the reactor core and the fuel pool are the relevant locations from the risk assessment point of view. Single-unit PSA can be also understood to refer the types of risk analyses that currently have been prepared for licensing of nuclear facilities.

Ideally, a single-unit PSA should also cover multi-unit scenarios to be able to represent comprehensively the risk (e.g. core damage risk and large release risk) associated with unit, i.e., SUPSA should be a model that provides correct unit-specific risk metrics. Realistically, most current single-unit PSAs are somewhat limited to consider multi-unit scenarios, which is one of the motivations for a site risk analysis.

A “multi-unit PSA” (MUPSA) or “site level PSA” means a PSA or a set of PSAs made to cover accident scenarios related to all fuel locations at the site, including spent fuel transportations within the site. Multi-unit PSA can be also understood to be an extension of a single-unit PSA which can be used to quantify multi-unit risk metrics.

Figure 1 illustrates the scope of various risk assessments with respect to the concepts “site”, “unit” and “source” (or fuel location) for a hypothetical site with two reactor units and an interim storage for spent fuel. “Site” covers all units and fuel locations at the site. “Unit” refers to each facility at the site, which has an operating license of its own. In this example, there are three units/facilities at the site. “Source” refers to each point at the site where spent fuel can be located and for which a separate risk assessment can be carried out.

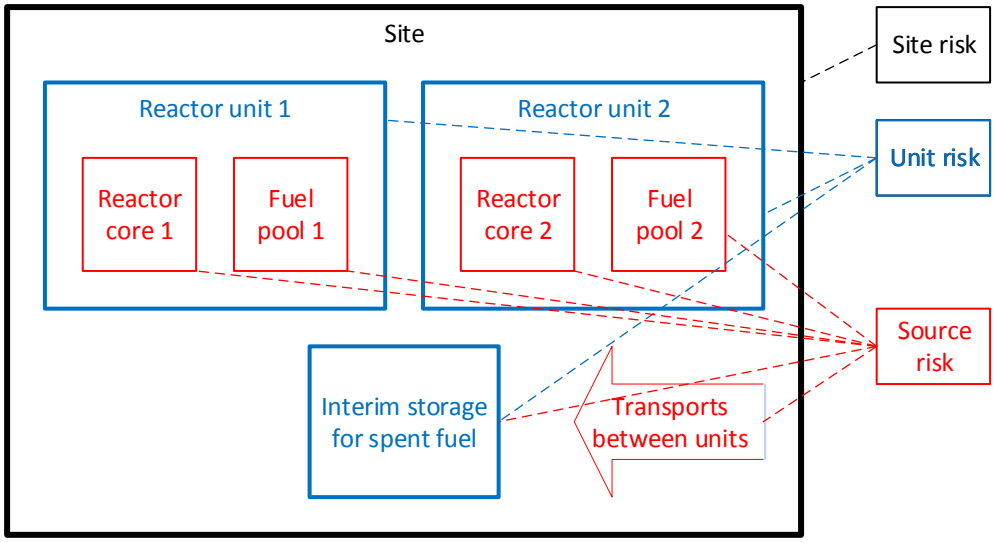


Figure 1. Illustration of concepts "site", "unit" and "source" from the PSA scope point of view.

In level 1 PSA, the main risk metric is core damage frequency (CDF), which is usually integrated into a single number: The annual core damage frequency representing the risk level of an average configuration of the reactor over all plant operating states. In the site risk analysis context, the meaning of CDF needs to be further specified by defining which sources and scenarios are included in the quantification of CDF. For instance, PSA for a reactor may also include accident scenarios for the fuel pool within the unit, though usually limited to scenarios that can happen during refuelling outage. Level 1 PSA risk metric for such accidents can be called fuel damage frequency (FDF).

In level 2 PSA, multiple risk metrics are applied to categorise various releases, e.g. large release or large early release. In SITRON, these risk metrics are generally called release category frequency (RCF), where the meaning of a release category has to be specified. As discussed above in the level 1 PSA risk metrics context, also the scope of the quantification must be specified. Site level risk metrics are further discussed in Section 2.4.

2.2. Current practice for single-unit PSAs in Finland and Sweden

SITRON project has considered risk metrics from the point of view of Nordic conditions. Both in Finland and Sweden, the requirement is to perform full scope level 1 and 2 PSA, but there is no requirement to perform level 3 PSA. There is also no requirement to quantify site level risk metrics.

In Finland, STUK's PSA guide YVL A.7 defines target values for a reactor, both for level 1 and 2 PSA to be applied in construction as well as operating license application phase (STUK 2013). In Finland, the main risk metric is related to the definition for a large release, 100 TBq of Cs-137, as defined in the regulatory guide (STUK 2013). In addition, the contribution from large early releases is quantified, but there is no specific requirement or definition for that.

The Finnish large release criterion is defined to "take into account all of the nuclear fuel located at the plant unit. A spent nuclear fuel storage external to the plant unit is considered a separate nuclear facility for whose analysis the aforementioned criteria apply."

In Sweden, the SSM regulation does not specify numerical risk criteria. The utilities have defined target values for level 1 and 2 PSA (Holmberg & Knochenhauer 2007). Core damage is defined similarly as in Finland. The main release category considered in level 2 PSA is "unacceptable release", which is a release more than 0.1 % of the core inventory of Cs-134 or Cs-137 from an 1800 MWt boiling water reactor (Barsebäck 1 unit). This is so called "RAMA" criterion defined in 1980's when the decision was made to implement severe accident mitigation systems for the nuclear power plants.

2.3. International status

Most countries apply CDF and large (early) release frequency (LRF/LERF) based risk criteria in the regulatory context. These are used as surrogates to higher, society level safety goals and they are applied per reactor (or facility). Comprehensive descriptions of nuclear risk criteria can be found in (Holmberg & Knochenhauer 2007), (OECD/NEA 2009), and (OECD/NEA 2012).

In UK and Canada, site level risk criteria have been defined for level 3 PSA. In Canada, site-based safety goals are under development. In UK, the Safety Assessment Principles (SAPs) have been clearly stated for multi-unit sites.

U.S.NRC (1986) Safety Goal Policy Statement, establishes two quantitative objectives that were to be used to determine achievement of the site-level qualitative safety goals:

- The risk to an average individual in the vicinity of a nuclear power plant of prompt fatalities that might result from reactor accidents should not exceed one-tenth of one percent (0.1%) of the sum of prompt fatality risks resulting from other accidents to which members of the U.S. population are generally exposed.
- The risk to the population in the area near a nuclear power plant of cancer fatalities that might result from nuclear power plant operation should not exceed one-tenth of one percent (0.1%) of the sum of cancer fatality risks resulting from all other causes.
- However, when the aggregate risk criteria based on CDF and LERF risk metrics are used, they are used per reactor unit.

2.4. Suggested risk metrics

2.4.1 Risk metrics for a single-unit PSA

Risk metrics for a single-unit PSA can be basically defined following the current practices. An important issue is in which manner the fuel pool related (and possibly some other release sources in the same reactor unit) accident scenarios should be treated. Since current licensing of NPPs is facility-based, we think that a risk aggregation should follow the same scope. As discussed in Section 2.1, single-unit PSA should also cover multi-unit scenarios.

Table 1 summarizes the proposed risk metrics for a single-unit PSA. In addition to these metrics, risk importance measures such as Fussell-Vesely importance measure and risk increase factors should be utilized to support the presentation and interpretation of the results.

Table 1. Proposed risk metrics for a single-unit PSA.

1. CDF/FDF per fuel location (core, pool, etc.)
2. RCF per fuel location (core, pool, etc.). This risk metric can cover one or more "release frequencies" corresponding with the defined release categories.
3. Integrated FDF for the reactor unit (all fuel locations)
4. Integrated RCF for the reactor unit (all fuel locations). This risk metric can cover one or more "release frequencies" corresponding with the defined release categories.

CDF = Core damage frequency, FDF = Fuel damage frequency, RCF = Release category frequency

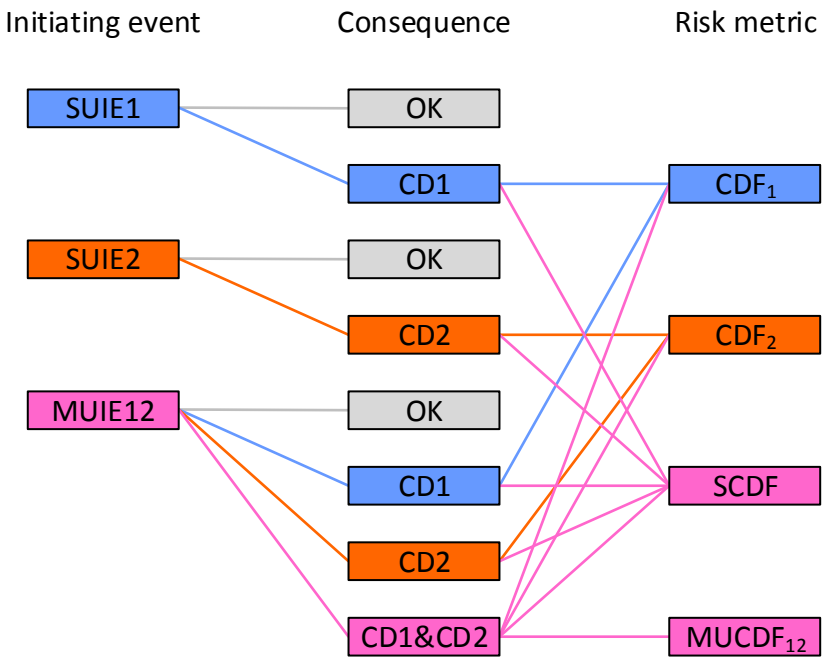
2.4.2 Risk metrics for a site PSA

There are several options for site level risk metrics, i.e., metrics for various double, triple and quadruple combinations of units (fuel locations) at the site. When accounting for combinations, it is important to notice that there is a principal difference between level 1 risk metrics and level 2 risk metrics. The level 1 risk metrics are based on binary conditions (fuel damage happens vs. does not happen), while level 2 risk metrics are derived by partitioning a "continuous" property (magnitude and timing of release) into a limited number of classes by threshold values. Thus, the level 1 risk metrics concern the number of damaged units, but level 2 risk metrics are defined by the release magnitudes regardless of the number of units involved. Therefore, the level 1 and 2 risk metrics are discussed separately below.

Figure 2 presents the link between site risk metrics and site risk accident sequences. The example represents two-unit site and is limited to level 1 PSA accident sequences. Accident end states can be defined depending on which unit is damaged or if multiple units are damaged ("CD1", "CD2" or "CD1&CD2" in Figure 2). Risk metrics are obtained by summing the frequencies of the corresponding sequences. Summing provides correct frequencies since the accident sequences are exclusive.

The blue respectively red risk metrics should be obtained by a single-unit PSA model, if properly modelled and quantified. The pink risk metrics cannot be directly obtained from a single-unit PSA, but a further elaboration is needed or a development of a site PSA model.

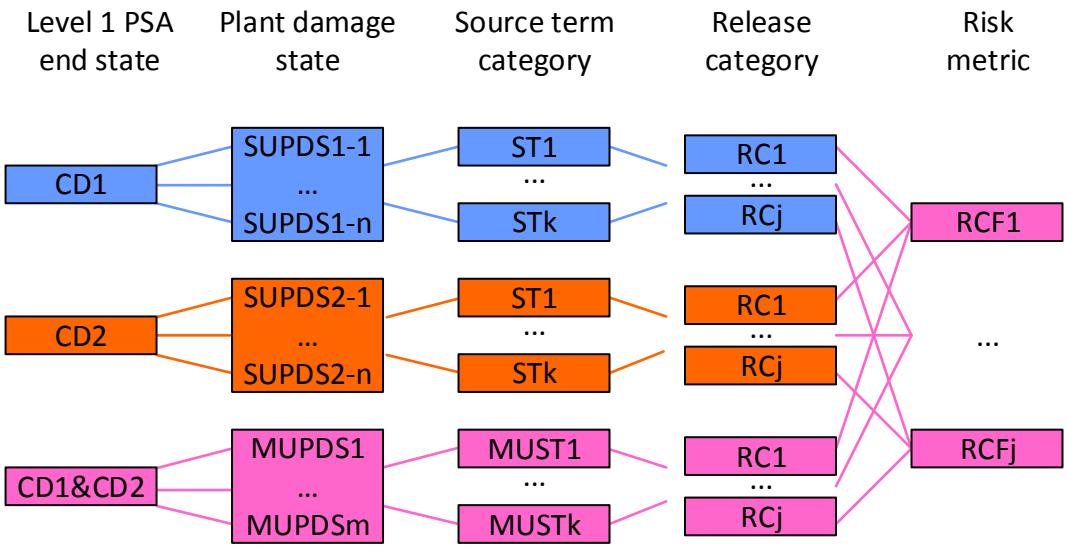
In case of more than two units, the number of combinations increases. It must be specified whether MUCDF is calculated for a particular unit combination or e.g. considering all combinations with at least two units. This definition is left open here since it depends on the intended application of such risk metrics.



SUIE = Single-unit initiating event
MUIE = Multi-unit initiating event
CD = Core damage
CDF = Core damage frequency
SCDF = Site core damage frequency
MUCDF = Multi-unit core damage frequency

Figure 2. Link between site risk accident sequences and site risk metrics in level 1 PSA for a two-unit site.

The risk metrics for level 2 PSA are principally different from level 1 risk metrics due to the release magnitude and timing component of the metrics. Figure 3 depicts a schematic level 2 PSA model for a site risk analysis, starting from the end states of site level 1 PSA. The proposed principle is that same release categories and associated risk metrics could be applied for multi-unit PSA as for single-unit PSA. This approach means that multi-unit source terms (MUST) shall be categorised into applicable release categories. A single-unit source term is characterised by the release magnitude and timing. A multi-unit source term can be obtained by aggregating single-unit source term so that release magnitude is sum of the magnitude of single-unit source terms and timing is determined by the timing of the earliest release. Table 2 summarises the proposed risk metrics.



CD = Core damage
SUPDS = Single-unit plant damage state
MUPDS = Multi-unit plant damage state
ST = Source term category
MUST = Multi-unit source term category
RC = Release category
RCF = Release category frequency

Figure 3. Event sequences and associated release category risk metrics for a level 2 PSA of a two-unit-site**.**

Table 2. Proposed risk metrics for a multi-unit PSA.

Risk metric
1. Site core/fuel damage frequency (SCDF/SFDF)
2. Multi-unit core/fuel damage frequency (MUCDF/MUFDF). For this risk metric, one needs to specify whether particular combinations or "full disaster" at the site are considered.
3. Site release category frequency. This risk metric can cover one or more "release frequencies" corresponding with the defined release categories. The same release categories can be applied to single-unit and multi-unit scenarios. In multi-unit release scenarios, the categorisation of releases is based on the aggregated source term, i.e., the magnitude of the release is the sum of releases and timing of the release could be determined by the time point exceeding the release category limit.

3. Method for site risk analysis

This section is summary of the WP2 report (Appendix B). The first analysis step is to select the scope of the site level PSA. This includes selection of which radioactive sources to consider, possible plant operating states, initiators to include and end states to study as illustrated in Figure 4. The scope of the single-unit PSA needs to be consistent with the selected site level scope.

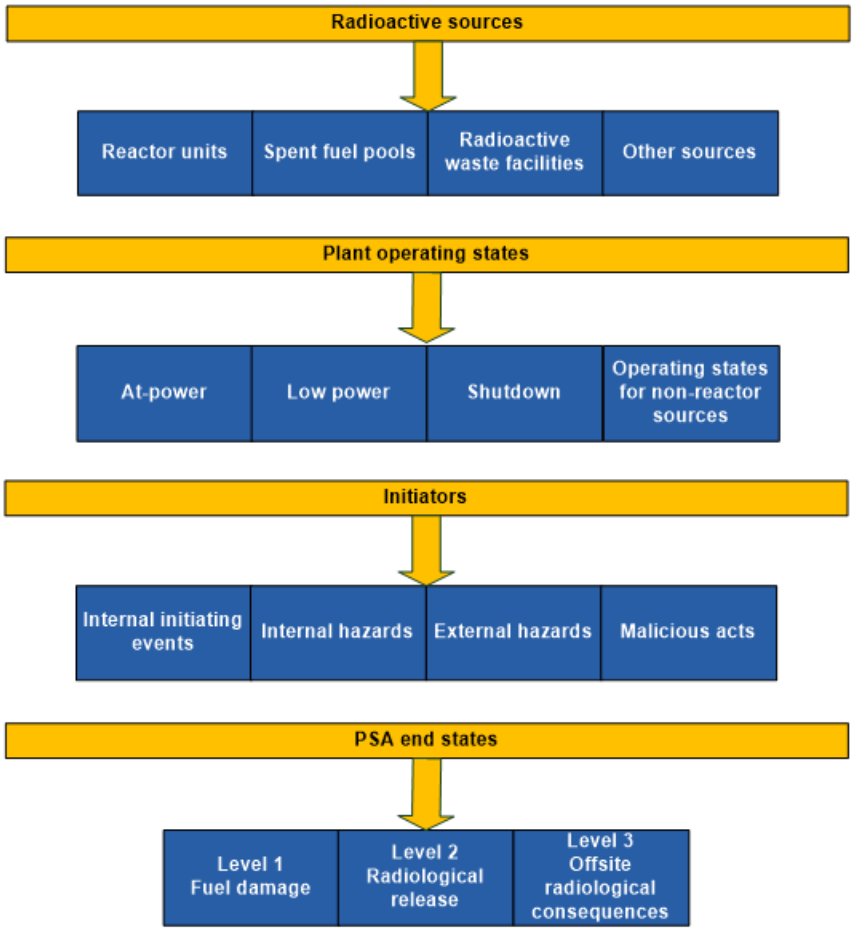


Figure 4. Selection of analysis scope for site level PSA.

3.1. General screening principles

The number of multi-unit scenarios is expected to be large even for a site with only two reactor units. For this reason, some screening principles are needed to reduce the number of analysed scenarios. Qualitative screening follows qualitative principles to classify dependencies, see further discussion in Section 3.4. Quantitative screening applies probabilistic criteria to screen out insignificant dependencies. In site PSA context, quantitative screening can be performed based on the risk importances of basic events related to the dependencies in single-unit PSAs. A dependency can mean a potential multi-unit initiating event, a combination of plant operating states (POS) or some potential dependency between systems, structures, components or operator actions.

When studying the risk importance of a dependency, a good practice is to group together all related items so that so called slicing error is avoided when screening is performed individually. In other words, similar initiating events are grouped together, POSs are considered as larger entities and other dependencies as groups of related basic events.

Based on literature surveys, e.g. (Hudson 2018), results from current Nordic PSAs and results from pilot studies, it has been concluded that a reasonable individual screening criterion for level 1 PSA risk importance can be set to 1E-8/yr and for level 2 PSA to 1E-9/yr. This means that if the contribution of scenarios where the dependency is present in single-unit PSA can be shown to be smaller than 1E-8/yr for level 1 PSA and smaller than 1E-9/yr for level 2 PSA

(using appropriate release category in level 2), it can be concluded with a good confidence that the dependency will not be significant from the site risk perspective.

One application of this screening principle is that it can be used to justify that it is not meaningful to study combinations of independent initiating events in a site PSA. Another practical application is that it can be used to justify that there are only few relevant POS combinations that are worth studying (see more discussions in the next sections).

3.2. Plant operating state (POS) impact

A comprehensive multi-unit scenario assessment may have to account for the units' various combinations of POSs. Available safety systems and recovery actions differ between the different POSs. A reasonable approach should be identified to cover relevant configurations from the site level point of view. A complete consideration of all possible combinations of POSs between several units could lead to a large number of "site" POS combinations.

To limit the amount of POS combinations to consider, it is suggested that POSs are merged together into a fewer POS groups. Since the multi-unit scenarios typically have impact on core cooling and residual heat removal functions, regrouping of POSs can be based on the configuration of residual heat removal systems. The analysis of multi-unit POSs could thus include the following steps:

- Estimate the time shares of these larger POS groups.
- Define time windows for core/fuel damage in case of loss of residual heat removal in each POS group.
- Consider possibly screening out of a POS group due to short duration or due to very long time window to fuel damage.
- Categorise multi-unit initiating events from their season and POS group dependency point of view to screen out irrelevant combinations. Season dependency is related to external hazards which can have different likelihood, e.g. during winter compared to summer season, while longer outages are typically carried out in Nordic NPPs during the summer season.

The analysis of POS impact is an iterative process together with the selection of multi-unit initiating events (see next section).

3.3. Identification of relevant initiators

The initiating event analyses in the existing single-unit PSAs should be reviewed to identify which events can affect one unit only and which events can impact multiple units concurrently. The initiating events could be categorized as follows:

- Single-Unit Initiating Events – the initiating events occur in one unit only and will not affect other units or radioactive sources (except possibly in a later phase of the accident), e.g. a primary circuit pipe break.
- Multi-Unit Initiating Events (MUIE) – the initiating events challenge two or more units or radioactive sources on the site concurrently, e.g. seismic events and other external hazards.
- Partial Multi-Unit Initiating Events – the initiating events occur on a single unit or impact multiple units, depending on the cause. An example is loss of offsite power which can

affect a single unit or any combination of units depending on the specific causes. Events in this category are placed into one of the previous initiating event categories depending on the specific cause(s).

Partial multi-unit events may, conservatively, be considered as multi-unit events to limit the work.

A single-unit event may be relevant from a multi-unit perspective if the single-unit event has a potential to propagate, e.g. through causing a secondary loss of offsite grid or through a fire that spreads between units. A single-unit event could also potentially, through a severe accident, cause an initiating event for the other units.

3.4. Identification and selection of dependencies

For each relevant initiator relevant dependencies need to be identified. The dependencies can be:

- Shared structures, systems and components (SSCs)
- Identical components (common cause failures)
- Spatial dependencies
- Human and organizational dependencies
- Simultaneous maintenance
- State-of-knowledge dependencies.

The dependencies related to shared SSCs, inter-unit common cause failures (CCF) and operator actions will likely be of importance to a multi-unit analysis. Dependencies through spatial interaction may be relevant if the initiating event has a potential to spread to another unit (for example fire) or if the accident sequence causes damage that would affect an adjacent unit. Simultaneous maintenance is likely possible to screen out (for example simultaneous scheduled maintenance).

State-of-knowledge dependency is created by the epistemic uncertainty in the estimation of probabilities of events. An example is phenomenological events, such as a steam explosion, considered in level 2 PSA. If two identical reactor units are under same severe accident conditions, same probabilities would be applied for phenomenological events. The applied probabilities reflect both the epistemic uncertainty and randomness of the event.

The identification process is suggested to be done in two steps, qualitative screening and selection of dependencies. In the qualitative screening, the importance of the multi-unit dependencies relevant for identified initiators is ranked qualitatively. The dependencies are ranked in the categories ‘very important’, ‘important’, ‘less important’ and ‘insignificant’ to:

- Ensure that the dependencies that are considered likely to be relevant are captured correctly in the quantitative analysis.
- Screen out dependencies that do not require further analysis.

Table 3 summarizes the definition of the four different categories.

Table 3. Importance categories for qualitative identification.

Category	Description
Very important	Dependencies where no additional SSCs are available to cope with an initiating event, e.g. a shared water intake.
Important	Dependencies where a limited number of additional SSCs are available to cope with an initiating event, e.g. diesel generators at a site with a station blackout gas turbine system.
Less important	Dependencies where a number of additional SSCs are available to cope with an initiating event, e.g. a shared fire water system.
Insignificant	Dependencies without effect on the risk for core damage or a radioactive release, e.g. a shared domestic water system.

Dependencies ranked as 'very important' or 'important' in the qualitative analysis are expected to be relevant in the selection of dependencies for further analysis using the quantitative evaluation in the PSA model to select dependencies important from a quantitative aspect. The qualitative identification is hence a support to the selection of relevant dependencies.

In the quantitative screening, all dependencies identified as 'very important', 'important' or 'less important' are analysed with regard to representative basic event(s) to make it possible to quantitatively evaluate the dependency. This evaluation relies on using the Fussell-Vesely risk importance measure of scenarios including the representative basic events. From the Fussell-Vesely risk importance measure, which expresses the relative contribution of the events to the total risk metric, it can be concluded what the maximum contribution of the dependency could be, when a full dependency is assumed. If this result is below the screening criterion discussed in Section 3.1, the dependency can be screened out.

3.5. Data analysis

Probability parameters of the screened in multi-unit dependencies need to be estimated. They can include:

- frequencies of initiating events including partial multi-unit events,
- probabilities that specific single-unit scenarios propagate to other units,
- probabilities of common cause failures where components from multiple units fail,
- human error probabilities.

The estimation of initiating event frequency will follow the same principles as for a single unit analysis. There may be a need to specifically treat partial multi-unit events. Probabilities that specific single-unit scenarios propagate to other units is very case specific, and it will not be possible to develop a generic approach to such situations.

3.5.1 Common cause failures (CCF)

Inter-unit CCF can be defined in the same way as normal CCF, see e.g. (Wierman et al. 2007). The only difference is that components fail in multiple units instead of a single unit. Compared to CCF treatment for a SUPSA, the two additional considerations in MUPSA context are:

- Which inter-unit CCF combinations need to be considered?
- How to estimate inter-unit CCF model parameters?

The conclusion from pilot studies and a proposal of SITRON to the first question is that usually the inter-unit CCFs can be limited to the cases with a failure of *all* identical components at the site (excluding identical components that appear in different systems), e.g. all identical diesel generators. This assumption simplifies the analysis and modelling considerably. However, it may be relevant to consider some combinations of partial CCFs, which can be risk-significant, but the number of such scenarios is limited.

The second question is more difficult, since inter-unit CCF data are scarce. ICDE survey (Håkansson 2017) shows that such events have occurred, but the study does not provide support for statistical estimation. In the pilot studies, a conservative approach was followed that single-unit CCF parameters were extended a multi-unit group. For instance, U.S. CCF data includes impact vectors and alpha factors for generic 8-component groups (U.S.NRC 2016), and these data could be used to quantify a complete CCF between two identical 4-component groups.

3.5.2 Human reliability analysis (HRA)

For multi-unit risk, HRA will continue to play an important role in the analysis. A few pilot studies have been performed (Bareith et al. 2016) (Le Duy et al. 2014) or are being performed for multi-unit HRA issues (Germain et al. 2017). A number of challenging Performance Shaping Factors (PSFs) were identified in these studies, e.g. shared resources, shift control from operators in the main control room (MCR) to emergency response team, use of Severe Accident Management Guidelines (SAMGs), etc.

The technical support centre (TSC) is an organizational unit at nuclear power plants whose purpose is to support the main control room operators in emergency conditions and, in many plants, to direct operations in case of extreme events and severe accidents. The functional role and implementation of TSC should be reflected in the multi-unit HRA.

In general, HRA methodologies developed and used in internal events PSA may have to be modified for intended applications in multi-unit PSA. HRA methodologies developed for external event scenarios, if available, could be a good starting point for multi-unit issues. Multi-unit HRA will need to put more emphasis on organizational and management aspects in the analysis. These factors need to be included in not only quantification, but also task analysis and modelling.

Assuming that certain operator action and scenario has already been analysed in SUPSA, the reconsideration that is required for MUPSA consists of two questions:

- Should the performance shaping factors applied in SUPSA be revised to reflect possible additional complexity of the MUPSA scenario (not fully taken into account in the analysis made for SUPSA)?
- Should a dependency be modelled between the unit-specific actions to reflect the fact that same persons can be involved in both actions?

Two quantification approaches are proposed in SITRON method to handle the above question: 1) penalty factor method and 2) dependency approach. The penalty factor method

combines the additional PSFs as a multiplier to the original HEP based on an EDF approach developed for multi-unit PSA (Le Duy et al. 2014). The penalty factor is estimated by expert judgement based on a number of factors through a decision tree.

Penalty factor method, which assumes a conditional context independency, is an assumption that should work well for many MUPSA scenarios. A prerequisite for this is that there are no common actors for both units and that the outcome of the action (success or failure) at one unit does not change the context for the other one. If these conditions cannot be met, then there is an action dependency that should be taken into account. The purpose with the dependency approach is to capture action dependencies, i.e., the scenarios where the probability of the HFE at one unit is dependent on the value (TRUE or FALSE) of the same HFE at the other unit. Dependency approach follows the same principles as the usual operator action dependency assessment approach applied in HRA, e.g., the conditional human error probability categories suggested in THERP (Swain & Guttman 1983).

3.6. Quantification

In the pilot studies two different quantification approaches were applied. These are briefly described below and referred to as the MCS list approach and the Multi-unit event combinations approach. The methods are described in more detail in Appendix B.

3.6.1 MCS list approach

In the MCS list approach, it is assumed that MCS lists of single-unit PSAs are correct representations of the combinations basic events that lead to the top event (e.g. a core damage in level 1 PSA) for the respective unit. Correspondingly, combinations of two units cut sets must be correct cut sets for the joint top event. The only things that have to be quantified are the evaluation of the probabilities of each cut set combination and the minimization of the combined cut set list. The latter step is needed when there are full dependencies between some of the unit-specific basic events.

For the quantification, rules need to be defined how to treat combinations of minimal cut sets which include dependent basic events, and especially how to quantify the probability of such combined minimal cut set. In principle, one could consider numerous rules how to manipulate cut set combinations, in a similar way as, e.g., post-processing of cut sets could be done by PSA tools. In this case, only one kind of rule, which takes into consideration dependencies between pairs of identical basic events, has been applied.

In the developed MCS list approach, the pairs of basic events are manipulated in such a manner that the needed multi-unit risk metrics can be obtained by the usual way of quantifying any minimal cut set list, i.e., the post-processed joint minimal cut set list represents the appropriate multi-unit top event. Risk importance measures for basic events or basic event groups can be obtained in a standard way.

3.6.2 Multi-unit event combinations approach

In the multi-unit event combinations approach, for each multi-unit initiator a pre-event tree is set up. The event tree is set up for branch points for all dependencies relevant for the initiator. The sequences of the event tree correspond to multi-unit scenarios, and the frequencies of the scenarios can be calculated from the event tree.

For each sequence in the pre-event tree, each single-unit model is evaluated as conditional that the multi-unit event(s) related to the dependency(ies) occur or not to calculate conditional accident probabilities, e.g. conditional core damage probabilities. When a branch-point has been passed in the pre-event tree, there are two options:

- The event related to the dependency did occur: The frequency of the sequence in the pre-event tree is multiplied with the probability of the dependency. All sequences following should be evaluated conditionally that the event related to the dependency has occurred (when the separate PSA models are evaluated).
- The event related to the dependency did not occur: The frequency of the sequence in the pre-event tree is multiplied with the probability of success event of the dependency. The event in the PSA model for the individual unit is set conditional success of the dependency (e.g. if the multi-unit CCF did not occur, then that probability needs to be subtracted from the individual plant event probability). The treatment of success may not be needed (conservative) if the evaluation is performed manually.

Finally, the multi-unit accident frequency of each scenario can be calculated as the frequency of the scenario (calculated from the pre-event tree) multiplied by the conditional accident probabilities of the units.

The probabilities of the important operator actions relevant in the scenarios of the pre-event tree sequences might be adjusted for the conditional evaluation of the single-unit models according to the penalty factor method as described in section 3.5.2.

3.6.3 Level 2 PSA quantification considerations

Quantification in level 2 follows the same principles as in level 1 PSA. The practical performance of quantifications is dependent on the applied risk metrics. As discussed in Section 2.4 and illustrated in Figure 3, a level 2 PSA can include multiple end states of interest, i.e., multi-unit release categories. Each multi-unit release category can be associated with a quantification task combining certain accident sequences from two (or more) PSA models. Selection of relevant accident sequences is dependent on the sequence specific source terms so that the combined source term shall match with the intended release category.

One finding with the pilot studies is that the rules to combine of accident sequences for a two-unit risk analysis can be quite simple. Source term analyses made for the pilot study NPPs indicate that a sufficient and necessary condition for an unacceptable release (from the site) is that an unacceptable release occurs at one of the units. In other words, if a core damage occurs at two units but release can be limited below the criterion for an unacceptable release at both units, the joint release will not likely exceed the criterion for an unacceptable release. This fact will considerably simplify two-unit level 2 PSA quantifications, if the assessment is limited to the unacceptable release frequency only. In practice, one only needs to quantify the two-unit unacceptable release case to get the site-level frequency for an unacceptable release by the formula

$$f\left(\mathrm{TOP}^{12}(\mathrm{una})\right) = f\left(\mathrm{TOP}^{1}(\mathrm{una})\right) + f\left(\mathrm{TOP}^{2}(\mathrm{una})\right) - f\left(\mathrm{TOP}^{1}(\mathrm{una})\&\mathrm{TOP}^{2}(\mathrm{una})\right),$$

where $f(\mathrm{TOP}^1(\mathrm{una}))$ and $f(\mathrm{TOP}^2(\mathrm{una}))$ are the unacceptable release frequencies quantified by the single-unit PSA models, and $f(\mathrm{TOP}^1(\mathrm{una})\&\mathrm{TOP}^2(\mathrm{una}))$ is the frequency for the occurrence of an unacceptable release at both units.

4. Model management issues

This section is summary of the WP3 report (Appendix C). Besides general method development, procedures are needed for documenting the site PSA, managing possible modifications made to the single-unit PSA models, and managing the data and computation. Table 4 presents the main documentation and model management tasks in different analysis phases (see Section 3) and in the maintenance phase.

Table 4. Documentation and management tasks in different analysis phases.

Analysis phase	Documentation	Model and database management
Selection of analysis scope and risk metrics	Documentation of the scope and risk metrics	
Preparations before analysis	Documentation of source materials and PSA model versions	
Analysis of POS impact	Documentation of the POS analysis process and results	Insertion of POSs, POS groups and POS group combinations to the database
Identification of multi-unit initiators	Documentation of the initiator screening process and results	Insertion of multi-unit initiators to the database
Identification and selection of dependencies	Documentation of the dependency screening process and results	Insertion of dependencies to the database, screening of dependencies with the single-unit models, insertion of multi-unit basic events to the database
Analysis of source terms (level 2 only)	Documentation of the source term analysis process and results	Insertion of source terms, source term combinations and release categories to the database
Data analysis	Documentation of the data analysis process and results	Systematic analysis of those multi-unit initiators and basic events that were screened in using the database, insertion of frequencies of initiating events and probability parameters related to multi-unit basic events to the database
Quantification of multi-unit risks	Documentation of the results	Computation based on the single-unit models and database
Maintenance of site PSA	Update of relevant parts of the documentation when needed, documentation of changes	Process for updating site PSA, model configuration management, version control, verification and validation of model changes

A database system is needed to manage the analysis process. Analysis elements included in the database can be e.g. plant operating states, POS groups, POS group combinations, multi-unit initiators, partial multi-unit initiating events, multi-unit analysis cases, multi-unit dependencies, multi-unit basic events, inter-unit CCFs, multi-unit human error events, source terms, source term combinations and release categories (see Appendix C for details). The

database can be just a set of MS Excel sheets, but since many of the analysis elements are interrelated a more advanced database system could be considered. For example, a POS group combination consists of POS groups, whereas a POS group consists of single POSs. In a database, these interrelations between different analysis elements can be presented as database relationships. A database can provide several useful functionalities to manage the data, e.g., sorting and filtering of data, and links between data elements.

5. Pilot studies

5.1. Pilot study scope

This section is summary of the WP4 reports. Two Swedish pilot studies have been made, one for the Forsmark nuclear power station (Cederhorn et al. 2018, Holmberg 2018) and second for the Ringhals nuclear power station (Bäckström et al. 2018b). Forsmark pilot study is limited to reactor units 1 and 2, and the Ringhals pilot study to reactor units 3 and 4. Forsmark 1 and 2 are boiling water reactors (BWR) of Asea-Atom design and Ringhals 3 and 4 are pressurised water reactors (PWR) of Westinghouse design.

In both cases, the two units are practically identical reactors located close to each other and have several common systems and structures such as sea water intake. For both cases, there exist complete level 1 and 2 PSAs covering all initiating event categories (internal events, internal hazards, external hazards) and plant operating states (power operation, shutdown, outage, power up-rate).

5.2. Findings from the qualitative analyses

Identified dependencies in both pilot studies are very similar even though one study concerns with two BWRs and the other with two PWRs. Therefore, the discussion given below is valid for both studies.

For initiating events, both PSA-studies include a comprehensive analysis of external hazards. The list of external hazards can be directly taken as a list of potential multi-unit initiating events, including events like loss of offsite power and organic material in sea water. Assessment of propagating initiating events was left out-of-the-scope of the pilot studies, since this task would require plant visits and walk-downs. It was however identified that there are few common buildings for which fire and flooding hazards may be considered as propagating events.

Both pilot cases have almost same important system and building dependencies. Examples of important common systems are the offsite grid connections and sea water intake. There are also several less important common systems such as the fire water system, and the demineralized water system.

Since in both pilot studies the units at the site are identical, practically all CCF groups could be considered potential inter-unit CCF groups. Assessment of relevant CCF groups was limited to the example scenario, LOOP.

Both pilot studies consider a full scope of plant operating states. The average time share that the twin-units are simultaneously at-power is about 90%. Since maintenance outages are not

carried out in parallel, it can be assumed that the other possible POS-combinations include one unit being at-power and the second unit being at some shutdown state.

5.3. Results of the quantitative analyses

5.3.1 Level 1 PSA

In both PSAs, LOOP initiating events are divided into several sub-cases. In the pilot study, the multi-unit LOOP, leading to simultaneous loss of external grid for twin-units is considered. This initiating event has rather high risk importance in both PSA studies.

LOOP event has been considered for all POSs. When quantifying the time shares of POSs and risk importances of LOOP during various POSs, the result was that only both units being at-power is a significant POS combination. The reason for this is that other POSs are very short except one longer POS during maintenance outage during which the core/fuel damage risk is very low due to long time window to recover the situation. Also, the POSs immediately after and before at-power POS are from the PSA-modelling point of view very similar to the at-power scenarios. Same inter-unit dependencies are important for those POSs as for at-power POS.

Most important minimal cut sets for the multi-unit LOOP have been analysed qualitatively to group similar minimal cuts sets together and to characterize the minimal cut sets from the time window and system failures point of view. There are about ten groups of minimal cut sets that dominate the result.

In almost all cases, the core damage happens due to loss of power supply to systems required for core cooling. A common feature is that house turbine operation fails after which the safety functions are dependent on emergency diesel generator, gas turbines or mobile diesel generators. Recovery of external grid is also a possibility.

Regarding operator actions, multi-unit dependent actions are important only in later phase of scenarios and they do not have large risk importance.

The conditional probability of a double-unit core damage given one core damage was in the order of magnitude of 10% in one pilot study and 2% in the other pilot study. The difference can be explained by turbine-driven auxiliary feedwater pumps in the other case. The most important uncertainty is the assessment of the probability of the inter-unit CCF. If no inter-unit CCF is assumed, MUCDF decreases by a factor more than 100.

5.3.2 Level 2 PSA

The frequency for an unacceptable release is low for the considered initiating event already in the single-unit PSA in both pilot studies, below 1E-8/yr. Since the degree of dependencies is less in level 2 safety functions than in level 1 safety functions, the frequency for a multiple unacceptable release is very low. The conditional probability of a second unacceptable release given the first one is about a factor 10 lower than the conditional probability of a second core damage given the first one. This difference can be explained by the longer MCSs in level 2 PSA containing some more basic events, which decrease inter-unit dependencies, i.e., some more events are needed that an unacceptable release would happen.

Same basic events as in level 1 are also important in level 2 and include significant inter-unit dependencies. These include house turbine operation failures, battery CCFs, gas turbine failures and failure to recover 400 kV grid. From the site release frequency point of view, the ranking of MCSs and basic events is same in SUPSA as it would be in MUPSA.

5.4. Spent fuel pool

A common feature for Nordic nuclear power plants is that each unit has a spent fuel pool, which has a function to be a temporary storage for spent fuel elements after their being in reactor core for power production. Spent fuel pool is thus a potential source for radioactive release in case its safety functions fail.

In the multi-unit risk assessment, it is worth analysing whether there are risk-significant scenarios where dependencies between safety systems for protecting reactor core and for protecting spent fuel pool play a role. Spent fuel pool risk is typically considered as a part of the shutdown PSA, and this is also the case with the pilot study NPPs. During refuelling outage, spent fuel pool and the reactor core are interconnected, which means that same systems take care of residual heat removal. The risk for fuel damage due to loss of residual heat removal is however very low due to a long time window to warm-up and to boil the water. Besides, there are multiple means to recover residual heat removal.

Spent fuel pool risk during at-power operation mode of a unit is seldom analysed in PSA. This can be also motivated by the fact that loss of residual heat removal would be a very slowly progressing accident sequence and other possible fuel handling errors can be regarded as a group of certain individual accident scenarios which do not require similar comprehensive analysis approach as PSA for reactor accident scenarios is (and these scenarios do not have a multi-unit/source character).

Nevertheless, a possible multi-source (reactor & spent fuel) scenario is the case where, when the reactor is in at-power mode, an initiating event occurs and combined with a complete residual heat removal (e.g. loss of ultimate heat sink) leads to a core damage or even to a release from the reactor/containment. Due to system dependencies, the spent fuel pool will likely lose residual heat removal, too. Despite of the long time window to recover residual heat removal for the spent fuel pool, there can be harsh conditions to perform actions at the unit, and one might assume that the conditional probability to fail to recover spent fuel cooling is quite high. According to pilot study PSAs such scenarios, where residual heat removal is lost both for reactor core and spent fuel pool and not only a core damage occurs but also a release from the containment, are very unlikely. From the quantitative risk assessment point of view this scenario could be screened out, but it could be nevertheless worth having a strategy how pool cooling could be recovered.

6. Role of technical support centre

This section is summary of the WP5 report (Appendix D). Site-level risk analysis needs to evaluate the likelihood that actions taken by plant personnel will prevent, reduce, or delay, large radioactive releases that may follow single or multi-source severe fuel damage accidents. In these accidents, almost all safety issues are resolved through operator actions which serve as preventive measures. The Emergency Response Organization (ERO) and the Technical Support Center (TSC) have thus a crucial role.

WP5 of SITRON has studied the ERO/TSCs at Nordic nuclear power plants for identifying functional characteristics that might impact operational decisions during severe and multi-unit accidents. These include the roles, responsibilities and the allocation of accident mitigation tasks, including the criteria for activation and location of the TSCs, their interactions and communications with the main control room personnel and other plant personnel, as well as the staff competence building. Plants' self-assessed general and specific operational challenges to their TSCs/EROs in severe/multi-unit accidents are reported.

WP5 has compared how the different plants credit the TSC role in PSA for multi-unit events. The TSC is not modelled in detail as this is assumed to have a limited impact on the HRA accuracy and the PSA results. Appendix D provides a concise reference source of generic and plant-specific information related to the TSC role in responding to severe and site-level accidents, a necessary first step for including it in PSA/HRAs and, possibly, a useful complement for further progress on severe accidents preparedness.

7. Conclusions

An approach for estimating multi-unit risk has been outlined. The approach starts from the identification of multi-unit initiators and the POS combinations where the initiators may be relevant. The identification of multi-unit dependencies uses a combination of qualitative and quantitative approaches, considering dependencies relevant for the identified initiators. The qualitative identification serves as a basis for the quantitative selection, and it also assures that relevant dependencies are not overlooked due to simplifications in the existing single-unit PSA.

The quantification of site level core damage frequency is straightforward, and it can be achieved by quantifications of conditional core damage probability for each unit, considering the initiator and the dependencies. Quantification of the multi-unit risk will likely require some modification of the single-unit risk assessment to consider limitations in the availability of shared resources and impact on the human reliability assessment. One obstacle can be that relevant reliability data may lack to assess dependencies such as inter-unit common cause failures and degree of uncertainty in phenomenological events. Expert judgements need to be applied in those cases.

Results from pilot studies show that the degree of dependency is less in level 2 than in level 1. The same dependencies that are important in level 1 PSA are also important in level 2 PSA. A difference from level 1 PSA is that minimal cut sets are more complex and contain more events in level 2 PSA, which decreases the contribution from inter-unit dependencies. From the site release frequency point of view, the ranking of minimal cut sets and basic events is same in the single-unit PSA as it would be in the multi-unit PSA.

The Emergency Response Organizations and the role of the TSC in the Nordic countries NPPs differ, sometimes also reactor units within the same site have differences regarding, for instance, the location and instrumentation of the different control centers. A common trait is that at all four NPPs the ultimate decision maker is the Emergency Manager (EM), who has the responsibility for the entire site. The plants have self-assessed challenges that the TSC and the wider ERO could face in a severe/multi-unit accident. The plants generally consider the access to relevant plant information for decision making to be good. Potential improvements are spotted in more precise task definitions for the TSC and in communication and cooperation.

8. References

Bareith, A., Hollo, D., Karsa, Z., Siklossy, P., Siklossy, T. A pilot study on developing a site risk model. In Proc. of 13th International Conference on Probabilistic Safety Assessment and Management (PSAM 13), 2–7 October, 2016, Seoul, Korea. Paper A-420.

Bäckström, O., Cederhorn, E., He, X., Holmberg, J.-E., Tyrväinen, T. 2018a. SITRON — Site risk assessment developed for Nordic countries. In: Proceedings of Probabilistic Safety Assessment and Management PSAM 14, September 2018, Los Angeles, CA. Paper 179.

Bäckström, O., Häggström, A., He, X. 2018b. SITRON – Pilot study Ringhals 3&4, Report 212634-R-002, Lloyd's Register Consulting, Sundbyberg. (limited distribution)

Bäckström, O., He, X., Holmberg, J.-E., Tyrväinen, T. 2019. SITRON — WP2 — Method development. Site level risk assessment. Report 212634-R-001, Lloyd's Register Consulting, Sundbyberg.

Cederhorn, E., Holmberg, J.-E. Sunde, C. 2018. SITRON — Pilot study Forsmark 1 and 2. Report 14124_R007, Risk Pilot AB, Espoo. (limited distribution)

Germain S., Boring R., Banaseanu G., Aki, Y., Chatri, H. 2017. Multi-Unit Considerations for Human Reliability Analysis, In: Proceedings of PSAM Topical Conference on Human Reliability, Quantitative Human Factors, and Risk Management, 7–9 June 2017, Munich, Germany.

Holmberg, J.-E., Knochenhauer, M. 2007. Probabilistic Safety Goals. Phase 1 — Status and Experiences in Sweden and Finland, SKI Report 2007:06, SKI, Stockholm.

Holmberg, J.-E. 2017. SITRON — Risk metrics. Report 14124-R005, Risk Pilot AB, Espoo.

Holmberg, J.-E. 2018. SITRON — Pilot study Forsmark 1 and 2 2018. Report 14124_R010, Risk Pilot AB, Espoo. (limited distribution)

Holmberg, J.-E., Bäckström, O., Cederhorn, E., Sunde, C., Tyrväinen, T. 2018a. Site risk analysis for nuclear installations — Nordic method developments and pilot studies. In: S. Haugen et al. (eds.) Safety and Reliability – Safe Societies in a Changing World: Proceedings of ESREL 2018, June 17–21, 2018, Trondheim, Norway, Taylor & Francis Group, London, Pp. 1581−1588.

Holmberg, J.-E., Andersson, C., Authén, S., Bäckström, O., He, X., Hellström, P., Karlsson, A., Tyrväinen, T., 2018b. Nordic Pilot Studies on Site Risk Analysis (SITRON Project) — Risk Metrics Developments. In: Proceedings of the International Workshop on Status of Site Level PSA Developments organised by OECD/NEA Working group RISK, July 18–20, 2018 Munich, Germany, Paper II-8.

Hudson, D. 2018. The U.S. Nuclear Regulatory Commission's Proposed Approach to Developing an Integrated Site Probabilistic Risk Assessment (PRA) Model. In: Proceedings of the International Workshop on Status of Site Level PSA Developments organised by OECD/NEA Working group RISK, July 18–20, 2018 Munich, Germany, Paper II-2.

Håkansson, M. 2017. Action item 43-09 (42-05, 41-04, 40-16): Summary of workshops on Multi-unit events. ICDE Work note. Draft 2017-03-10 (limited distribution).

Le Duy, T.D., Vasseur, D., Serdet, E. 2014. Multi Units Probabilistic Safety Assessment: Methodological elements suggested by EDF R&D. Probabilistic Safety Assessment and Management PSAM 12, June 2014, Honolulu, Hawaii.

Massaiu, S. 2019. Decision-making during severe and multi-unit accidents: Technical Support Centers and Emergency Response Organizations at Nordic Countries, IFE/F-2018/189, Institute for Energy Technology, Halden.

Muhlheim, M. D., Wood R. T. 2007. Design Strategies and Evaluation for Sharing Systems at Multi Unit Plants Phase I. ORNL/LTR/INERI-BRAZIL/06-01, Oak Ridge National Laboratory.

OECD/NEA. 2009. Probabilistic Risk Criteria and Safety Goals, NEA/CSNI/R(2009)16, OECD/NEA, Paris.

OECD/NEA. 2012. Use and development of probabilistic safety assessment, An overview of the situation at the end of 2010. NEA/CSNI/R(2012)11, OECD/NEA, Paris.

Schroer, S., Modarres, M. 2013. An Event Classification Schema for Evaluating Site Risk in a Multi-Unit Nuclear Power Plant Probabilistic Risk Assessment, Reliability Engineering and System Safety 117, 40–51.

STUK. 2013. Probabilistic risk assessment and risk management of a nuclear power plant, Guide YVL A.7, Radiation and Nuclear Safety Authority in Finland, Helsinki.

Tyrväinen, T., Björkman K. 2019. SITRON — Site PSA model management, VTT-R-06885-18, VTT, Espoo.

U.S.NRC. 1986. Safety Goals for the Operations of Nuclear Power Plants; Policy Statement. (51 FR 28044; August 4, 1986 as corrected and republished at 51 FR 30028; August 21, 1986), U.S. Nuclear Regulatory Commission.

U.S.NRC. 2016. CCF Parameter Estimations, 2015 Update, http://nrcoe.inel.gov/resultsdb/ParamEstSpar/.

Wierman, T.E., Rasmuson, D.M., Mosleh, A. 2007. Common-cause failure database and analysis system: Event data collection, classification, and coding, NUREG/CR-6268, Rev. 1 INL/EXT-07-12969, U.S. Nuclear regulatory commission, Division of risk assessment and special projects, Washington D.C., USA.

Bibliographic Data Sheet **NKS-419**

Title	Site risk analysis for nuclear installations
Author(s)	Jan-Erik Holmberg[1], Stefan Authén[1], Kim Björkman[3], Ola Bäckström[2], Xuhong He[2], Salvatore Massaiu[4], Tero Tyrväinen[3]
Affiliation(s)	[1]Risk Pilot AB, [2]Lloyds Register Consulting – Energy AB, [3]VTT Technical Research Centre of Finland Ltd, [4]IFE (Institute for Energy Technology)
ISBN	978-87-7893-508-3
Date	February 2019
Project	NKS-R/SITRON
No. of pages	26 + appendices
No. of tables	4
No. of illustrations	4
No. of references	24

Abstract
max. 2000 characters

Currently, multi-unit risks have not typically been adequately accounted for in risk assessments, since the licensing is based on unit-specific probabilistic safety assessment (PSA) with focus on a reactor accident. NKS-R project SITRON (SITe Risk Of Nuclear installations) has searched for practical approaches for Nordic utilities to assess the site level risk. Starting point of SITRON work has been the fact that the Nordic utilities already have good unit-specific PSAs. Therefore, the question is what additional efforts are needed to obtain a site level risk assessment. Practically, it means two tasks: 1) to identify relevant inter-unit dependences, and 2) to quantify the site level risk. Inter-unit dependences consist of multi-unit initiating events, shared systems, structures and components, dependences in human actions, inter-unit common cause failures, and plant operating state combinations. SITRON provides guidance how to perform the identification of dependences and how to select relevant dependences for quantification (screening). Quantification of site risk can be performed quite straightforwardly, given that the quality of the single-unit PSAs is sufficient.

SITRON project has also included a survey on the role of Emergency Response Organisation (ERO), often referred to as the Technical Support Centre (TSC) in accident management. Based on responses from four plants in Finland and Sweden, SITRON has investigated different implementations of EROs with respect to possible impact on operational decisions in severe accident and multi-unit scenarios. The human role in severe accidents differs markedly: new decision makers (ERO and TSC rather than main control room);

different instructions (guidelines rather than procedures); different decisions (involving trade-offs, novel actions, and strategies contrary to conventional knowledge); inter-unit influences; unreliability of instrumentation; and long time windows for actions.

Key words Probabilistic safety assessment, nuclear power plant, site risk, multi-unit risk, technical support centre

Appendix A – WP1 Risk Metrics

Holmberg, J.-E. 2017. SITRON — Risk metrics. Report 14124-R005, Risk Pilot AB, Espoo.

Type of Document REPORT			Page 1 (15)
Date 2017-12-16	Doc. No. 14124_R005		Rev. No. U001

Author Jan-Erik Holmberg	Phone	No of Attachments —	Replaces Doc. No.
	Reviewed by Anna Häggström, Tero Tyrväinen	Approved by Jonas Sevrell	
Distribution to SAFIR RG2, FKA/Anders Karlsson, Julia Ljungbjörk RAB/Stefan Eriksson, Cilla Andersson SSM/Per Hellström Lloyds Register/Anna Häggström VTT/Tero Tyrväinen	Used Software MS Word		
	Path		
Title **SITRON — Risk metrics**			Saved 2017-12-18 07:58:00

Summary

Risk metric is a concept quantified by a risk model such as probabilistic safety assessment (PSA) for nuclear power plants (NPP). In the nuclear safety context, most regulators have defined numerical risk criteria based on core damage frequency and large release frequency risk metrics, and these are applied e.g. in the licensing of NPPs. These risk criteria are applied per reactor or facility, with few national exceptions. It is thus internationally an open issue, which risk metrics and possibly even risk criteria should be considered at the site level. There are several international efforts where site level risk metrics are discussed, but no consensus has been reached, yet.

This report proposes risk metrics for site level risk studies. The risk metrics are divided into two groups: one group of risk metrics for a single-unit PSA, which even accounts for multi-unit scenarios, and a second group for a site PSA.

The risk metrics for a single-unit PSA are rather conventional. A possible extension to current practices is to consider risk metrics that aggregate all fuel locations at the facility, i.e., to account for both fuel accidents in the reactor and in the fuel pool.

The risk metrics for a site PSA are complementary to the single-unit PSA risk metrics. Site fuel damage frequency (for level 1 PSA) and site release category frequency (for level 2 PSA) represent a frequency of a fuel damage accident corresponding to an external release from any fuel location at the site. In addition, a multi-unit CDF can be defined for level 1 PSA. At level 2 PSA, the amount of released radionuclides is the most important quantity, not from how many units it is released. Therefore, there is no need to define a "multi-unit release frequency".

Address:
Risk Pilot AB Suomen sivuliike
P.O.Box 72
02101 Espoo, Finland

Business ID:
2603561-5

Phone:
+358-40-827 6656
Fax:
+46-(0)8-652 84 50

E-post:
info@riskpilot.se
Home page:
www.riskpilot.fi

Table of Contents

Abbreviations

Acronym	Description
BWR	Boiling water reactor
CD	Core damage
CDF	Core damage frequency
CSNI	Committee on the Safety of Nuclear Installations (OECD/NEA)
FDF	Fuel damage frequency
IAEA	International Atomic Energy Agency
IE	Initiating event
LERF	Large early release frequency
LRF	Large release frequency
MUCDF	Multi-unit core damage frequency
MUIE	Multi-unit initiating event
MULERF	Multi-unit large early release frequency
MUPDS	Multi-unit plant damage state
NEA	OECD Nuclear Energy Agency
NPP	Nuclear power plant
NRC	U.S. Nuclear Regulatory Commission
OECD	Organisation for Economic Co-operation and Development
PDS	Plant damage state
PSA	Probabilistic safety assessment
RC	Release category
RCF	Release category frequency
SAFIR	Finnish Research Programme on Nuclear Power Plant Safety
SAP	Safety Assessment Principles (UK)
SCDF	Site core damage frequency
SRCF	Site release category frequency
SSM	Strålsäkerhetsmyndigheten, Swedish Radiation Safety Authority
SUIE	Single-unit initiating event
SUPDS	Single-unit plant damage state
STUK	Säteilyturvakeskus, Radiation and Nuclear Safety Authority
SUCDF	Single-unit core damage frequency
VTT	Technical Research Centre of Finland
WGRISK	OECD/NEA CSNI Working Group on Risk Assessment
YVL	Ydinvoimalaitos (nuclear power plant), STUK’s regulatory guide series for nuclear facilities

Acknowledgements

The work has been financed by SAFIR2018 (The Finnish Research Programme on Nuclear Power Plant Safety 2015–2018), Forsmark Kraftgrupp AB, Ringhals AB and Swedish Radiation Safety Authority (SSM).

1 Introduction

Currently, multi-unit risks have not typically been adequately accounted for in risk assessments. A site-level probabilistic safety assessment (PSA) is an extension of unit-specific PSAs aiming at a more comprehensive analysis of single-unit and multi-unit scenarios. From the risk metrics point of view, a site level PSA means two questions:

- Do we need to reconsider risk metrics for a single-unit PSA?
- What type of risk metrics, if needed, should be applied at the site level?

This report will address both questions. Basic definitions for multi-unit risk metrics are given in the 2016 study report (Tyrväinen et al. 2017). This report complements the 2016 report by an overview of internationally applied risk criteria for site risk, also taken into consideration non-reactor release sources, too. Proposals for risk metrics for site-level PSA applications will be made, but the question of suitable risk criteria, i.e., the levels for acceptable risk at the site level, is left open.

According to the objectives with this project, the main purpose with the site level PSA is to improve unit-specific risk analyses. Therefore, single-unit risk metrics have the priority in the discussion. The site level risk metrics can be considered additional metrics whose usage depends on the purpose, scope and method of the site level PSA.

Risk metrics are mainly discussed from the level 1 and 2 PSA point of view (core/fuel damage risk and large release risk), since these are the current levels of PSA for Nordic PSAs.

2 Definitions

Safety goals are definitions for acceptable risk. Safety goals answer to the question: "how safe is safe enough?". Safety goals provide a measure of sufficiency of safety provisions embedded in the design of a nuclear installation and its operational process.

Safety goals can be defined at various levels beginning from the society level, site level, facility level, and system level. Safety goals can be also formulated qualitatively or quantitatively. Qualitative goals can be e.g. high-level safety objectives "Measures for controlling radiation risks must ensure that no individual bears an unacceptable risk of harm", but also defence-in-depth requirements and safety margin requirements can be understood as safety goals.

This report focuses mainly on quantitative safety goals, which are often called probabilistic safety goals or risk criteria such as core damage frequency criterion and large release frequency criterion.

Risk criteria generally refer to any quantitative decision-making criterion used when results of risk assessment are applied to support decision making. In this context, the discussion is limited to risk criteria defining goals or limits for acceptable risk. Various types of criteria can be used, such as: absolute criteria, relative criteria, differential criteria and trade-off criteria. Risk criteria are always associated with a corresponding risk metric.

Risk measure and risk metrics are two concepts used in the presentation and interpretation of results from a risk assessment. The risk measure is an operation for assigning a number to something, and the risk metrics is our interpretation of the assigned number. In the PSA context, the various numeric results obtained from the quantification of the model are risk measures. The interpretations of these numbers as core damage risk, plant risk profile, safety margin, etc., are risk metrics.

In level 1 PSA, the main risk metric is core damage frequency (CDF), which is usually integrated into a single number: The annual core damage frequency representing an average configuration of the reactor over all plant operating states. Meaning of a core damage may slightly vary as well as the scope of the studies can vary. See (OECD/NEA 2009) for examples.

Level 1 PSA for a reactor may include accident scenarios for the fuel pool, e.g., accidents that can happen during refuelling outage. As a distinction to a core damage, these accidents can be called fuel damages and the risk metric is then the fuel damage frequency (FDF). The fuel damage frequency can be used as a generalisation of the core damage frequency for both reactor and non-reactor facilities.

In level 2 PSA, multiple risk metrics are usually applied to categorise various releases. Large release frequency (LRF) is the annual frequency of an event leading to a radioactive release above a certain criterion, typically defined in a regulatory framework, e.g., 100 TBq of Cs-137 in Finland (STUK 2013).

Large early release frequency (LERF) is a subcategory of LRF considering releases which occur before sufficient time for offsite protective measures.

In Swedish level 2 PSAs, four groups of release categories are used:

- Acceptable release, which is a release less than 0.1 % of the core inventory of Cs-134 or Cs-137 from an 1800 MWt BWR (Barsebäck 1 unit). This is so called "RAMA" criterion defined in 1980's when the decision was made to implement severe accident mitigation systems for the NPPs.
- Unacceptable release, which is a release above the RAMA criterion.
- Large release, which is a release of more than 10% of volatile fission products of the core inventory. 10% criterion has been adopted from IAEA guidelines (IAEA 1995).
- Large early release, which is a large release occurring prior to effective evacuation of the close-in population such that there is a potential for early health effects (U.S.NRC 2011).

Since the meaning of term "large release" is dependent on the national practice, it is not used hereinafter in this report (except when referring to a specific reference). Instead of that, a neutral term "release category frequency" (RCF) will be applied so that RCF is the frequency of accident involving a release that belongs to a certain category.

A "single-unit PSA" means a PSA made for a nuclear facility such as the reactor facility and the interim storage for spent fuel. A "single-unit PSA" is assumed to cover all fuel locations within the facility. For a reactor facility, the reactor and the fuel pool are the relevant locations from the risk assessment point of view. In practice, a single-unit PSA can be split into fuel location specific studies.

A "site level PSA" means a PSA or a set of PSAs made to cover accident scenarios related to all fuel locations at the site, including spent fuel transportations.

3 International safety goals and risk criteria

3.1 Status of safety goals and risk criteria

Most countries apply CDF and LRF/LERF based risk criteria in the regulatory context. These are used as surrogates to higher, society level safety goals and they are applied per reactor (or facility). Comprehensive descriptions of nuclear risk criteria can be found in (Holmberg & Knochenhauer 2007), (OECD/NEA 2009), and (OECD/NEA 2012).

In UK and Canada, site level risk criteria have been defined for level 3 PSA. In Canada, site-based safety goals are under development. In UK, the Safety Assessment Principles (SAPs) have been clearly stated for multi-unit sites.

U.S.NRC (1986) Safety Goal Policy Statement, establishes two quantitative objectives that were to be used to determine achievement of the site-level qualitative safety goals:

- The risk to an average individual in the vicinity of a nuclear power plant of prompt fatalities that might result from reactor accidents should not exceed one-tenth of one percent (0.1%) of the sum of prompt fatality risks resulting from other accidents to which members of the U.S. population are generally exposed.
- The risk to the population in the area near a nuclear power plant of cancer fatalities that might result from nuclear power plant operation should not exceed one-tenth of one percent (0.1%) of the sum of cancer fatality risks resulting from all other causes.

However, when the aggregate risk criteria based on CDF and LERF risk metrics are used, they are used reactor-specific.

In Finland, STUK's PSA guide YVL A.7 defines target values for a reactor, both for level 1 and 2 PSA to be applied in construction as well as operating license application phase (STUK 2013). The Finnish large release criterion is defined to "take into account all of the nuclear fuel located at the plant unit. A spent nuclear fuel storage external to the plant unit is considered a separate nuclear facility for whose analysis the aforementioned criteria apply."

In Sweden, the SSM regulation does not specify numerical risk criteria. The utilities have defined target values for level 1 and 2 PSA (Holmberg & Knochenhauer 2007).

3.2 Multi-unit discussions

International interest in multi-unit PSA and risk metrics has increased, especially after Fukushima Daiichi accident. Multi-unit PSA has been a main subject at many international conferences, e.g., PSAM13 in Seoul 2016 and ANS PSA 2017 in Pittsburgh. Several proposals have been made and method development is going on in several contexts, such as by IAEA, OECD/NEA and Euratom. There is no consensus yet on which approaches and risk metrics should be adopted.

At the time point of preparing this report (2017), the IAEA and OECD/NEA activities have just been initiated and there are no publications available from those efforts. The Euratom project ASAMPSA_E (Advanced Safety Assessment Methodologies: extended PSA) has published a report on risk metrics (Wielenberger et al. 2016), which also includes a section on site level risk metrics.

As a pre-activity, an international workshop was arranged in 2014 (CSNC 2014). The workshop concluded that the main technical issues and challenges related to site-based safety goals were:

- Current risk acceptance and risk significance criteria largely based on reactor-based risk metrics such as CDF and LERF.
- Method of aggregating risk contributions across different reactor units and facilities, single- and multi-unit and facility accidents, hazard groups and operating states with due regard to differences in level of realism/conservatism, level of detail in modelling, and uncertainty treatment.
- Methods for comparing calculated risks against existing and new site-based safety goals.
- Question of whether safety goals should be quantitative or qualitative, supported by quantitative safety design objectives.
- Lack of multi-unit site-based acceptance criteria for evaluating the integrated risks from a multi-unit site PSA.
- Need for more international consensus on approach to safety goals and use of such goals to interpret PSA results.
- Difficulty in communicating risk information from piecemeal risk studies to assure that safety goals have been achieved.

3.3 SAFIR-2016 summary

This section summarizes the definitions for risk metrics presented in (Tyrväinen et al. 2017).

As an example, a site with three reactors is discussed from the core damage risk point of view (level 1 PSA). Combinatorially, there are six different core damage scenarios for a three-unit site, as demonstrated in Figure 1.

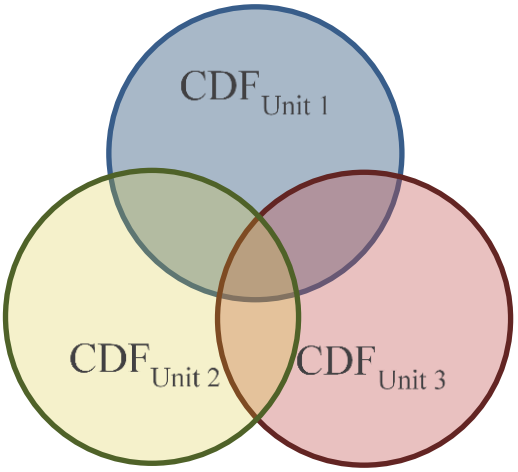


Figure 1. Diagram of possible core damage combinations for a three-unit-site.

In a site PSA, the following CDF metrics can be considered:

- Single-Unit Core Damage Frequency (SUCDF) – frequency of a reactor accident involving core damage on one and only one reactor unit per site calendar-year.
- Multi-Unit Core Damage Frequency (MUCDF) – frequency of an accident involving core damage on two or more reactor units concurrently per site calendar-year
- Site Core Damage Frequency (SCDF) – frequency of a reactor accident involving core damage on one or more reactor units concurrently per site calendar-year.

Tyrväinen et al. (2017) point out that SUCDF is not the same as a specific unit's CDF. CDF normally reflects the estimated frequency of core damage per reactor-calendar-year associated with a particular unit on the site. SUCDF is the sum of all CDFs involving single core damage.

In Figure 2, SUCDF and MUCDF are separated to highlight the contributions to SCDF from single and multi-reactor accidents. The sum of the core damage frequencies from all contributions, measured on a frequency per site year basis, is the SCDF.

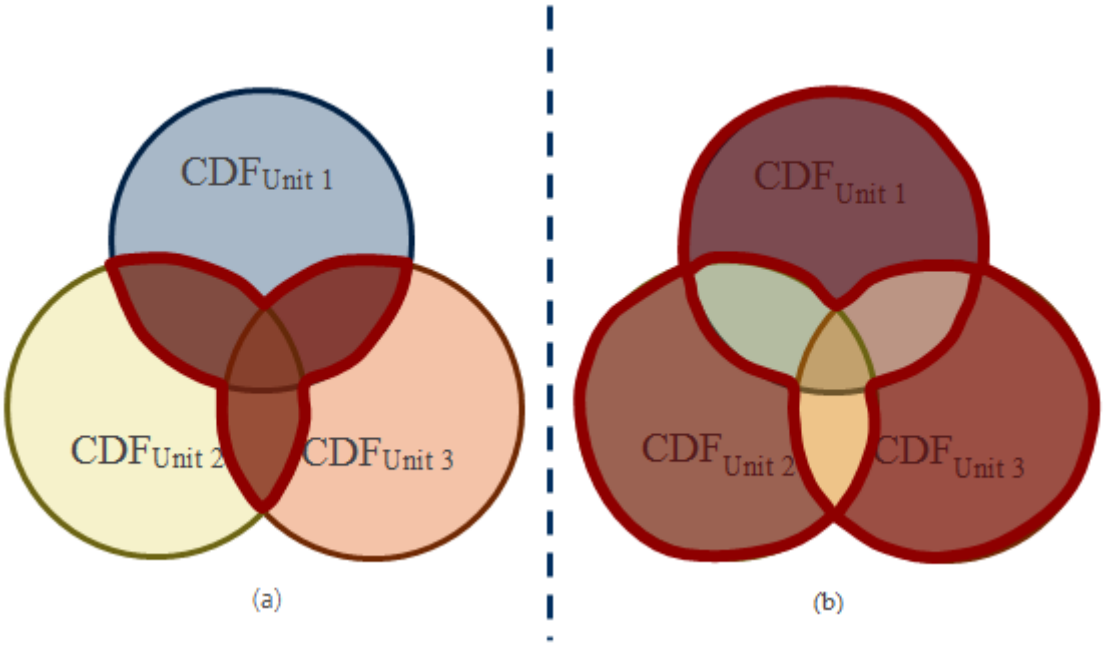


Figure 2. (a) The red shaded area represents multi-unit CDF (MUCDF). (b) Area representing single-unit CDF (SUCDF).

Proposals for the release frequency metrics for multi-unit PSA were taken from (Samaddar et al. 2014) as follows:

- Site Large Early Release Frequency (SLERF) – frequency of a large early release from an accident involving one or more reactor units simultaneously per site calendar year.
- Site Release Category Frequency (SRCF) – the frequency per site-calendar-year of each distinct release category for a multi-unit level 2 PSA. These release categories include the release categories already defined in the single unit level 2 PSA for each unit, for releases from a single reactor unit, as well as categories for accidents involving multiple units.

Tyrväinen et al. (2017) discusses that the SLERF may involve single reactor accident sequences with releases from a single unit as well as releases from multiple reactor accidents that combine to meet these same criteria. For the large release, there is hence no meaning in splitting up large releases from one or several reactor units, a large release is large irrespective of the number of sources. For a full scope level 2 site PSA, the SRCF can be used.

In the methodology outlined by Tyrväinen et al. (2017), MUCDF was used as the main risk metric for level 1 because the main objective was to identify the most important multi-unit dependencies with limited resources for the analysis. In addition, the risk metric multi-unit large early release frequency (MULERF) was defined for level 2. The MULERF is just a part of the total large early release frequency from a site, but it is used here to capture dependencies that can lead to large early releases from more than one unit concurrently.

4 Proposal for risk metrics for site level risk assessments

4.1 Risk metrics for a single-unit PSA

Risk metrics for a single-unit PSA can be basically defined as before. An important issue is in which manner the fuel pool related (and possibly some other release sources in the same reactor unit) accident scenarios should be treated. The situation is in principle same as depicted in Figures 1 and 2 with the interpretation that each "unit" can be interpreted as a release source, e.g., the fuel in the reactor core, the fuel in the fuel pool, etc. Therefore, fuel damage and release category related risk metrics can be firstly defined and quantified separately for each activity source. Obviously, some accident scenarios may concern multiple sources. Secondly integrated risk metrics can be defined for the whole reactor unit. This is e.g. the interpretation given in STUK's YVL guide for the release metrics.

One group of interesting risk metrics could be the relative contribution of multi-unit scenarios to unit specific CDF. Provided a proper site level PSA, it should be straight-forward to quantify relative contributions of multi-unit scenarios.

Table 1 summarizes the proposed risk metrics for a single-unit PSA. In addition to these metrics, risk importance measures such as Fussell-Vesely importance measure and risk increase factors should be utilized to support the presentation and interpretation of the results.

Table 1. Proposed risk metrics for a single-unit PSA.

Risk metric
1. CDF/FDF per fuel location (core, pool, etc.)
2. RCF per fuel location (core, pool, etc.). This risk metric can cover one or more "release frequencies" corresponding with the defined release categories.
3. Integrated FDF for the reactor unit (all fuel locations)
4. Integrated RCF for the reactor unit (all fuel locations). This risk metric can cover one or more "release frequencies" corresponding with the defined release categories.

4.2 Risk metrics for a site PSA

As discussed in Section 3.3, there are several options for site level risk metrics, i.e., metrics for various double, triple, quadruple combinations of units (fuel locations) at the site. When accounting for combinations, it is important to notice that there is a principal difference between level 1 risk metrics and level 2 risk metrics. The level 1 risk metrics are based on binary conditions (fuel damage happens vs. does not happen), while level 2 risk metrics is derived by partitioning a "continuous" property (magnitude and timing of release) into a limited number of classes by threshold values. Thus, the level 1 risk metrics are derived by counting the number of affected units but level 2 risk metrics it is determined by the release magnitudes regardless of number of affected units. Therefore, the level 1 and 2 risk metrics are discussed separately below.

4.2.1 Level 1 PSA

Figure 3 presents the link between site risk metrics and site risk accident sequences. The example represents two-unit site and is limited to level 1 PSA accident sequences.

The idea is that accident sequences can be grouped into sequences related to a single-unit (unit 1 or 2 in Figure 3) and sequences related to multiple units. Those affecting multiple units are caused by multi-unit initiating events, which IE category also includes single-unit event propagating to other units.

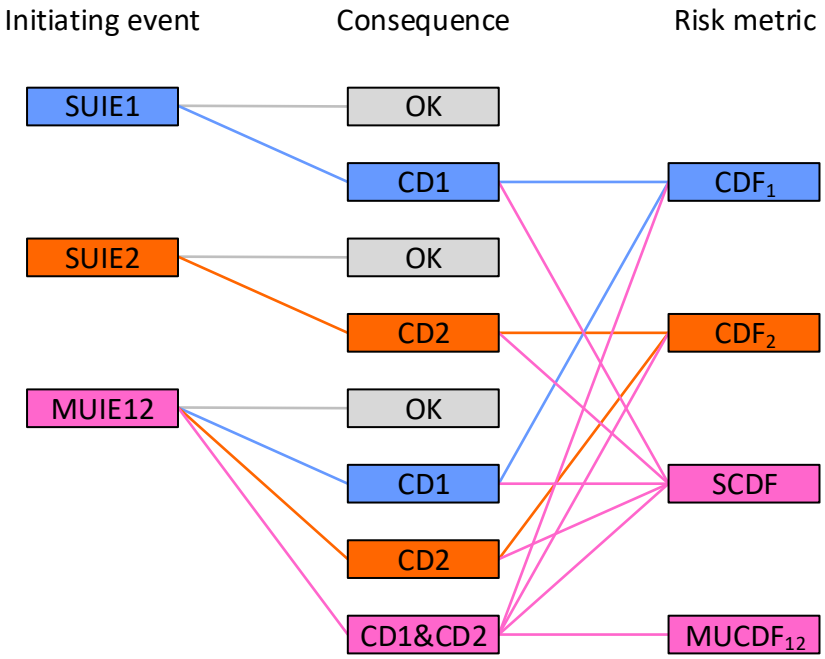


Figure 3. Link between site risk accident sequences and site risk metric.

Accident end states can be defined accordingly depending on which unit is damaged or if several units are damaged ("CD1", "CD2" or "CD1&CD2" in Figure 3). Risk metrics are obtained by summing the frequencies of the corresponding sequences of Figure 3. Summing provides correct frequencies since the accident sequences are exclusive.

The blue respectively red risk metrics should be obtained by a single-unit PSA-model, if properly modelled and quantified. The pink risk metrics cannot be directly obtained from a single-unit PSA, but some further elaboration is needed or a development of a site PSA-model. This will be further discussed in the SITRON methods report (Häggström et al. 2017).

In case of more than two units, the number of combinations increases. The meaning of MUCDF must be then specified whether a particular combination or e.g. "full disaster" at the site is considered. This issue is left open here, since it depends on the intended application of such risk metrics, which is out of the scope of this report.

4.2.2 Level 2 PSA risk metrics

As pointed out in the introduction of section 4.2, the risk metrics for level 2 PSA are principally different from level 1 risk metrics due to the release magnitude and timing component of the metrics. Figure 4 depicts a schematic level 2 PSA model for a site risk analysis, starting from the end states of site level 1 PSA. For the accident sequences where only one unit has a fuel damage, plant damage state categorisation and subsequent level 2 PSA modelling and quantification follows the basic principles for a single-unit level 2 PSA.

The bottom accident sequence of Figure 3, where more than one unit experiences a fuel damage, may require a special treatment. This is indicated by the plant damage state categorisation (MUPDS1, ..., MUPDSm), which may be different from a single-unit PSA categorisation (SUPDSx-1, ..., SUPDSx-n, x = 1, 2 (the damaged unit)).

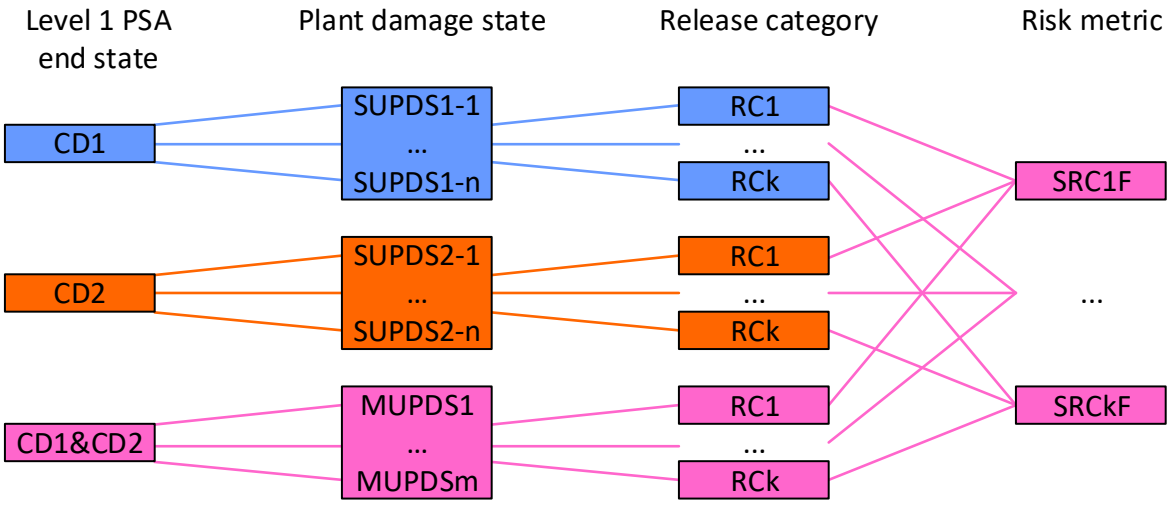


Figure 4. Event sequences and associated release category risk metrics for a level 2 PSA for a two-unit-site.

Release categorisation (RC1, ..., RCn) depends on the national practice. As an example, a release categorisation similar to the Swedish praxis is assumed here:

- RC1 "Acceptable release": A release less than the criterion for unacceptable release
- RC2 "Unacceptable, small release": A release more than the criterion for unacceptable release but less than the criterion for large release
- RC3 "Large, late release" A release larger than the criterion for large release. Sufficient time for evacuation exists.
- RC4 "Large, early release": A release more than the criterion for large release, occurring prior to effective evacuation of the close-in population such that there is a potential for early health effects

The example release categorisation is also illustrated in Figure 5. The release category is determined by two parameters: 1) magnitude of the release, and 2) timing of the release. For simplicity, it is assumed that the magnitude of the release is determined by the magnitude of released Cs-137 from the fuel inventory and timing is determined by the start point of the release (e.g. when the limit for unacceptable release is exceeded). One should note in multi-unit applications, it may be advisable to define release magnitude criterion in absolute units (e.g. TBq of released Cs-137) than in relative terms (e.g. x% of core inventory).

In a single-unit PSA, the release category is determined by the source term associated with the accident sequence. Sum of frequencies of level 2 PSA accident sequences belonging to a certain category yields the corresponding RCF.

In the multi-unit PSA, the release category is determined by the aggregated source term associated with the accident sequence. In case of releases from multiple sources, the size of the release is the sum of sizes of the individual releases. The timing point could be the time point when the release criterion is exceeded.

It should be noted that one consequence of the above approach is that there may be accident sequences which are acceptable (RC1) from the single-unit point of view but are unacceptable (RC2) from the multi-unit point of view.

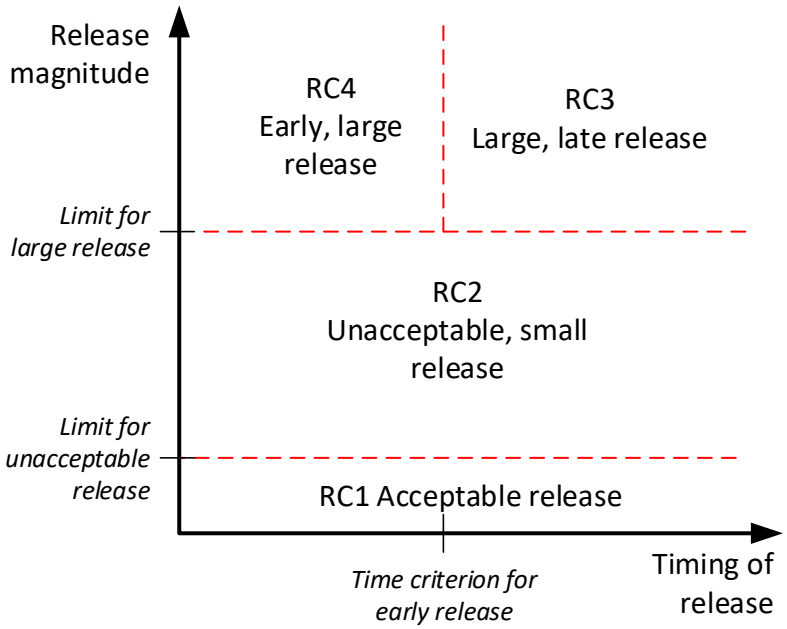


Figure 5. Release categorisation example.

4.2.3 Calculcation of site level risk metrics

Accurate calculation of the multi-unit risk metrics can be a tedious task. Examples of theoretical discussion of multi-unit risk metrics and their quantification can be found e.g. in (Modarres et al. 2017) and (Tyrväinen et al. 2017). The approach proposed here and further discussed in the SITRON methods report (Häggström et al. 2017) assumes that practical MCS quantifications are done by single-unit PSA models. Multi-unit risk metrics can be obtained by post-processing the single-unit results using some simple spreadsheet application. See SITRON methods report for further discussion.

4.2.4 Summary

Table 2 summarizes the proposed risk metrics for a site PSA. These risk metrics should be seen complementary to the single-unit risk metrics presented in Table 1.

Table 2. Proposed risk metrics for a site PSA.

Risk metric
1. Site core/fuel damage frequency
2. Multi-unit core/fuel damage frequency. This risk metric needs to specify whether particular combinations or "full disaster" at the site are considered.
3. Site release category frequency. This risk metric can cover one or more "release frequencies" corresponding with the defined release categories. The same release categories can be applied to single-unit and multi-unit scenarios. In multi-unit release scenarios, the categorisation of releases is based on the aggregated source term, i.e., the magnitude of the release is the sum of releases and timing of the release could be determined by the time point exceeding the release category limit.

5 Conclusions

Risk metric is a concept quantified by a risk model such as PSA for NPPs. For level 1 PSA, the main risk metrics is the core damage frequency (CDF) or fuel damage frequency when other fuel locations than the reactor core are considered. For level 2 PSA, there are usually more than one release category frequency used for the presentation and interpretation of results, such as LRF, LERF and the unacceptable release frequency.

In the nuclear safety context, most regulators have defined numerical risk criteria based on these risk metrics, and these are applied e.g. in the licensing of NPPs. These risk criteria are only defined and applied per reactor or facility, with few exceptions. It is thus still internationally an open issue, which risk metrics and possibly even risk criteria should be considered at site level. There are several international efforts (Euratom, IAEA, OECD/NEA) where site level risk metrics are discussed, but no consensus has yet been reached.

This report proposes several risk metrics for site level risk study purposes. The risk metrics are divided into two groups: one group of risk metrics for a single-unit PSA, which even accounts for multi-unit scenarios, a second group for a site PSA.

The risk metrics for a single-unit PSA are rather conventional. One possible extension to current practices is to consider risk metrics that aggregate all fuel locations at the facility, i.e., to account for both fuel accidents in the reactor core and in the fuel pool.

The risk metrics for a site PSA are complementary to the single-unit PSA risk metrics. Site CDF/FDF and site RCF represent frequency of a fuel damage accident corresponding to an external release from any fuel location at the site. In addition, a multi-unit CDF can be defined for level 1 PSA. For a level 2 PSA, the total magnitude of released radionuclides is the most important quantity, not the number of units and sources that contribute to the release. There is therefore no need to define a "multi-unit release frequency".

6 References

CSNC. 2014. Summary Report of the International Workshop on Multi-Unit Probabilistic Safety Assessment, Ottawa, Ontario, Canada, November 17–20, 2014, CNSC E-doc reference #4704298, Canadian Nuclear Safety Commission.

Holmberg, J.-E., Knochenhauer, M. Probabilistic Safety Goals. Phase 1 — Status and Experiences in Sweden and Finland, SKI Report 2007:06, SKI, 2007.

Häggström, A., et. al. 2017. SITRON — WP2 — Method development. Site level risk assessment. Report 212634-R-001, Lloyd's Register, Sundbyberg. Draft under preparation.

IAEA. 1995. Procedures for Conducting Probabilistic Safety Assessment of Nuclear Power Plants (Level 2) – Accident Progression, Containment Analysis and Estimation of Accident Source Terms, IAEA Safety Series No. 50-P-8.

Modarres, M., Zhou, T., Massoud, M. 2017. Advances in multi-unit nuclear power plant probabilistic risk assessment, Reliability Engineering and System Safety 157, 87–100.

OECD/NEA. 2009. Probabilistic Risk Criteria and Safety Goals, NEA/CSNI/R(2009)16, OECD/NEA, Paris.

OECD/NEA. 2012. Use and development of probabilistic safety assessment, An overview of the situation at the end of 2010. NEA/CSNI/R(2012)11, OECD/NEA, Paris.

Samaddar, S., Hibino, K., Coman, O. 2014. Technical Approach for Safety Assessment of Multi-Unit NPP Sites Subject to External Events, In Proceedings of Probabilistic Safety Assessment and Management (PSAM 12), Honolulu, HI, 2014.

STUK. 2013. Probabilistic risk assessment and risk management of a nuclear power plant, Guide YVL A.7, Radiation and Nuclear Safety Authority in Finland, Helsinki.

Tyrväinen, T., Häggström, A., Bäckström, O., Björkman, K. 2017. A methodology for preliminary probabilistic multi-unit risk assessment, VTT-R-00086-17, VTT Technical Research Centre of Finland Ltd, Espoo.

U.S.NRC. 1986. Safety Goals for the Operations of Nuclear Power Plants; Policy Statement. (51 FR 28044; August 4, 1986 as corrected and republished at 51 FR 30028; August 21, 1986), U.S. Nuclear Regulatory Commission.

U.S.NRC. 2011. Regulatory Guide 1.174, Revision 2, An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Licensing Basis, U.S. Nuclear Regulatory Commission.

Wielenberg, A., Hasnaoui, C., Burgazzi, L., Cazzoli, E., Jan, P., La Rovere, S., Löffler, H., Siklóssy, T., Vitazkova, J., Raimond, E. 2016. Risk Metrics and Measures for an Extended PSA. Technical report ASAMPSA_E/ WP 30 / D30.7 / 2017-31 volume 3, IRSN-PSN-RES/ SAG/2017-0018.

Appendix B – WP2 Method development

Bäckström, O., He, X., Holmberg, J.-E., Tyrväinen, T. 2019. SITRON — WP2 — Method development. Site level risk assessment. Report 212634-R-001, Lloyd's Register Consulting, Sundbyberg.

Lloyd's Register

Working together
for a safer world

SITRON - Method development

Site risk assessment of nuclear installations

Report for:
FKA, RAB, SSM, and SAFIR

Report no: 212634-R-001 Rev: V 2.0

Date: 18 January 2019

Summary

SITRON - Method development

Site risk assessment of nuclear installations

Security classification of this report: Open distribution

Report no:	**Revision:**	**Report date:**
212634-R-001	V 2.0	18 January 2019

Prepared by:	**Reviewed by:**	**Approved by:**
Ola Bäckström Xuhong He Jan-Erik Holmberg/Risk Pilot Tero Tyrväinen/VTT	Project Team/NPSAG	Ola Bäckström

Entity name and address:	**Client name and address:**
Lloyd's Register Consulting - Energy AB P.O. Box 1288 SE-172 25 SUNDBYBERG Sweden	FKA, RAB, SSM, and SAFIR

Our contact:	**Client contact:**
Ola Bäckström	
T: +46 (0)70 742 13 93	T:
E: ola.backstrom@lr.org	E:

Document history

Revision	Date	Description/changes	Changes made by
1.0	23-01-2018	With focus on level 1 PSA. Reviewed by NPSAG	OBA, etc.
2.0	18-01-2019	With focus on both level 1 and level 2 PSA. Also includes a discussion on fuel pool. Reviewed by NPSAG	OBA, etc.

Glossary/abbreviations

Acronym	Description
BWR	Boiling Water Reactor
CD	Core Damage
CDF	Core Damage Frequency
CSNI	Committee on the Safety of Nuclear Installations (OECD/NEA)
EME	Emergency Mitigation Equipment
ERO	Emergency Response Organization
FDF	Fuel Damage Frequency
HEP	Human Error Probability
HFE	Human Failure Event
HRA	Human Reliability Analysis
IAEA	International Atomic Energy Agency
IE	Initiating Event
LERF	Large Early Release Frequency
LOCA	Loss-Of-Coolant Accident
LRF	Large Release Frequency
MCR	Main Control Room
MUCDF	Multi-Unit Core Damage Frequency
MUIE	Multi-Unit Initiating Event

Acronym	Description
NEA	OECD Nuclear Energy Agency
NPP	Nuclear Power Plant
NRC	U.S. Nuclear Regulatory Commission
OECD	Organisation for Economic Co-operation and Development
POS	Plant Operating State
PPE	Personal Protective Equipment
PSF	Performance Shaping Factor
PWR	Pressurised Water Reactor
RCF	Release Category Frequency
SAFIR	Finnish Research Programme on Nuclear Power Plant Safety
SAM	Severe Accident Management
SAMG	Severe Accident Management Guidelines
SCDF	Site Core Damage Frequency
SSCs	Structures, Systems and Components
SSM	Strålsäkerhetsmyndigheten, Swedish Radiation Safety Authority
STUK	Säteilyturvakeskus, Radiation and Nuclear Safety Authority of Finland
SUCDF	Single-Unit Core Damage Frequency
SUIE	Single-Unit Initiating Event
VTT	Technical Research Centre of Finland
WGRISK	OECD/NEA CSNI Working Group on Risk Assessment

Table of contents

Page

Appendix

1 Introduction

The fundamental purpose of performing a probabilistic safety assessment (PSA) is to assess the risk and to provide information necessary to manage this risk. Current PSAs typically assess the risk on a reactor unit basis and ignore the possibility of multi-unit accidents including concurrent challenges to spent fuel pools and other sources of radioactive material. The Fukushima Daiichi accident involved releases from three damaged reactor cores and also challenges to the spent fuel integrity on the other units. Effective risk management strategies, requires evaluation and consideration of multi-unit accident scenarios. Such evaluation is here named "site PSA". Essentially, the purpose of a site PSA is the same as for a single-unit PSA. It is to provide information about the risk of different scenarios and which the contributors and uncertainties are, so that effective preventive and mitigation measures can be prioritised.

The objective of this report is to develop guidance on evaluation of site risk for nuclear installations using already existing single-unit PSA models. Focus is on identifying technical issues to address in such an evaluation and propose solutions to them. The methodology presented in this report is based on the work performed in the 2017 year version of the methodology report (Bäckström et al. 2018), the 2016 study report (Tyrväinen et al. 2017) and experience gained in site PSA pilot studies performed for Forsmark and Ringhals NPPs during years 2017 and 2018.

The scope of the report includes issues relevant for operating reactor units with focus on level 1 and level 2 PSA. The report also includes a discussion on fuel pool.

Section 2 in this report discusses general principles on consideration and treatment of dependencies when performing a site PSA. Section 3 presents an overview of the analysis scope and risk metrics, whereas section 4 discusses the impact of different plant operating states. In section 5, identification of multi-unit dependencies is discussed. Section 6 covers dependencies in PSA level 2. Section 7 and 8 discusses data analysis and human reliability analysis (HRA) respectively. Extensions to single unit PSAs are discussed in section 9, while quantification of multi-unit risk is described in section 10. Finally, conclusions are presented in section 11.

Figure 1-1 illustrates the steps included in the analysis.

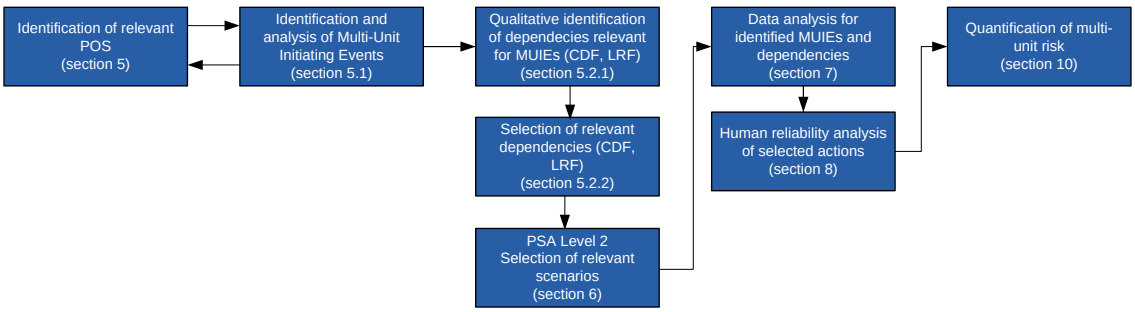


Figure 1-1 – Overview of the analysis process

2 Site dependencies

2.1 Types of site dependencies

There are several types of dependencies that may be relevant to consider in a site PSA. This includes dependencies between different radioactive sources within a reactor unit, such as the reactor core and spent fuel related sources, and dependencies between the radioactive sources of different reactor units.

Figure 2-1 illustrates the scope of various risk assessments with respect to the concepts "site", "unit" and "source" (or fuel location) for a hypothetical site with two reactor units and an interim storage for spent fuel. "Site" covers all units and fuel locations at the site. "Unit" refers to each facility at the site, which has an operating license of its own. In this example, there are three units/facilities at the site. "Source" refers to each point at the site where spent fuel can be located and for which a separate risk assessment can be carried out. In this paper, the source risk is not specifically addressed but the emphasis is on the relationship between the unit risk and the site risk.

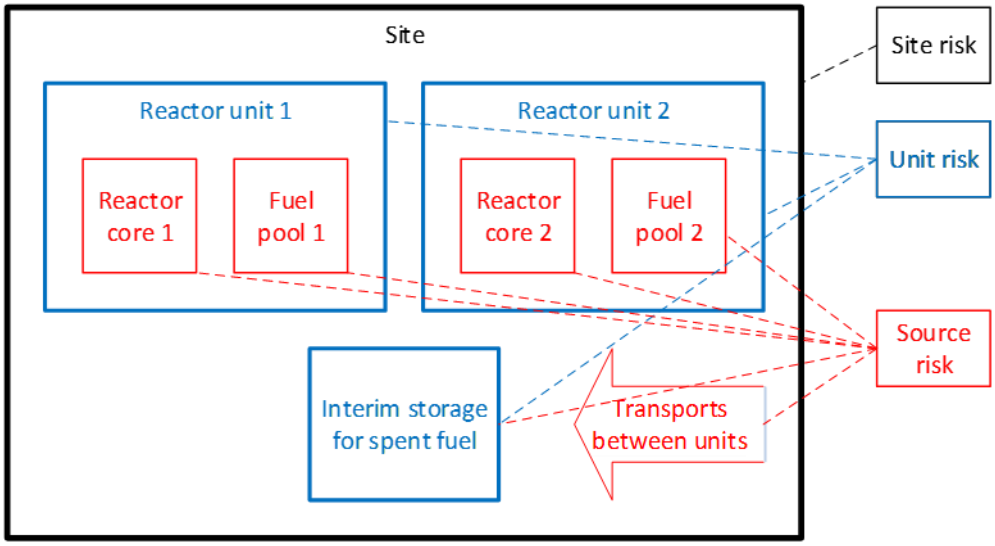


Figure 2-1 - Illustration of concepts "site", "unit" and "source" from the PSA scope point of view.

A "single-unit PSA" (SUPSA) means a PSA made for a nuclear facility such as the reactor facility or unit and the interim storage for spent fuel. A single-unit PSA is assumed to cover all fuel locations within the facility. For a reactor unit, the reactor core and the fuel pool are the relevant locations from the risk assessment point of view. Single-unit PSA can be also understood to refer the types of risk analyses that currently have been prepared for licensing of nuclear facilities.

A "multi-unit PSA" (MUPSA) or "site level PSA" means a PSA or a set of PSAs made to cover accident scenarios related to all fuel locations at the site, including spent fuel transportations. Multi-unit PSA can be also understood to be an extension of a single-unit PSA which can be used to quantify multi-unit risk metrics.

In an analysis of Site risk dependencies between units will play a major role. The importance of the dependencies will be triggered by initiating events that are affecting more than one unit at a time.

In an analysis of the Unit risk it needs to be considered that the safety systems are connected and there are spatial dependencies. This means that within a unit the likelihood of a threat that will expose the radioactive sources at the same time should be significantly higher than between reactor units.

2.2 Relevance of site dependencies

Site dependencies have the potential to contribute to complex scenarios, in particular regarding accident management actions. This impact has not necessarily been considered in safety analyses and emergency/Severe Accident Management procedures that are based on evaluations for single source scenarios.

It can be noticed that site dependencies may be relevant to consider in:

- The risk calculated from a single unit perspective (covering dependencies between units)

- The risk of simultaneous damages and release from multiple radioactive sources

Single unit impact of site dependencies

The relevance of site dependencies from a single unit perspective is that they could potentially affect the single unit risk analysis. Such impact on the single unit risk analysis could be:

- Initiating events could possibly be generated by another unit
- The use of resources (systems, persons) may be affected if more than one unit is challenged at the same time

Generally, all initiating events that can affect one unit shall already be covered by the analysis of initiating events within the unit. Additional initiating events can potentially be generated by scenarios in another unit. Such an event is for example secondary loss of offsite power after an initiating event within a nearby unit. If the statistical analysis of loss of offsite grid is capturing all causes of loss of the offsite grid, then it can be claimed that also the secondary events are covered. It can also be expected that most of these types of secondary events will be of significantly lower frequency and that, if the initiating event frequency in the first unit is already low, they can be considered negligible from a frequency point of view (for example fire initiated propagating scenarios).

Shared resources/dependencies that may be called upon from different units simultaneously could make it relevant to separately study such multi-unit events also in the single-unit PSA. In this report, a single unit PSA is assumed to sufficiently correct represent the relevant dependencies (or modified to do so) to be able to estimate the single unit risk estimate.

Multi-unit impact of site dependencies

The relevance of site dependencies from a multi-unit perspective is that core damage and release from more than one unit at a time may challenge the emergency response in a different way than a single-unit accident. As there are currently no requirements on multi-unit risk metrics, the selection of which risk metrics (if any) that are of relevance will likely be triggered from a severe accident management perspective.

2.3 General screening principles

The number of multi-unit scenarios is expected to be large even for a site with only two reactor units. For this reason, some screening principles are needed to reduce the number of analysed scenarios.

The main focus of the screening is the selection of relevant multi-unit initiating events, and especially combinations of multi-unit events and plant operating states.

When quantitative screening is applied, the slicing effect must be considered (that is, if a dependency is represented by several events its overall impact should be considered). Practically this means that initiating events, plant operating states (POSs) and dependencies need to be properly grouped before screening criteria are applied.

US NRC presented suggested criteria at the WGRISK workshop 2018 (Hudson 2018). According to the presentation it is considered relevant to capture (1) the set of accident scenarios that together contribute at least 95% of the total value for a selected risk metric (where the selected risk metric is typically the mean frequency of a specific end-state of interest); or (2) individual accident scenarios that contribute at least 1% of the total value for a selected risk metric. These criteria are based on ASME and ANS standard (ASME 2009).

If the purpose with the analysis is to quantify a multi-unit risk metrics between two or more units, the contribution criterion refers to the multi-unit accident frequency. This frequency can be expected to be lower than the single unit risk metric. The selection of relevant dependencies may be accomplished in following ways:

- Using an iterative process, where conservative estimates of level of dependency is used prior to the selection of relevant dependencies
- Using the single unit PSA model results to identify all relevant dependencies with a potential to influence the top result

If an iterative process is used, the initial estimates must surely be conservative. When the top result is calculated, an evaluation of the dependencies contributing to 95% of the risk metric is performed. Thereafter the dependency estimates are refined. Note that this approach may need several iterations to properly define the numerical estimates of relevant dependencies.

The other approach, which is described further in this report, is to use the single unit PSA results of the risk metric to identify the relevant dependencies. If it can be demonstrated that the dependency contributes less than 1% to the top result for each of the single unit PSAs, then its impact is not expected to be relevant for the multi-unit risk metric. This assumption may not be true if the multi-unit risk result is much lower than the single unit results, but then the multi-unit risk frequency will be insignificant. It shall be noticed that in the evaluation process there may be a need to adjust the probability for the event (if it does not properly account of the multi-unit perspective).

It is suggested to directly identify all the dependencies that may be relevant when studying level 2 PSA, to avoid having additional dependencies that is affecting the level 1 PSA results when level 2 PSA is studied. This can be achieved by using the level 2 PSA results as the basis for the screening, also in the level 1 PSA identification process.

In the pilot studies within the project a screening level of 1E-8/year was applied on the single unit results to identify relevant dependencies. The same screening level was used both for level 1 and level 2 PSA. As expected, the level 2 PSA did not identify any additional dependencies affecting level 1, and the screening level was found reasonable in pilot studies.

Demonstration of screening of combinations of independent single-unit events

Occurrence of independent initiators could potentially lead to multi-unit core damage. If the sequences are completely independent the probability of multiple core damages will be negligible. Also with dependencies considered, scenarios with two independent initiators will be insignificant from a multi-unit risk perspective and are screened out from further analysis.

The probability of simultaneous initiating events can be studied by analysing a case with two independent initiators occurring within 72 hours. The reason for selecting 72 hours is that for frequent initiators, it can be assumed that the plant is in a stable state after 72 hours.

The highest frequency for a generic single-unit initiating event is typically in the order of 1E-1/year (at-power). The frequency for a second initiating event occurring in another unit within the 72 hour time frame is already quite low:

$$f = \text{1E-1} \times \text{1E-1} \times \frac{72}{8088}\ /yr = \text{8.9E-5/yr.}$$

The frequency of this combination of events leading to an undesired end state would also require the failure of the safety systems. Assuming — very conservatively — a total dependency between the units, the frequency of the undesired event state is obtained by multiplying the frequency above with the conditional failure probability of the safety systems for one unit (which should be at most 1E-4 to meet the risk criterion for CDF below 1E-5/yr). The core damage frequency for such scenarios could hence be estimated as 1E-1 * 1E-1 * 72/8088 * 1E-4 < 1E-8 /yr and can therefore be screened out.

Events that represent a greater challenge to a plant than the above assumed initiator typically have a much lower frequency, and such sequences will therefore fall well below the screening criterion.

3 Selection of analysis scope and risk metrics

The first analysis step is to select the scope of the site level PSA. This includes selection of which radioactive sources to consider, possible plant operating states, initiators to include and end states to study as illustrated in Figure 3-1. The scope of the single-unit PSA needs to be consistent with the selected site level scope.

Which risk metrics to select, representing the chosen end states, is dependent on the purpose with the analysis, whether it is to evaluate the single-unit risk taking the multi-unit aspects into consideration or if it is to evaluate the multi-unit risk. The SITRON risk metrics report (Holmberg 2017) proposes two groups of risk metrics for site level risk: one group of risk metrics for a single-unit PSA, which accounts for multi-unit scenarios, and a second group for a site PSA.

The single-unit risk metrics proposed are:

- Core or fuel damage frequency per fuel location
- Release frequency per fuel location (different groups of release categories included)
- Integrated fuel damage for the reactor unit
- Integrated release frequency for the reactor unit.

The multi-unit risk metrics proposed are:

- Site core/fuel damage frequency
- Multi-unit core/fuel damage frequency
- Site release category frequency.

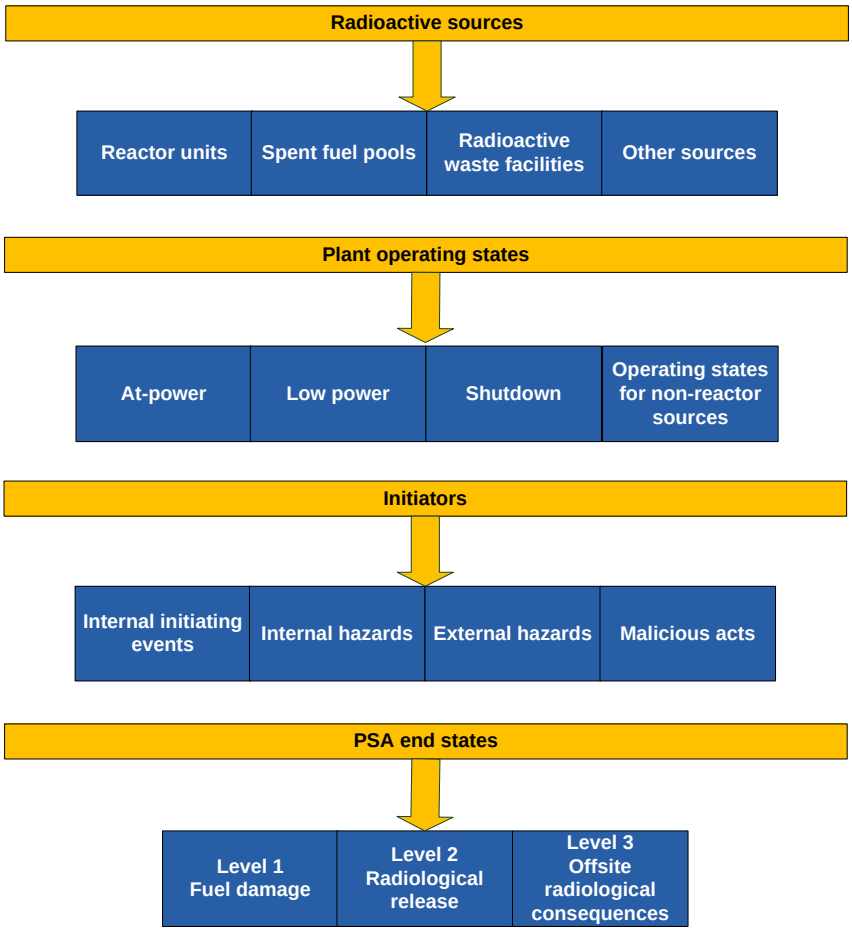


Figure 3-1 – Selection of analysis scope for site level PSA

4 Analysis of POS impact

4.1 Introduction

A realistic multi-unit scenario assessment has to account for the units' various combinations of possible plant operating states (POS). POSs need to be defined at unit level considering all radioactive sources in the unit. In addition to reactor related systems, the status of the spent fuel pool, e.g. fuel pool gates, needs to be taken into account. Available safety systems and recovery actions differ between the different POSs. A reasonable approach should be identified to cover relevant configurations from the site level point of view.

A complete consideration of all possible combinations of POSs between several units could lead to a large number of "site" POS combinations. For instance, in a Hungarian pilot study (Bareith et al. 2016), 123 distinct site POS combinations were identified for a site with four reactors and four spent fuel pools.

Basically, there are two approaches to manage POS combinations: 1) brute force analysis of all possible combinations, 2) limited analysis of most relevant combinations. The first option is impractical since, for instance, the PSA models for Forsmark 1&2 respectively Ringhals 3&4 both handle tens of individual POSs. Theoretically, there could be more than 100 POS combinations for a two-unit site, even if simultaneous refuelling outage at two units could be ruled out. Therefore, the second option is considered the only reasonable approach.

4.2 Approach to a two-unit site

The following approach is intended for a site with two reactor units, and each unit has both the reactor and the spent fuel pool as major sources of radioactive release to be considered. The approach follows the second option described in the previous subsection, meaning that the analysis will be limited to the most relevant POS combinations.

As a starting point, the following combinations (a two-unit site) can be considered:

1) both units are in power operation
2) unit 1 is in power operation, unit 2 is in outage
3) unit 1 is in outage, unit 2 is in power operation.

It is obvious that the POS combination 1 (both at-power) shall be analysed in a site PSA. Therefore, only aspects related to treatment of outage POS combinations (2 and 3) are discussed below.

It should also be noted that operational state of the spent fuel pool follows the state of the reactor. In this sense, there is no need to specifically address spent fuel pool states when identifying relevant POS combinations. Whatever POS combination between reactor units will be considered, dependencies between the reactor and spent fuel pool need to be considered, and that can be included in a separate study, see Section 4.3.

Since the outage consists of several somewhat different POSs, some further elaboration of shutdown POSs is needed to identify the important ones. This elaboration is dependent on the type of multi-unit initiating events that are to be analysed. Outage POSs can roughly be divided into two groups:

a) Outage POSs where the primary circuit is closed. In these POSs, the plant's status is close to power operation POS. The spectrum of interesting multi-unit initiating events is presumably almost the same as when both units are in power operation. The duration of these POSs is short (few days per year), and one possibility could be to claim that these POSs combination are covered by POS combination 1 (both units at power).

b) Outage POSs where the primary circuit is open. The configuration of the plant is quite different from power operation configuration, which means that the spectrum of interesting multi-unit initiating events needs to be analysed in more detail. The duration of these POSs is considerably longer than the duration of outage POSs of case (a). On the other hand, at this stage the time windows to recover residual heat removal is usually long, for which reason there is not necessarily a need to analyse this POS combination.

It shall be noticed that for a pressurised water reactor (PWR), there is a special case of b), where the primary circuit is open, but the recovery time is short. This POS has to be considered separately.

Approach to screen relevant outage POS combinations and multi-unit initiating events in these combinations:

- For the purpose of multi-unit assessments, merge together POSs into a fewer POS groups. Since the multi-unit scenarios typically have impact on core cooling and residual heat removal functions, regrouping of POSs can be based on the configuration of residual heat removal systems.
    - Estimate the time shares of these larger POS groups.
    - Define time windows for core/fuel damage in case of loss of residual heat removal in each POS group.
    - Consider possibly screening out of a POS group due to short duration or due to very long time window to fuel damage.

- Categorise multi-unit initiating events from their season and POS group dependency point of view to screen out irrelevant combinations. Season dependency is related to external hazards which can have different likelihood, e.g. during winter compared to summer season, while longer outages are typically carried out in Nordic NPPs during the summer season.

The analysis of POS impact is an iterative process with the selection of multi-unit initiating events. Some part of the POS analysis can be performed on a general level, whereas the last part of the analysis requires the list of multi-unit initiators. Screening principles should be same as discussed in Section 2.2.

4.3 Spent fuel pool

Reactor units of typical BWRs and PWRs include a spent fuel pool, and the assessment of fuel damage risk and release risk is a part of single-unit PSA. From MUPSA point of view, the most interesting question is the dependency between the reactor and the spent fuel pool within a reactor unit. Risk contribution from the dependencies of spent fuel pools at different reactor units is covered by risk contribution from the dependencies between reactors.

Although there are differences in design and operational practices, the following main dependencies are valid for a typical BWR/PWR. From the POS point of view, there are two main operational states:

1. power operation, when the fluid systems of the reactor and spent fuel pool are disconnected but there are nevertheless dependencies via the residual heat removal systems
2. refuelling outage, when the fluid systems of the reactor and spent fuel pool are connected, meaning not only dependencies via the residual heat removal but possibly also via the water inventory control.

For the case 1, one can limit the analysis of dependencies into events that lead to loss of residual heat removal. Usually there is much longer time to recover residual heat removal for spent fuel pool (days) than for the reactor (hours), meaning that most scenarios can be screened out (using principles of Section 2.2). However, in case of core damage and a release happen for the reactor, one should study in which manner the fuel pool cooling can be managed in long term. Such scenarios have not usually been analysed in single-unit PSAs, and they can require further consideration.

The case 2, refuelling outage, is a POS that should normally be covered by the shutdown PSA. For this operational state, the guidance for shutdown PSA should be followed.

To calculate the integrated fuel damage frequency or integrated release category frequency (Holmberg 2017) of a unit, reactor and fuel pool analyses need to be combined. EPRI presents an integrated reactor unit model covering also spent fuel pool risks (EPRI 2013, EPRI 2014). The end states of containment event trees of the reactor PSA are linked to spent fuel pool event trees, and the model contains accident sequences covering both radionuclide releases from the reactor core and spent fuel pool accidents. There are also event trees for independent spent fuel pool accidents. In principle, reactor and spent fuel pool analyses could also be combined by the same method that is applied to the dependencies between units in this report if their models are separate.

We assume that dependencies between a reactor and a spent fuel pool in the same unit are handled in single-unit PSA. In multi-unit analysis, we assume that either spent fuel pool accident sequences can be screened out or it is possible to produce minimal cut sets for fuel damage of a unit including minimal cut sets related to the fuel pool.

5 Identification of multi-unit dependencies

5.1 Identification of multi-unit initiators

The next step in the multi-unit analysis is to identify the initiators that can lead to multi-unit sequences. The initiating event analyses in the existing single-unit PSAs should be reviewed to identify which events can affect one unit only and which events can impact multiple units concurrently. The initiating events could be categorized as follows:

- Single-Unit Initiating Events – the initiating events occur in one unit only and will not affect other units or radioactive sources (except possibly in a later phase of the accident), e.g. pipe break (LOCA).
- Multi-Unit Initiating Events (MUIE) – the initiating events challenge two or more units or radioactive sources on the site concurrently, e.g. seismic events and other external hazards.
- Partial Multi-Unit Initiating Events – the initiating events occur on a single unit or impact multiple units, depending on the cause. An example is loss of offsite power which can affect a single unit or any combination of units depending on the specific causes. Events in this category are placed into one of the previous initiating event categories depending on the specific cause(s).

It might be necessary to go back to a more comprehensive list of potential initiating events in the individual PSAs (before screening) to see if any events screened out might be relevant to analyse in a multi-unit context.

Partial multi-unit events may, conservatively, be considered as multi-unit events to limit the work. Some loss of offsite power events can for example be caused by internal plant faults that may be confined to a single unit, while others are caused by switchyard faults that could impact any combination or all units on a site. To fully analyse the appropriate unit combinations affected by each cause, more detailed analyses will be necessary.

Different MUIEs may impact different combinations of units.

All identified MUIEs are relevant for further analysis if their frequency is greater than the screening criterion.

Single-unit events may be relevant from a multi-unit perspective if:

a An initiating event in unit *x* introduces an initiating event in unit *y*.

Examples are a transient at one unit that causes a secondary loss of offsite power for another unit, or a fire in one unit that spreads through fire barriers to another unit.

b The accident sequence, *when the sequence becomes a severe accident,* following an initiating event in unit *x* introduces an initiating event in unit *y*.

Even if an initiating event at one unit will not itself introduce an initiating event at another unit there is a possibility that the accident sequence following the initiating event will do it. A severe accident induced hydrogen explosion may for example damage the structure of a neighbouring unit or lead to missiles hitting the switchyard inducing another initiating event.

If the scenario, starting from a single unit event, can be shown to be below the screening threshold considering the conditional probability of propagation (a or b above) it can be screened out.

The expected scenarios that may need to be evaluated for case a) is a secondary loss of offsite power and fire and flood events.

For scenario b) the important question is if the accident sequence somehow can induce an initiating event at another unit. It is assumed that this cannot happen unless the accident sequence involves an explosion of some kind or a hydrogen leak directly to a nearby unit. In all cases, the initiating event must however have caused core damage. If it can be demonstrated that these scenarios will be less than the applied screening level, e.g. 1E-8/year, scenario b) can be screened out. The screening can hence focus on a justification that the other unit has a maximum conditional core damage probability of 1E-3 (assuming that the single unit core damage frequency is 1E-5 /year or less).

5.2 Identification and selection of dependencies

Relevant dependencies for the identified initiators need to be identified. The dependencies can be:

- Shared structures, systems and components (SSCs)
- Identical components
- Spatial dependencies
- Human and organizational dependencies
- Containment and vessel design
- Simultaneous maintenance

These are described separately below.

Shared SSCs

There are different types of shared connections in a nuclear power plant. These connections can be categorized according to the approach used in (Muhlheim & Wood 2007), where the two main categories "structures and facilities" and "systems and equipment" are used, the latter having three sub-categories:

- Sharing of structures and facilities
    - Examples of shared structures and facilities include service water intake structures and different types of storage tanks. There are also plant designs where turbine and/or auxiliary buildings are shared.
- Sharing of systems and equipment
    - Systems that can support multiple units simultaneously.

      Systems in this sub-category include station blackout gas turbines and common fire protection systems.
    - Independent systems at each unit that can be cross-connected to support another unit or single systems able to fully support only one single unit at a time.

      Systems in this sub-category include demineralized water distribution and emergency diesel generators that may be configured to support only one unit at a time.
    - Independent systems at each unit sharing standby or spare equipment.

      Systems in this sub-category include portable pumps for independent cooling.

Connections that are shared differ widely between plants, even between plants with the same vendor. Many of the shared connections are however not important from a PSA point of view, e.g. shared office buildings and shared communication systems.

Identical components

This dependence category refers to common cause failures (CCF) of identical systems or components at multiple units due to causes other than external hazards (e.g. design errors or maintenance errors repeated on several units). In (Schroer & Modarres 2013) strong evidence is presented that dependent failures occur with a relatively high frequency involving multiple units.

It is very site specific which component types could be sensitive to inter-unit CCF. On a site with two reactor units of the same design the number of identical systems or components is larger than if the reactor units are of different design.

All identical components are potential CCF candidates. The CCF candidates are selected by studying the scenarios for the relevant multi-unit initiators. For component types where inter-system CCF has been found negligible in the single-unit PSAs, it is considered applicable to exclude inter-system CCF between units for the same reason.

Spatial dependencies

Spatial dependencies may be of importance in a site PSA in two principal ways:

- An initiating event in one unit has the potential to spread to at least one other unit

  For units sharing structures and facilities or being closely located, internal hazards, such as an internal fire, can affect or spread to a neighbouring unit. Events of importance in this sub-category are typically identified in the initiating event step (see section 5.1).

- An accident sequence in one unit has the potential to affect at least one other unit

  Even if the initiating event is considered a single-unit event there is a possibility that an accident sequence affects another unit. A severe accident induced hydrogen explosion may for example damage the structure of a neighbouring unit or generate missiles hitting the switchyard inducing another initiating event. See also discussion in section 5.1.

Human and organizational dependencies

Multi-unit accidents pose additional challenges on operators and these additional challenges are not modelled in a single-unit PSA. These challenges may arise from constrained human resources, additional complexity in managing multiple scenarios from a common location, shared system prioritization, prioritizing the deployment of portable equipment, etc. Challenges also include that a radioactive release from one unit in case of a multi-unit accident might affect critical operator actions that have to take place outside the main control room of another unit.

The human and organizational dependencies related to the multi-unit scenarios should be identified and covered in the HRA. In general, multi-unit HRA will need to put more emphasis on organizational and management aspects in the analysis. These factors need to be included in not only quantification, but also task analysis and modelling.

The degree of added complexity in the analysis of operator actions in multi-unit accidents will depend greatly upon the amount of interdependence between the individual units. This interdependence may come from the nature of the initiating event, the amount of shared systems/equipment or the amount of shared resources.

The identification of human and organizational dependencies is further elaborated in Section 8.

Containment and vessel design

In level 2 PSA, the containment and vessel design will be an important area to evaluate. The knowledge about the different containments ability to withstand stress and how well the containments can handle damage scenarios will be crucial. If the plants are of same or similar design, and subject to the same failure scenario, the likelihood of both failing simultaneously can be greater than if they are of different design. Vessel design and vessel failure modes will also be very important input. The containment and vessel design are expected to have significant importance in the evaluation of dependency for phenomena.

Simultaneous maintenance

Within a unit the Technical Specifications govern which systems can be out for maintenance at the same time and also how many redundancies within a specific system can be unavailable. Between units at a site no such rules exist. It is therefore possible that for example a number of diesel generators are out for maintenance at all units at a site simultaneously. In case of a loss of offsite power all units will then have an already degraded system barrier.

The multi-unit event of two independent corrective maintenance actions, ongoing on more than one unit at the initiation of a multi-unit event, can be screened out. Preventive maintenance actions that can occur simultaneously on multiple units may need to be considered.

5.2.1 Qualitative identification of potential dependencies

The different types of dependencies listed in previous section need to be identified. The identification process is based on:

- Plant documentation, for example safety analysis report
- PSA model, for example systems and events included
- Experience from other multi-unit risk analysis demonstrating which type of dependencies were found relevant in those analyses

The identification process is in this step qualitative and intended to create a list of all potentially relevant dependencies. The dependencies are ranked in the categories ‘very important’, ‘important’, ‘less important’ and ‘insignificant’ to:

- Ensure that the dependencies that are considered likely to be relevant are captured correctly in the quantitative analysis.
- Screen out dependencies that do not require further analysis (provide evidence).

Table 5.1 summarizes the definition of the four different categories.

Table 5.1 – Importance categories for qualitative identification

Category	Description
Very important	Dependencies where no additional SSCs are available to cope with an initiating event, e.g. a shared water intake.
Important	Dependencies where a limited number of additional SSCs are available to cope with an initiating event, e.g. diesel generators at a site with a shared station blackout gas turbine system which back-ups unit-specific EDGs
Less important	Dependencies where a number of additional SSCs are available to cope with an initiating event, e.g. a shared fire water system.
Insignificant	Dependencies without effect on the risk for core damage or a radioactive release, e.g. a shared domestic water system.

Dependencies ranked as ‘very important’ or ‘important’ in the qualitative analysis are expected to be relevant in the quantitative selection of dependencies for further analysis.

5.2.2 Selection of relevant dependencies

Following the qualitative identification of dependencies, the relevant dependencies also considering the quantitative impact shall be selected. With relevant dependencies is meant any dependency that from a multi-unit perspective can have a non-negligible impact on the multi-unit risk metrics.

All dependencies identified as 'very important', 'important' or 'less important' shall be analysed with regard to representative event(s) to make it possible to quantitatively evaluate the dependency. If the PSA model does not capture a dependency that is classified as 'very important' or 'important', this will need to be evaluated to ensure that the dependency is properly accounted for in the further analysis. This may mean that the PSA model should be extended.

If a quantitative screening is applied to screen out dependencies, such approach should cover all relevant initiators (identified in Section 5.1) to avoid the slicing effect. The importance of the dependency should be represented by all relevant basic events (also to avoid slicing). One possible way to perform a quantitative screening is outlined below.

For each initiator, dependencies are analysed based on the Fussell-Vesely importance of the basic events related to each dependency. Combinations of relevant dependencies also have to be considered. The use of importance measure could be performed by:

1. Generate a CDF MCS list for each identified multi-unit initiating event for each unit. For each unit the importance is studied separately following steps 2 and 3.
2. For identified dependencies, select appropriate basic event(s) to represent each dependency *i* respectively. If no suitable basic event(s) exist, the dependency cannot be screened out at this point and the PSA models should likely be completed to represent the dependency.
3. Calculate the maximum contribution from potential multi-unit sequences for each relevant dependency *i* (represented by selected basic events) according to:

$$Fmu_i = \sum_{n=IE1}^{IEy} FV_{i,n} \times CDF_n \times D_{i,n}$$

where:

$FV_{i,n}$ is the Fussell-Vesely importance for dependency *i* at initiating event *n,*

CDF_n is the core damage frequency for initiating event *n*, and

$D_{i,n}$ is a factor to account for a potential probability increase (if the single-unit PSA is potentially not fully capturing the multi-unit impact). If the dependency studied is a shared system that can only be used at one unit at a time or an operator action where its probability may increase in a multi-unit scenario, a factor ($1/P_i$) shall be applied to account for the potential increase. P_i for a shared system is the failure probability of that specific system function and for an operator action the value basic event before penalizing it (see section 8). In other cases $D_{i,n} = 1.0$.

4. If Fmu_i is lower than the selected screening criterion for one unit, the dependency can be screened out in all combinations including this unit. The screening criterion is discussed in section 2.2.

The above suggested screening process can be applied on dependencies relevant in level 1 PSA. If the identified sequences have a sufficiently low frequency, then the screening ensures that the dependencies relevant for level 1 PSA sequences, that are to be continued in the level 2 PSA, are taken into account. The same screening process can also be applied for level 2 PSA, where CDF in the above formula is then exchanged for the risk metric studied (for example LRF).

When relevant dependencies are identified, combinations of dependencies need to be evaluated. The evaluation of relevant combinations is performed by studying their relevance (if they may appear together in MCSs) and by consideration of the likelihood of such combinations. Many combinations of dependencies can easily be screened out based on the frequency of the multi-

unit event combination. The evaluation of the likelihood of combinations requires estimation of the probabilities (see sections 7 and 8).

The output of this approach is a list of initiating events and combinations of dependencies that eventually shall be quantified.

6 Multi-unit dependencies in level 2 PSA

When multi-unit PSA is extended to level 2, there are a few practical and technical differences how the analysis can be carried out. Section 6.1 discusses selection of relevant scenarios for further considerations. Section 6.2 discusses identification of item-specific dependencies comparable to discussion in Section 5.2.

6.1 Screening of scenarios

An important part of the identification process is the screening of scenarios. Screening means in this context selection of multi-unit plant damage states (PDS)[1], source terms (ST)[2] and release categories (RC)[3] to be considered quantitatively. Screening process is somewhat dependent on the quantification approach (Section 10.2), but we can nevertheless assume that screening as well as quantification will be performed stepwise:

- assessment of multi-unit plant damage states
- assessment of multi-unit source terms
- assessment of multi-unit release categories.

These steps should *not* be understood so that we assume that units experience, in a more or less synchronized way, firstly a core damage (that is further associated with a plant damage state) and secondly a release (that is further associated with a source term and corresponding release category). In fact, one possible multi-unit accident scenario could be such that one unit first experiences core damage and a release and the release from this unit makes things worse for the other unit(s). This scenario is further discussed in the next section.

The point here is to identify those plant damage state combinations and containment event trees that are worth studying from the dependency identification point of view. Most PDS-combinations are unlikely due to few dependencies between events contributing to different PDSs. With regard to ST and RC-combinations, relevance of a combination is dependent on the applied risk metrics. See discussion below.

Figure 6-1 depicts a schematic level 2 PSA model for a site risk analysis, starting from the end states of site level 1 PSA. For the accident sequences where only one unit has a fuel damage, plant damage state categorisation and subsequent level 2 PSA modelling and quantification follow the basic principles of a single-unit level 2 PSA.

[1] Plant damage state: Group of accident sequence end states that have similar characteristics with respect to accident progression and containment or engineered safety feature operability. (ASME 2014)

[2] Source term: The characteristics of a radionuclide release at a particular location including the physical and chemical properties of released material, release magnitude, heat content (or energy) of the carrier fluid, location relative to local obstacles that would affect transport away from the release point, and the temporal variations in these parameters (e.g., time of release duration, etc.). (ASME 2014)

[3] Release category: A group of accident progression sequences that would generate a similar source term to the environment. Similarity in this context depends on the level of fidelity of the analysis and the number of release categories used to span the entire spectrum of possibilities. Similarity is generally measured in terms of the overall (cumulative) release of activity to the environment, the time at which the release begins, and (in certain applications) other physical characteristics of the source term. (ASME 2014)

The bottom accident sequence of Figure 6-1 , where more than one unit experience a fuel damage, may require a special treatment. This is indicated by the plant damage state categorisation (MUPDS1, ..., MUPDSm). Multi-unit PDSs can simply be defined as products of single-unit PDSs.

In level 2 PSA, each sequence of the containment event tree (CET) is associated with a source term, and further with a release category. Multi-unit STs can also simply be defined as products of single unit STs.

With regard to release categories, we propose in the risk metrics report (Holmberg 2017) use of the same risk metrics for single-unit PSA as for multi-unit PSA. Therefore, release categories could be the same for single-unit and multi-unit sequences.

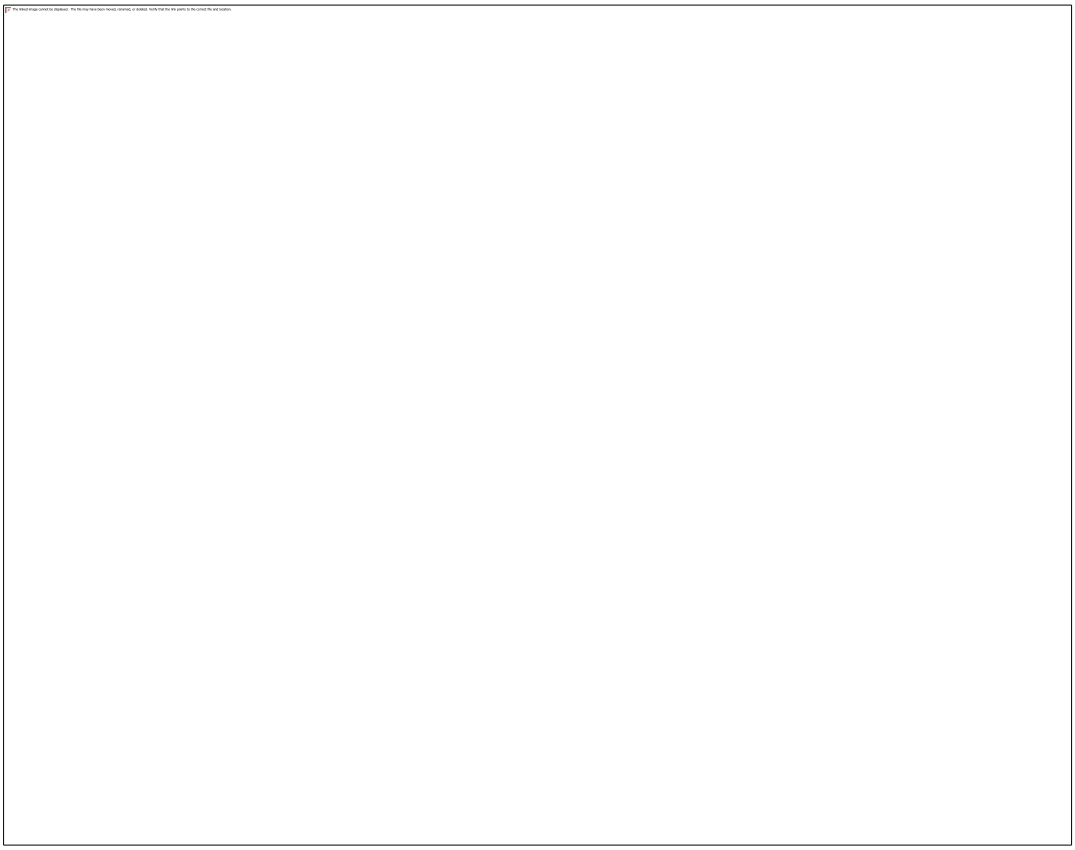


Figure 6-1 - Event sequences and associated release category risk metrics for a level 2 PSA for a two-unit-site.

As can be seen from Figure 6-1 , there can easily be a lot of different cases to be quantified in a multi-unit PSA, if one wants to quantify various PDS-, ST- and RC-combinations. However, if the focus is, e.g., only on quantifying the frequency for an unacceptable release[4] at the site level, the quantification can be simplified considerably, as discussed below.

One of the findings of the pilot studies is the fact that a condition for a multi-unit sequence to be classified unacceptable release is that one of the unit-specific sequences leads to unacceptable release. A combination of two acceptable releases will hardly lead to an unacceptable release, when combined together. This means that all PDSs and STs not leading to an unacceptable release can be screened out from further identification process and the assessment can be

[4] Release more than 0.1 % of the core inventory of Cs-134 or Cs-137 from an 1800 MWt BWR (Barsebäck 1 unit). This is so called "RAMA" criterion defined in 1980's in Sweden when the decision was made to implement severe accident mitigation systems for the NPPs.

focused on a single case where both units experience an unacceptable release. This is based on the assumption that SUPSA provides correct risk metrics from the single-unit point of view, and the fact that

SRCF(unacceptable) = 2 × SURCF(unacceptable) – MURCF(unacceptable).

If the aim is to quantify frequencies of more release categories, the same procedure as described above can be applied to find out which PDS and RC combinations need to be analysed, i.e., one should check how much each PDS contributes to each RC.

6.2 Identification of dependencies

Given that it has been possible to identify relevant PDS combinations and CET sequences, the next step is to identify item-specific dependencies. Identification of multi-unit dependencies in level 2 PSA is similar to level 1 PSA. Shared SSC dependencies and inter-unit CCFs shall be handled in the same way as in level 1 PSA.

With regard to operator action dependencies, the scenarios can become more complex in level 2. A specific issue for level 2 to be considered is the case when one unit experiences a core/fuel damage resulting in a release or at least a threat of release. The question is how the other unit(s) are affected. Here, we can distinguish between single-unit IE and multi-unit IE. In the case of single-unit IE, the other unit has not, by definition, been affected by the initiating event, and there are thus not much relevant system dependences in this scenario. Even though, the other unit may be e.g. forced to shut down, and initiate some precautionary actions to protect personnel, it is not likely that the other unit will suffer a core damage, since the technical system are unaffected. The scenario can thus presumably be screened out.

The other case, multi-unit IE, is different and it is relevant to analyse the impact of release from one unit to operator actions in the other unit, even from level 1 PSA point of view. Basically, all relevant operator actions in level 1 PSA should be reassessed, but focus can be limited to actions later in the scenario. Especially local actions can be much more difficult to perform in these scenarios, but also the main control room can be impacted.

Analysis of operator action dependencies should otherwise follow the same approach as in level 1, see Section 8. Similar screening principles as discussed in Section 2.2. are applicable.

One new feature in level 2 PSA is the handling of phenomenological uncertainties (which are usually not an issue for level 1 PSA). Uncertainties related to the occurrence of certain phenomena during severe accidents (e.g. steam explosion) mean that there could be state-of-the knowledge dependencies between units, which should be taken into account. This topic is discussed in Section 7.5.

7 Data analysis

7.1 General dependency categories

Probabilistically, the task of the data analysis can be associated with the task to estimate the conditional probability of a multi-unit event given the probability of a single-unit event. Let A_1 and A_2 be a pair of dependent basic events at units 1 and 2 (for simplicity we only consider the case with two units). Assuming that single-unit PSAs have been developed correctly, the marginal probabilities $P(A_1)$ and $P(A_2)$ can be obtained from the corresponding single-unit PSA.

The main quantification task for MUPSA is to estimate the probability of the joint event $A_1 \cdot A_2$, i.e., $P(A_1 \cdot A_2)$. The joint probability is obtained from the formula

$$P(A_1 \cdot A_2) = P(A_1 \cdot A_2|A_1) \cdot P(A_1) = P(A_2|A_1) \cdot P(A_1) = P(A_1|A_2) \cdot P(A_2).$$

Obviously, if $P(A_2|A_1) = P(A_2)$, there is no dependency between the basic events. On the other hand, if $P(A_2|A_1) = 1$, there is a full dependency. Otherwise, there is a partial dependency.

Since most interesting cases belong to the category of partial dependencies, it would be practical to further partition them into subcategories "low", "medium" and "high" dependency.

The intent of the dependency levels would be

- To simplify estimates (make it possible to perform rough estimates quickly)
- To create a uniform way of defining dependencies between different types of dependencies
- To assist in the presentation of results from the data analysis (is this a low dependency, or a high dependency)

Different concepts of defining dependency levels have been studied during the project, but no numerical dependency levels and values are suggested for time being. An example of how to assign a numerical dependency level is found in one of the pilot studies.

7.2 Initiating events

7.2.1 Multi-unit events

By definition, the multi-unit events, which practically all are external events, always affect all units on the site. The estimation of the frequencies can be performed in the same way as in single-unit analyses.

7.2.2 Partial multi-unit events

Some events can affect different combinations of the units at the site. In such case, a separate frequency needs to be estimated for each possible combination of affected units, i.e. the total frequency needs to be divided for unit combinations.

If there is enough operating data and the affected unit combination is indicated in the records for each occurrence, the frequencies for different combinations can be estimated directly based on the number of occurrences or using some parametric model.

Usually, there is however not enough operating data because partial multi-unit events have small frequencies. It is expected that in most cases estimation of partial multi-unit event frequencies requires event specific analyses. As an example, loss of offsite power is discussed in Section 7.2.3.

One possibility is to identify different possible causes for the partial multi-unit event and analyse them separately. An alternative is to conservatively assume that all units are always affected. It is likely sufficient to use this conservative assumption in tentative analysis. If the risk contribution of a partial multi-unit event appears to be significant under this assumption, more detailed analysis can be performed.

7.2.3 Loss of offsite power

Loss of offsite power can be caused by different types of events (Johnson & Schroeder 2016) including:

- weather-related events,
- grid-related events,
- switchyard-centered events,
- plant-centered events.

Plant-centered events affect only the corresponding unit. Switchyard-centered events can affect any combination of units depending on what components in the switchyard are failed. Weather-related and grid-related events can also affect any combination of units, even though they affect all units most often. The frequency for the simultaneous loss of offsite power at all units on the site is

$$F(all\ units) = F_w(all\ units) + F_G(all\ units) + F_S(\text{all units}),$$

where $F_w(all\ units)$ is the frequency of weather-related events where all unit are affected, $F_G(all\ units)$ is the frequency of grid-related events where all units are affected, and $F_S(\text{all units})$ is the frequency of switchyard events where all units are affected. The frequency of the loss of offsite power event where only one unit (A) is affected is

$$F(A) = F_P(A) + F_S(A) + F_w(A) + F_G(A),$$

where $F_P(A)$ is the frequency of the unit A plant-centered loss of offsite power events, $F_S(A)$ is the frequency of switchyard events where only unit A is affected, and $F_w(A)$ and $F_G(A)$ are respectively the frequencies of weather- and grid-related events where only unit A is affected.

The loss of offsite power frequency of a unit combination including more than one unit but not all units is estimated in the same way based on those weather-related, grid-related and switchyard-centered events that affect the considered combination of units.

7.3 Identical components

Inter-unit CCF (Le Duy et al. 2018, Kim et al. 2018) can be defined in the same way as normal CCF, see e.g. (Wierman 2007). The only difference is that components fail in multiple units instead of a single unit.

Currently, Inter-unit CCF data are scarce, but there are some CCF data collection activities in progress (Håkansson 2017). The situation may be improved in the future. (Le Duy et al. 2018) introduced multi-unit impact vectors, as well as a method to generate inter-unit CCF data by simulation. Here, we take slightly different approach and introduce an impact matrix:

$$IM = \begin{bmatrix} I_{0,0} & I_{0,1} & \cdots & I_{0,m} \\ I_{1,0} & I_{1,1} & \cdots & I_{1,m} \\ \vdots & \vdots & \ddots & \\ I_{m,0} & I_{m,1} & \cdots & I_{m,m} \end{bmatrix},$$

where we assume a site with two units, m is the number components in one unit, and $I_{i,j}$ is the probability that a CCF event included i components in the first unit and j components in the second unit. The impact matrixes can be estimated with similar type of parametrization as used in (Le Duy et al. 2018), i.e. based on component impairment factor, shared cause factor and time factor. The difference to (Le Duy et al. 2018) is that here we separate inter-unit combinations from intra-unit combinations completely, including combinations with two components.

Now assume that we have N impact matrixes related to different failure events or demands. For CCF probability estimation, the total impact matrix is calculated entrywise summing the impact matrixes:

$$TIM = \begin{bmatrix} T_{0,0} & T_{0,1} & \cdots & T_{0,m} \\ T_{1,0} & T_{1,1} & \cdots & T_{1,m} \\ \vdots & \vdots & \ddots & \\ T_{m,0} & T_{m,1} & \cdots & T_{m,m} \end{bmatrix} = \sum_{k=1}^{N} IM(k),$$

Value $T_{0,0}$ is the number of demands without failures.

The probability that specific a components fail in one unit and specific b components fail in the other unit can be calculated as

$$Peg(a,b) = \frac{T_{a,b} + T_{b,a}}{2\binom{m}{a}\binom{m}{b} \cdot ND},$$

where ND is the total number of demands for the whole group of $2m$ components:

$$ND = \sum_{i=0}^{m} \sum_{j=0}^{m} T_{i,j}.$$

If there are more than two units, impact matrixes can be generalised to include as many dimensions as there are units. In the case of three units, the probability estimation formula is

$$Peg(a,b,c) = \frac{T_{a,b,c} + T_{a,c,b} + T_{b,a,c} + T_{b,c,a} + T_{c,a,b} + T_{c,b,a}}{3!\binom{m}{a}\binom{m}{b}\binom{m}{c} \cdot ND}.$$

In the case of four units, the probability estimation formula is

$$Peg(a,b,c,d) = \frac{T_{a,b,c,d} + T_{a,b,d,c} + \cdots + T_{d,c,b,a}}{4!\binom{m}{a}\binom{m}{b}\binom{m}{c}\binom{m}{d} \cdot ND}.$$

If there is not enough multi-unit data, an option is to use single-unit data and to assume conservatively that inter-unit CCFs are as probable as intra-unit CCFs. In that case, the best option is to use the same data that is used in the single-unit PSA. However, if the data does not cover enough components, some other data source can be used for multi-unit analysis. For example, if one unit contains four components and the data has been collected only for the case of four components, it cannot directly be applied to the multi-unit case with eight components.

Generally, the analysis of dependencies in the screening step should identify which combinations of CCFs that are of relevance from a multi-unit perspective. It is most likely not relevant to study all combinations, but a few CCF combinations may be of relevance. Concerning the case of two units, the complete CCF with all identical components is typically the most significant event to the multi-unit risk. In that case, the conditional probability that all components fail in one unit given that all components fail in the other unit needs to be estimated. The inter-unit CCF probability can be calculated as

$$P(CCF\ in\ units\ 1\ and\ 2) = P(CCF\ in\ unit\ 2) \cdot P(CCF\ in\ unit\ 1 \mid CCF\ in\ unit\ 2).$$

If intra-unit CCFs have different probabilities in different units, the smaller probability can be used, i.e. if the probability is smaller in unit 1, switch the places of the units in the above formula. The conditional probability can be estimated as

$$P(CCF\ in\ unit\ 1 \mid CCF\ in\ unit\ 2) = \frac{\widehat{Psg}(2m)}{\widehat{Psg}(m)},$$

where $Psg(m)$ is the probability that at least m specific components fail, in this case m components in one unit. Therefore, $Psg(2m)$ and $Psg(m)$ should be estimated. According to (Mankamo 2017), $Psg(a)$ can, for example, be estimated based on impact vectors as

$$\widehat{Psg}(a) = \sum_{k=a}^{2m} \frac{\binom{2m-a}{k-a} \cdot V(k|2m)}{\binom{2m}{k} \cdot ND},$$

where $V(k|2m)$ is the number of CCFs with k components (i.e. the sum value obtained from impact vectors), and ND is the total number of demands for the whole group of $2m$ components:

$$ND = \sum_{k=0}^{2m} V(k|2m).$$

Impact vectors for various components and failure modes can be found e.g. in (U.S.NRC 2016). It is straightforward to generalise the estimation formula for the case of more than two units.

If a system has a failure criterion q-out-of-m in one unit, the conditional probability that at least q components fail in one unit given that at least q components fail in the other unit can be estimated as

$$P(q\ fail\ in\ unit\ 1 \mid q\ fail\ in\ unit\ 2) = \frac{\widehat{Pmu}(q,q,m)}{\widehat{Pmu}(q,0,m)},$$

where $Pmu(a,b,m)$ is the probability that at least a components fail in the first unit and at least b components fail in the second unit:

$$\widehat{Pmu}(a,b,m) = \sum_{k=a+b}^{2m} \frac{\sum_{l=\max(k-m-a,0)}^{\min(k-a-b,m-a)} \binom{m}{a+l}\binom{m}{k-a-l} \cdot V(k|2m)}{\binom{2m}{k} \cdot ND},$$

where

$$\sum_{l=\max(k-m-a,0)}^{\min(k-a-b,m-a)} \binom{m}{a+l}\binom{m}{k-a-l}$$

is the number of possible CCF combinations with k components of which at least a are in the first unit. It can be noticed that

$$P(m\ fail\ in\ unit\ 1 \mid m\ fail\ in\ unit\ 2) = \frac{\widehat{Pmu}(m,m,m)}{\widehat{Pmu}(m,0,m)} = \frac{\widehat{Psg}(2m)}{\widehat{Psg}(m)}.$$

7.4 Correlation of fragilities due to external hazards

In external event analysis, the fragility of each relevant SSC to the external event needs to be analysed. The fragility is typically represented as a curve which represents how the conditional failure probability of the SSC depends on the size of the external hazard. The fragility curves can be adapted into the PSA model as basic events representing the conditional failure probabilities. In the external event scenario, failures of certain components can be assumed correlated, e.g. identical components, components in the same location or components in similar position in similar buildings.

Considering a single unit, significant correlations should be modelled in the single-unit PSA.

In site PSA, the correlation modelling needs to be expanded to cover components in all units. The correlation modelling can be quite complicated, but the principles used in single-unit analysis should be quite well applicable also to the multi-unit case.

The seismic PSA implementation guide (EPRI 2003) provides guidelines concerning seismic events. However, other external events should be covered in the analysis as well.

7.5 Accident propagation between units

A severe accident with e.g. fire, explosion and radioactive release has the potential to affect other reactor units /sources of radioactivity. The conditional probabilities for such effects (propagation) given particular events or conditions in the originating unit are needed. The case has to be defined clearly concerning

- the conditions in the originating unit
- the effects in other units.

Estimation of the probability is very case specific requiring e.g. explosion or fire analyses. Further guidance for such assessment has not been within the scope of this study.

7.6 Phenomena

By inter-unit phenomena dependencies, we mean the state-of-the knowledge dependencies that can exist between the probabilities of certain phenomenological events at different but identical

units. Typical examples of such are possible phenomena in reactor pressure vessel or reactor containment under severe accident conditions.[5]

In multi-unit PSA context, the question is that what the probability that the same phenomenon occurs in multiple units under same severe accident conditions is. It should be noted here that we do *not* assume any physical, causal dependency between the phenomenological events. The probabilistic dependency thus only exists due to the uncertainty concerning the probability of the event.

In this section, we provide two approaches to assess dependencies between phenomenological events. In the first approach, two events are interpreted to be coupled by the common epistemic uncertainty related to the estimation of the probability of the event. This is called state-of-knowledge (SOK) dependency or correlation (Haim 1993), and it should be a standard part of the parametric uncertainty analysis for PSA (ASME 2009).

In the second approach, a phenomenological event is interpreted to be caused by some load which exceeds the strength of some part of the unit. Load and strength are uncertain random variables, but a coupling between units exists if the random variables are correlated. This is a kind of SOK dependency, but it has also a physical interpretation. Load-strength model has been applied e.g. in CCF modelling (Mankamo 2017).

7.6.1 Modelling of phenomenological dependencies by means of state-of-knowledge correlation

Let A_i denote the event that the phenomenon happens at unit i, $i = 1,2$. The phenomenon probability is same for both units,

$$P(A_i) = p.$$

The state-of-knowledge dependency between A_1 and A_2 can be assessed by postulating some uncertainty distribution for p, denoted here by $f(p)$. Without loss of any generality, we can define that it is a beta-distribution, $f(p) = B(\alpha, \beta)$.

In the single-unit PSA, we normally use the mean value of p as the point value

$$P(A_i) = \int p f(p)\, dp = \frac{\alpha}{\alpha+\beta}.$$

In the multi-unit PSA, we need to assess the following quantity

$$P(A_1 \cap A_2) = \int p^2 f(p)\, dp = \frac{\alpha}{\alpha+\beta} \cdot \frac{\alpha+1}{\alpha+\beta+1}.$$

Generally, formula above yields a probability for the two-unit event which is higher than square of the single-unit phenomenon probability. Only in case of no uncertainty, which corresponds with α and β approaching infinity, we have "no dependency",

$$P(A_1 \cap A_2) = P(A_1)P(A_2) = p^2.$$

Another extreme case is if we think that the phenomenon either happens with full certainty or cannot happen at all, but we do not know which statement is true. In terms of beta distributions, this corresponds with α and β approaching 0. In this case,

$$P(A_1 \cap A_2) = P(A_1) = P(A_2) = p.$$

From the multi-unit perspective, we have thus three possibilities to represent the state-of-knowledge dependency

- No dependency (purely aleatory uncertainty)
- Some dependency (aleatory and epistemic uncertainty)

[5] It should be noted that the issue with phenomenological uncertainties is by no means limited to level 2 PSA, but same issue appears in many assessments in level 1 PSA. For instance, if the two units have some identical software-based systems, one might speculate whether same SW fault will occur at both units if the triggering conditions are same.

- Full dependency (purely epistemic uncertainty).

The assessment of degree of dependency is challenging since there is no data to support the judgements. One can assume that no dependency is too optimistic (some epistemic uncertainty always exists), while full dependency is too conservative (triggering conditions are never fully identical). Some guidance can be taken from the uncertainty distributions defined for the probability parameters of concern.

Figure 7-1 presents how the conditional probability, $P(A_2|A_1)$ behaves as a function of the single event probability $P(A_1)$ and α-parameter of the beta distribution.

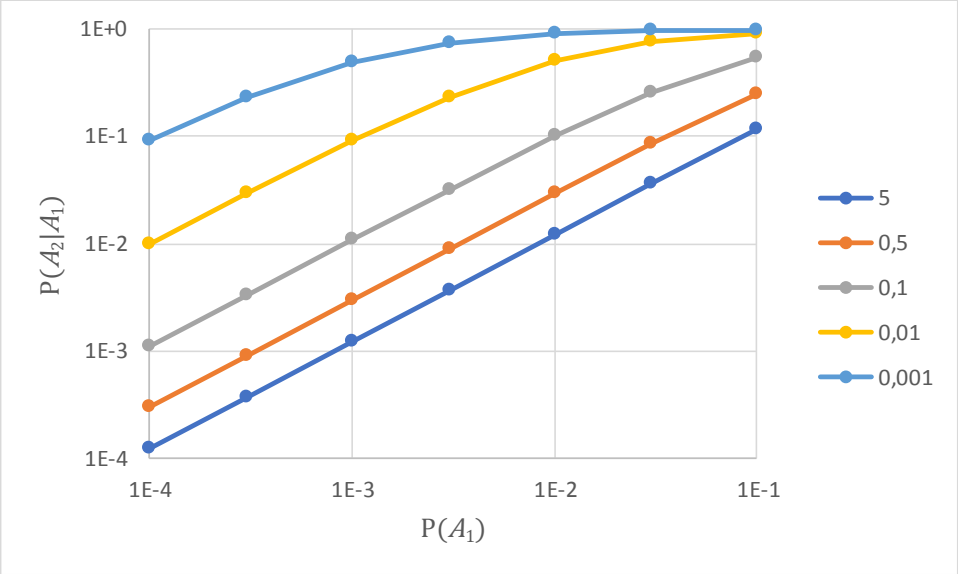


Figure 7-1 – Conditional probability of the second event, A_2, as a function of the probability of the first event, A_1, and the degree of epistemic uncertainty measured by the α-parameter of beta distribution (α = 5, 0,5, 0,1, 0,01, 0,001).

7.6.2 Modelling of phenomenological dependences by means of common load model

In the common load model, the probability of failure of a component is assumed to be given by a situation where a load, L, exceeds the strength, S, of the component

$$P(\text{failure}) = P(L > S) = P(L - S > 0).$$

A dependency between failures of multiple components is modelled by assuming component specific loads and strengths as correlated random variables. Degree of dependency can be associated with the degree of correlation.

Here we assume that load-strength dependency can be modelled by the basic common load model, which is a simplified and original form of the extended common load model (Mankamo 1977, 2017). In this model, the load is a common random variable, L, while strengths are component-specific independent and identically distributed random variables, $S_i, i = 1, \dots, n$. In the basic common load model, both L and S_i are normally distributed with mean values μ_L, μ_S and variances σ_L^2, σ_S^2.

The difference $Y_i = L - S_i$ is also normally distributed with a mean value

$$\mu_Y = \mu_L - \mu_S,$$

and variance

$$\sigma_Y^2 = \sigma_L^2 + \sigma_S^2.$$

The probability of multiple failures is obtained by the formula

$$P(\text{n components fail}) = P(L > S_1, \ldots, L > S_n) = P(Y_1 > 0, \ldots, Y_n > 0),$$

where $Y_i, i = 1, \ldots, n$, are correlated normally distributed random variables, i.e., it is a matter of a multivariate normal distribution.

In a practical application, the model can be re-parametrised into two parameters[6]:

- single failure parameter, $p_1 = P(L > S_i) = 1 - \Phi_Y(0)$,
- correlation coefficient $\rho = \frac{\sigma_L^2}{\sigma_L^2 + \sigma_S^2}$.

Similar to the assessment approach described in the previous section, we have three possibilities to represent the degree of dependency

- No dependency, $\rho = 0$. This is equivalent to zero variance for the load variable.
- Some dependency, $0 < \rho < 1$.
- Full dependency, $\rho = 1$. This is equivalent to zero variance for the strength variable.

Even for this approach, it can be difficult to assess the degree of dependency (a value for the correlation coefficient).

Figure 7-2 presents how the conditional probability, $P(A_2|A_1)$ behaves as a function of the single event probability $P(A_1)$ and the correlation coefficient.

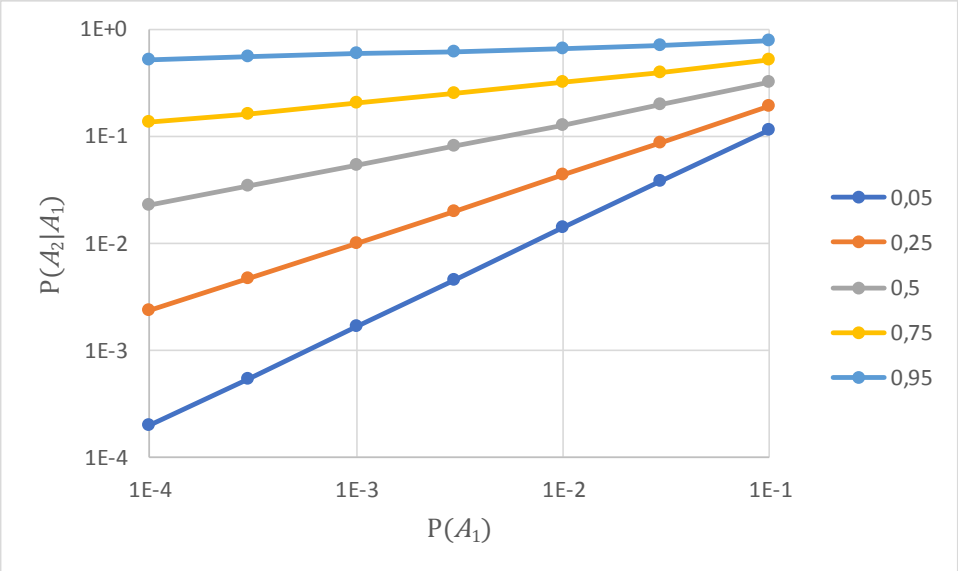


Figure 7-2 –. Conditional probability of the second event, A_2, as a function of the probability of the first event, A_1, and the correlation coefficient (ρ = 0,05, 0,25, 0,5, 0,75, 0,95).

6 In the common load model (Mankamo 2017), the mean values are fixed $\mu_Y = \mu_L - \mu_S = -1$.

8 Human reliability analysis

8.1 Overview of HRA in a site PSA perspective

Human reliability analysis is an important element in the 'traditional' PSA model for a single unit. Human failure events (HFEs) are identified, analysed and modelled for an accident event. Performance shaping factors (PSF) are evaluated for the accident scenarios for the single-unit for each action. HRA dependencies are also considered for the multiple human actions taken in sequence by the plant personnel in each accident scenario.

For multi-unit risk, HRA will continue to play an important role in the analysis. A few pilot studies have been performed (Bareith et al. 2016) (Le Duy et al. 2014) or are being performed for multi-unit HRA issues (Germain et al. 2017). A number of challenging PSFs were identified in these studies, e.g. shared resources, shift control from operators in the main control room (MCR) to emergency response team, use of Severe Accident Management Guidelines (SAMGs), etc. However, no systematic approach to deal with multi-unit HRA issues has been identified.

In general, HRA methodologies developed and used in internal events analysis will have to be modified for intended applications in multi-unit PSA. HRA methodologies developed for external event scenarios, if available, could be a good starting point for multi-unit issues. Multi-unit HRA will need to put more emphasis on organizational and management aspects in the analysis. These factors need to be included not only in quantification, but also in the task analysis and modelling. In the multi-unit accident scenarios, the existing human actions should be re-evaluated considering the site conditions, unit status and the challenging PSFs.

The degree of added complexity for multi-unit accidents will depend greatly upon the amount of interdependence between the individual units. This interdependence may come from the nature of the initiating event, the amount of shared systems/equipment or the amount of shared resources.

From a human reliability analysis point of view, the following information should be collected as the basis to understand the additional challenges in the multi-unit scenario:

- Constrained human resources
    - Increased workload for the decision makers (Emergency Response Organization Director / Technical support centre): number of units managed / supervised;
    - Number of control room operators and field operators by unit;
    - Any safety engineer: on site or on call, arrival time;
    - Time rigging for on-call staff (recovery actions)
- Additional complexity in managing the accident from multiple locations (MCR, TSCs, ERO centre) and requirements to communication and coordination.
- Shared system prioritization (This will be considered in the shared system analysis within the system fault tree structure)
- Prioritizing the deployment of portable equipment
    - What are the impacts on the time to deploy portable emergency mitigation equipment (EME) due to prioritization decisions and constrained resources?
- Reduced time available for some mitigation actions due to delays in communication and decision making in multi-unit event scenarios, and due to e.g., more demanding evaluations of pros and cons of actions, prioritization of shared human resources
- Training and experiences on the decision making and use of EMEs
- Validated plant specific procedures available to cope with the multi-unit scenarios

- Challenges on the human-machine interfaces, e.g. the reductions in instrumentation and lighting
- Impact from radiation/contamination from a damaged unit to the human actions at an adjacent unit in a different phase of accident progression
- Extreme environmental conditions impact to the field workers, including those from the initial event and any secondary events

When these influences are considered, the human error probabilities (HEPs) would be in general higher for some of the Human Failure Events (HFEs) in each unit PSA model. These influences can be considered by combining the additional PSFs into one penalty factor as a multiplier to the original HEP and/or by dependency evaluation. For dependency evaluation, a suitable dependency level is chosen and the HEP is adjusted to the corresponding dependency level. The dependency approach is not considered sufficient on its own, due to that an individual HFE might be influenced by the multi-unit environment. One may, however, have to explicitly consider dependencies between HFEs for different units.

Most scenarios, especially for internal events and internal hazards include well elaborated human actions in a controlled control room environment. Multi-unit scenarios are likely to be due to external hazards that introduce highly dynamic and unfriendly circumstances, during which the key human actions will be performed. Relevant actions need to be identified and analysed. Most of the human actions should have been modelled in the single-unit PSA. Some additional new human actions may need to be modelled for the multi-unit accident scenarios.

The proposed approaches, i.e. reassessment of PSFs with a penalty factor or dependency treatment, are based on the assumption that there are single-unit PSA and HRA models for each unit that can be used. No new HRA method for the analysis will be proposed. Instead, the focus will be on how to update the existing analysis, independent of the HRA methods applied in the existing studies. The procedure includes the following steps

(1) identification of existing relevant operator actions for identified initiators,

(2) identification of new actions (if any), and

(3) Characterization of multi-unit conditions and HFE re-quantification using penalty factor or dependency treatment.

Individual category A pre-initiator HFEs remain unchanged as the actions are performed under normal conditions and they are not related to multi-unit scenarios. Possible dependencies between multiple category A HFEs (the combinations) may exist. When needed, such dependencies can be evaluated considering the similarity amongst the category A actions in a similar way as in the single-unit analysis (He, 2016). Category B initiator HFEs are seldom modelled in the plant, though the potential for such actions need to be studied as part of the initiating events analysis. This leaves the focus of the multi-unit human reliability analysis to category C post-initiator HFEs.

8.2 Identification of relevant operator actions

Given a specific initiating event, existing operator actions and the corresponding HFEs are identified. The EOP actions by operators in the main control room directly after the initiating event are not likely to be much influenced by the multi-unit scenarios. The EOP actions performed locally and especially by shared personnel could be influenced by the multi-unit scenarios. These short time window actions, except for those actions performed by the shared local personnel, will therefore keep their original HEPs and can be screened out from further multi-unit evaluation.

The focus for the multi-unit evaluation is then the major HFEs (see 5.2.2 concerning relevant dependencies). In this step, the qualitative and quantitative evaluation of the existing HFEs should be collected.

8.3 Identification of new human actions

The following considerations, adjusted from the study by (Germain et al 2017), should be made in determining what new human failure events should be modelled (not an all-inclusive list):

- Are there additional opportunities for human errors due to a shared main control room? Are there additional opportunities for recovery afforded by other-unit operator resources in the main control room?
- Are there additional opportunities for human errors in deciding where to deploy shared systems initially or when to alternate between units, such as a shared emergency diesel generator (EDG) or makeup water systems?
- Is there an opportunity for human error for field workers performing a task on the wrong unit?
- If a shared TSC is managing multiple accidents at different accident phases from the same location, are there opportunities for human error induced by staff changing focus between units?
- How should decisions directed from SAMG related to mitigation strategies be modelled?

8.4 Quantification methods for operator actions

Two approaches are described as they are implemented in two pilot studies. The first approach is the PSF Penalty Factor which combines the additional PSFs as a multiplier to the original HEP. The second approach is to use dependency treatment. For dependency evaluation, a suitable dependency level is to be chosen for the multiple HFEs in the same cut sets and the HEP is adjusted to the corresponding dependency level.

8.4.1 PSF approach to quantify operator actions

8.4.1.1 Quantification

Re-quantification of existing HFEs will be performed by combining the additional PSFs into one penalty factor based on an EDF approach developed for multi-unit PSA (Le Duy et al. 2014). EDF proposed the use of a penalty factor with 3 levels for the risk significant human actions. The penalty factor is estimated by expert judgement based on a number of factors.

In this study the following five penalty factor levels (multipliers) are proposed:

- X1 (none). No need to increase HEP.
- X2 (low). The influence is low
- X5 (medium). The influence is medium based on the additional challenges
- X10 (high). The influence is high.
- HEP=1. The influence is extremely high and the action is considered as impossible.

Expert judgement is used to combine the additional challenges (based on information collected according to section 8.1) into an appropriate penalty factor. The preliminary expert judgement criteria include:

- If any of the influence factors show that one human action is not feasible anymore, its HEP would be 1. For example, there is no operator available, or the location is not accessible, etc.
- If additional challenges exist, the penalty factor would be selected (2, 5, or 10) based on the influence level (low, medium, or high). This would be judged based on the number of applicable challenges and the degree of influence. This process is very much expert judgement based, however a set of rules could be defined.

- If no additional challenge exists, no penalty factor needs to be assumed (1)

Penalty factors for different types of human actions are showed in Table 8.1. A decision tree is made to illustrate the penalty factors, as showed in Figure 8-1.

Table 8.1 – Penalty factors for HEPs for different human actions (the final HEP should be 1 when HEP*penalty factor is large than 1)

Penalty factor	Who and what	Where	Basis for Penalty factors (assumptions)
1	MCR staff diagnoses and performs the procedure (EOP or SAMG) based human action	In MCR	Decisions and action are performed by MCR staff. The available time is the same.
2	MCR staff diagnoses and performs the procedure (EOP or SAMG) based human action	Outside MCR, locally	Decisions and action are performed by MCR staff. Potential radiation/contamination from a damaged unit, however it is assumed that appropriate personal protective equipment (PPE) is available for staff.
2	Shared TSC staff performs recovery actions	In MCR	Supervision staff has good training level, however they are shared by multiple units and the available time would be reduced.
5	MCR staff diagnoses and asks shared field staff to perform local action	Outside MCR, locally	Field staff has good training level. Potential radiation/contamination from a damaged unit, however it is assumed that appropriate PPE is available for staff. There might be more resource constrains for local field staff if they are shared by multiple units.
5	Shared decision maker diagnoses and asks unit operators to perform SAMG based human action	In or outside MCR	See the multi-unit scenario challenges discussed in section 8.1: shared decision maker, SAMG, training and experience level, communications, etc.
10	Shared plant decision maker diagnoses and asks shared field staff perform actions	Outside MCR, locally	See the multi-unit scenario challenges discussed in section 8.1: shared decision maker and field staff, SAMG, training and experience level, communications, etc.

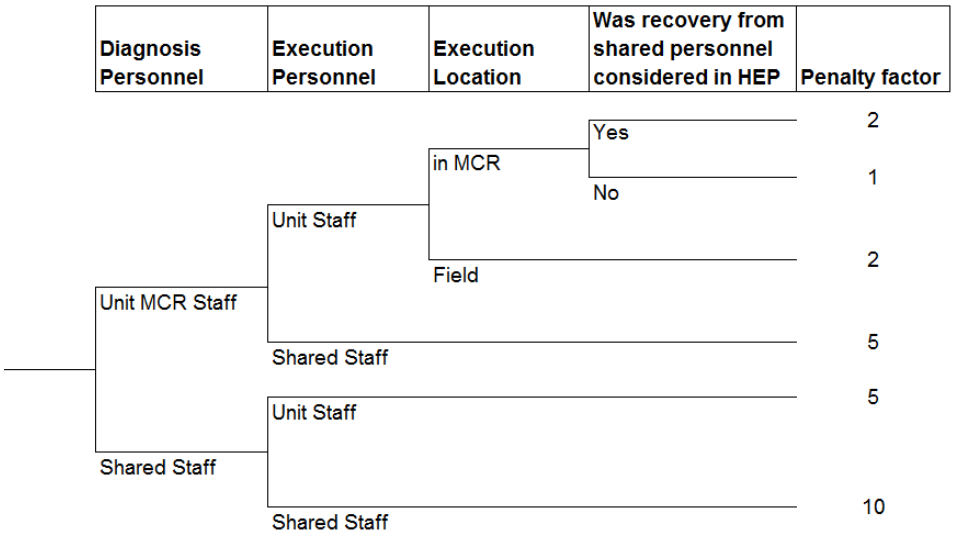


Figure 8-1 – Decision tree for Penalty Factors (the final HEP should be 1 when HEP*Penalty factor is large than 1).

If new HFEs are identified, they are suggested to be quantified with direct expert judgement or by the same HRA method as applied for the existing HFEs. A penalty factor can then be applied if these factors are not yet reflected in the quantification.

As level 1 PSA typically deals with the accident for 24 hours, most of the existing Category C human actions are likely to be performed by operators in the main control room (MCR) or locally. It is reasonable to assume that these actions are less influenced by the accident progression in other units. For the level 2 and SAMG case and with the shared decision maker, the influence from other units could be significant.

8.4.1.2 Discussion

Penalty factor approach aims to consider the additional challenges from multi-unit scenarios. One penalty factor will be derived for a specific human failure event according to the Table 8.1 or Figure 8-1. After this consideration, it is assumed there is no need for further multi-unit dependency treatment.

This is a simplified approach and also conservative as the penalty factor is assumed considering the neighbouring units are in severe conditions. The penalty factors are different for different category C human actions based on the potential influences from other units.

One drawback of the penalty factor is that it could be non-conservative for the same actions taken by a same group of people (e.g. TSC) in the multi-units for similar conditions. In this case if the TSC fails to make correct decision for unit 1, they will have higher probability to fail in unit 2. Such situation, if it is found in the risk significant MCSs, should be treated using dependency treatment.

8.4.2 Dependency approach for operator actions

8.4.2.1 Quantification

For dependency evaluation, a suitable dependency level is to be chosen for the multiple HFEs in the same cut sets and then the HEP is adjusted to the corresponding dependency level. Dependency approach is in this respect equivalent to the usual handling of operator action dependences in SUPSA, see e.g., THERP (Swain & Guttman 1983) and SPAR-H (Gertman et al. 2005).

In the SUPSA applications, the dependency case that is usually considered is the dependency between two consecutive human failure events related to same safety function, e.g., recovery of residual heat removal by means of two different systems. With regard to such examples, we refer to the usual HRA practice.

In the MUPSA applications, the main question is how to handle a possible dependency between an HFE1 at unit 1 and HFE2 at unit 2. We distinguish two different cases: 1) HFE1 and HFE2 are consecutive events, and 2) HFE1 and HFE2 are two identical events at different units.

The first case, where HFE1 and HFE2 are consecutive events, is in principal similar to typical SUPSA HFE dependency cases. The solution is to first determine the order of events (if not obvious) and then split the case into two subcases: a) p(HFE2 ✠ HFE1) and b) p(HFE2 ✠ not HFE1). Assessment of conditional probabilities can follow same principles as in SUPSA applications, i.e., depending on degree of common personnel, common cues, close in time, etc. factors, p(HFE2 ✠ HFE1) can be adjusted, see e.g. (Swain & Guttman 1983).

For the second case, two identical HFEs at different units, the degree of dependency depends on the degree of shared actors involved in HFEs. Following the usual HFE model, shared actors can be a) the decision makers, b) the crew performing the execution of the decision or c) an organizational unit that can recover a missed action.

Ideally, the HFEs have been analysed in SUPSA in such a manner that the contribution of each actor (diagnosis, execution and recovery) to the overall HEP is obtained from SUPSA. In this case, the dependency between identical HFEs with partially common actors can be assessed "exactly" by rules of probability calculus.

Often the information provided in SUPSA is not sufficient for an explicit assessment of dependencies. In that case, some judgmental rules can be applied. Table 8.2 - presents an example how to choose a dependency category. The rules are based on a general HFE model for category C actions that the action fails if the diagnosis and decision making or the execution fails and if, in addition, the recovery fails.

"Shared" should be understood to mean that personnel are partly common but not fully common. For instance, decision making can be usually assumed to be unit-specific, yet for some actions diagnosis of the situation can be common. Therefore, a medium degree of dependency is assumed when a common/shared diagnosis is assumed. High degree of dependency is assumed for local actions performed by shared personnel. For these scenarios, it can be complicated to coordinate resources, e.g., if there is not enough time w.r.t. to the complexity of the execution.

Column 3 of Table 8.2 presents an example how the qualitative dependency category could be assessed. It can be noticed that the dependency category formulas are close to conditional failure probabilities suggested in THERP (Swain & Guttman 1983), especially with regard to high and medium degree dependencies for typical HEP values. With regard to low dependency, THERP suggests clearly higher conditional probability than the rule suggested in Table 8.2 - .

Table 8.2 - Simplified assessment of dependency categories for type C actions applied in one of the pilot studies. Actions A_1 and A_2 refer to identical HFEs modelled in unit-specific PSAs, with a human error probability p_a estimated in SUPSA.

Dependency category	Criterion/*motivation*	$P(A_1 \cdot A_2)$
Zero	No common actors	$p_a \cdot p_a$
Low	Shared recovery *In this case, there is some site level organisational unit, such as TSC, that have not participated in diagnosis, but can follow-up the decisions made by units. Some degree of dependency can be assumed, though it is likely that the scenarios are not exactly identical at both units.*	$2p_a \cdot p_a$
Medium	Shared diagnosis *In this case, there is some site level organisational unit, such as TSC, that participates in diagnosis by supporting the main control room crew. Some degree of dependency can be assumed, though it is likely that the scenarios are not exactly identical at both units.*	$\sqrt{p_a} \cdot p_a$
High	Shared personnel for execution *In this case, local actions are performed by same personnel. Typical MUPSA scenarios (external hazards) are such that conditions for execution are same at both units. If one fails, then it is likely that the other fails.*	$0{,}5 \cdot p_a$
Full	Common action for both units	p_a

8.4.2.2 Discussion

The approach outlined above assumes that an HFE is decomposed into the steps: diagnosis, execution and recovery. If there are common actors in any of those three steps, a dependency assessment should be considered. If the steps have been assessed explicitly (actors involved in each step have been identified explicitly and each step is quantified separately) in the single-unit PSA/HRA, the multi-unit assessment could be assessed straightforwardly by considering common steps as fully dependent. If such a detailed analysis is not available, Table 8.2 suggests one possible approach, which, however, should be regarded as a screening approach, and a more detailed, explicit analysis of action dependencies is always recommended for risk-significant scenarios.

To be consistent, the dependency assessment should follow the same assessment principle as applied in a single-unit PSA/HRA. In practice, dependency assessments of single-unit PSA/HRA are not necessarily fully applicable for multi-unit cases, but nevertheless that should be used as a reference to the extent possible.

Dependency assessment and penalty factors could be seen complementary approaches that address different aspects of dependencies between HFEs in multi-unit scenarios. The penalty factor approach is a simplified approach to address the modified PSFs for actions in a multi-unit scenario compared to a single-unit scenario. See discussions in 8.4.1.2. The proposed above dependency assessment addresses explicitly the dependency caused by the involvement of same actors (operators, staff) in identical HFEs in multiple units.

9 Extending single-unit PSA models

The single-unit PSAs should cover all risk significant scenarios regarding core damage frequency. By extension of single-unit PSA models, we mean complementary modelling done to implement consistently (from the risk metrics perspective) multi-unit scenarios into the single-unit PSA.

From a multi-unit perspective, the challenges for the single unit are shared resources affecting equipment availability or operator actions. Therefore, the extension of the single-unit PSAs shall specifically study the sequences where shared systems (that cannot be accounted for at all units) may be used at another unit or where operator actions may have another failure probability.

There are different approaches to represent a multi-unit event in the single-unit PSA.

One approach is to define these sequences as sub-set of initiating events. For example, loss of offsite power and CCF between all diesels at two units may mean that a mobile diesel is not available at both units simultaneously. In this case a definition of an initiating event *loss of offsite power and simultaneous loss of all diesels* would make it possible to consider this by using a probability of availability of the mobile diesel of 0.5 in addition to the mobile diesel failure probability.

Another approach would be to represent the scenarios that could affect the probability directly in the fault trees. This would be accomplished by for example adding basic events representing the likelihood of the scenario, and basic events representing the availability of the equipment in this specific scenario.

10 Quantification of multi-unit risks

10.1 Approach for computing site level specific risk metrics

10.1.1 General approach to quantification of multi-unit risk metrics

The quantification of the different multi-unit risk metrics are based on a number of interrelated TOP events for each unit; TOP1, TOP2….,TOPN.

The risk metrics of interest may concern either scenarios occurring at the same time (for example multi-unit core damage frequency) or the total risk of the site (for example site core damage frequency).

This can be illustrated by:

- Multi-unit core damage - MUCDF: TOP(1&2&..&N) = TOP1 & TOP2 & … & TOPN
- Site core damage - SCDF: TOP(1+2+…+N) = TOP1 + TOP2 + … + TOPN

The quantification of the risk metrics follows the same Boolean laws and probability theory as in the single unit PSA. The application is exemplified in the following section using a two-unit site. An example of quantifying various two-unit risk metrics is provided in Appendix B.

10.1.2 Simplified, two-unit site

The multi-unit core damage frequency for a specific initiator (for a site having two units) can be calculated by:

$$MUCDF_{IE} = F_{IE} \times p(\mathrm{CD}_{unit1}|\mathrm{IE}) \times p(\mathrm{CD}_{unit2}|\mathrm{IE}\ \&\ \mathrm{CD}_{unit1})$$

where:

F_{IE} is the frequency for the initiating event studied,

$p(\mathrm{CD}_{unit1}|\mathrm{IE})$ is the conditional core damage probability of unit 1 given the initiating event,

$p(\mathrm{CD}_{unit2}|\mathrm{IE}\ \&\ \mathrm{CD}_{unit1})$ is the conditional core damage probability of unit 2 given the initiating event and core damage on unit 1.

The approaches that can be used will have to meet following characteristics:

- Enable consideration of different levels of dependency (ranging from no dependency to full dependency)
- Enable consideration of multiple dependencies (more than one dependency at a time can affect the results)
- Allow for modification of operator action probability, if such modification is relevant in some specific sequences
- Can handle shared systems (if a system can only be taken credit for in one unit at a time)

It is also desirable that the method:

- Can estimate the importance of each dependency
- Does not require a complete and integrated model of all units (for simplicity and maintainability)

In this method report, it has been considered best if the PSA models of the individual units can remain as individual models. Hence, the method applied should operate on the results produced from the individual units' PSA.

Two possible quantification approaches to calculate the MUCDF per MUIE are proposed in Appendix A and tested in the pilot studies. These methods are outlined and discussed in appendix A.

The total MUCDF of the two-unit site can be calculated by summing the MUCDF values of different initiating events:

$$MUCDF = \sum_{IE=1}^{m} MUCDF_{IE},$$

where m is the number of initiating events.

The CDF values of individual units can be calculated in the normal way from the PSA models. The site CDF can finally be calculated based on the CDFs of the individual units (total CDFs including multi-unit contributions) and MUCDF values:

$$SCDF = CDF_{unit1} + CDF_{unit2} - MUCDF.$$

10.1.3 Importance analysis of multi-unit events

The Fussell-Vesely (FV) risk importance for each dependency should preferably be calculated in the multi-unit analysis. The calculations of the FV for a dependency is easily computed by calculating the top result involving the dependency in question, and relate that to the total multi-unit risk measure in question.

10.2 Level 2 PSA

Quantification process for level 2 PSA follows same principles as for level 1 PSA. Especially, if the quantification is limited to a single risk metric such as the site level frequency for an unacceptable release, the quantification process is equal to the description in the previous subsection. If the

aim is to cover more release categories or if the aim is to use a single RC as surrogate for level 3 PSA, there are more aspects to be considered as discussed below.

The starting point for quantifying a spectrum of release category frequencies is the fact that each single-unit level 2 PSA event sequence is associated with one and only one source term and associated release category and that the end state of the multi-unit level 2 PSA sequence is a combination of single-unit source terms and associated release categories. Basically, it is thus a matter of book keeping of results from multiple quantifications. By applying addition and subtraction operations in an appropriate manner various multi-unit risk metrics are obtained. This is demonstrated in Appendix B.

In the SITRON risk metrics report (Holmberg 2017), it is suggested that multi-unit release category is defined based on the aggregated size of the release and time point of the earliest release. One important issue here is that the significance of timing of multiple releases is not self-evident. It is commonly assumed that early release is worse than late release. From the success countermeasures such as evacuation point of view, this is primarily true. On the other hand, if release happen during a longer time window, it is more likely that radionuclides will be spread into a larger area (due to changed wind directions), meaning that a larger area will be contaminated, and even that evacuation might not be fully successful. So, when using level 2 PSA results as surrogates for level 3 PSA, one might need to check the dominating source terms combinations (including timing information) which lay behind release category frequencies.

11 Conclusions

An approach for estimating multi-unit risk has been outlined. The approach starts from the identification of multi-unit initiators and the POS combinations where the initiators may be relevant. The identification of multi-unit dependencies uses a combination of qualitative and quantitative approaches, considering dependencies relevant for the identified initiators. The qualitative identification serves as a basis for the quantitative selection and also as assurance that relevant dependencies are not overlooked due to simplifications in the existing single-unit PSA.

An approach for quantitative screening is suggested. The analysis of selected dependencies will need support from data analysis, and the human reliability assessment need to be revisited to consider multi-unit aspects.

The single-unit PSA model should already consider limitations in the availability of shared resources and impact of multi-unit dependencies on operator actions. However, there may still be a need to re-assess the data for specific scenarios considered in the multi-unit risk assessment.

Given relevant reliability data, the quantification of site level core damage frequency is straightforward and can be achieved using the single unit PSA model. Computation of plant level estimates of large release is also straight forward, but there are more possibilities of what risk metrics are quantified than in level 1.

This report together with the pilot studies conducted have demonstrated that it is possible to quantify the multi-unit risk metrics of relevance using the existing PSA models within the Nordic countries. Hence, there is no need to create an integrated PSA model for multiple units.

12 References

ASME. 2009. Addenda to ASME/ANS RA-S–2008. *Standard for level 1/large early release frequency probabilistic risk assessment for nuclear power plant applications*, ASME/ANS RA-Sa-2009, the American Society of Mechanical Engineers.

ASME. 2014. ASME/ANS RA-S-1.2-2014: *Severe accident progression and radiological release (level 2) PRA standard for nuclear power plant applications for light water reactors (LWRs)*, the American Society of Mechanical Engineers. (trial use standard)

Bareith, A., Hollo, D., Karsa, Z., Siklossy, P., Siklossy, T. *A pilot study on developing a site risk model*. In Proc. of 13th International Conference on Probabilistic Safety Assessment and Management (PSAM 13), 2–7 October, 2016, Seoul, Korea. Paper A-420.

Bäckström, O., Häggström, A., He, X., Holmberg, J.-E, Tyrväinen, T., *SITRON – Method development*. Report 212634-R-001, Lloyds Register Consulting - Energy Ab, Stockholm, 2018

Electric Power Research Institute (EPRI). 2003. *Seismic probabilistic risk assessment implementation guide*, Palo Alto, California, USA.

Electric Power Research Institute (EPRI). 2013. *Spent fuel pool risk assessment integration framework (mark I and II BWRs) and pilot plant application,* Palo Alto, California, USA.

Electric Power Research Institute (EPRI). 2014. *PWR spent fuel pool risk assessment integration framework and pilot plant application,* Palo Alto, California, USA.

Germain S., Boring R., Banaseanu G., etc. *Multi-Unit Considerations for Human Reliability Analysis*, PSAM Topical Conference on Human Reliability, Quantitative Human Factors, and Risk Management, 7 - 9 June 2017, Munich, Germany.

Gertman, D., Blackman, H., Marble, J. , Byers, J., Smith, C. 2005. The SPAR-H Human Reliability Analysis Method, NUREG/CR-6883. U.S. Nuclear Regulatory Commission, Washington, D.C.

Haim, M. 1993. *The impact of new evidence on state-of-knowledge dependence*, Reliability Engineering and System Safety 40, 1–4.

He X. *Dependences in HRA*. NPSAG Report 41-001-01, 2016.

Holmberg, J.-E. *SITRON - Risk metrics*. Report 14124_R005, Risk Pilot Ab, Espoo, 2017.

Hudson, D. *The U.S. Nuclear Regulatory Commission's Proposed Approach to Developing an Integrated Site Probabilistic Risk Assessment (PRA) Model*, OECD/NEA WGRISK International Workshop on Status of Site Level PSA (including Multi-Unit PSA) Developments, Munich, July 18-20, 2018, Paper II-2

Håkansson, M. 2017. Action item 43-09 (42-05, 41-04, 40-16): Summary of workshops on Multi-unit events. ICDE Work note. Draft 2017-03-10 (limited distribution).

Johnson, N., Schroeder, J.A. 2016. *Analysis of loss-of-offsite-power events*, 1987-2015, INL/EXT-16-39575, Idaho National Laboratory, Idaho, USA.

Kim, D.-S., Park, J.H., Lim, H.-G. *An approach to inter-unit common cause failure modelling for multi-unit PSA*, International workshop on status of site level PSA (including multi-unit PSA) developments, 18-20 July 2018, Munich, Germany.

Le Duy, T.D., Vasseur, D., Serdet, E. *Multi Units Probabilistic Safety Assessment: Methodological elements suggested by EDF R&D*. Probabilistic Safety Assessment and Management PSAM 12, June 2014, Honolulu, Hawaii.

Le Duy, T.D., Vasseur, D. *A practical methodology for modeling and estimation of common cause failure parameters in multi-unit nuclear PSA model,* Reliability Engineering and System Safety 170, 159-174, 2018.

Mankamo, T. 2017. *Extended common load model: A tool for dependent failure modelling in highly redundant structures*. SSM report 2017:11, Strålsäkerhetsmyndigheten, Stockholm, Sweden.

Muhlheim, M. D., Wood R. T. *Design Strategies and Evaluation for Sharing Systems at Multi-Unit Plants Phase I*. ORNL/LTR/INERI-BRAZIL/06-01, Oak Ridge National Laboratory, 2007.

Schroer, S., Modarres, M. *An Event Classification Schema for Evaluating Site Risk in a Multi-Unit Nuclear Power Plant Probabilistic Risk Assessment*, Reliability Engineering and System Safety 117, 40–51, 2013.

Swain, A.D., Guttmann, H. E. 1983. Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications, Final Report, NUREG/CR-1278. U.S. Nuclear Regulatory Commission, Washington, D.C.

Tyrväinen, T., Häggström, A., Bäckström, O., Björkman, K. 2017. *A methodology for preliminary probabilistic multi-unit risk assessment*. VTT-R-00086-17, VTT Technical Research Centre of Finland Ltd, Espoo, Finland.

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

U.S.NRC. 2016. CCF Parameter Estimations, 2015 Update, http://nrcoe.inel.gov/resultsdb/ParamEstSpar/

Wierman, T.E., Rasmuson, D.M., Mosleh, A. 2007. *Common-cause failure database and analysis system: Event data collection, classification, and coding*. NUREG/CR-6268, Rev. 1 INL/EXT-07-12969, U.S. Nuclear regulatory commission, Division of risk assessment and special projects, Washington D.C., USA.

Appendix A

Description and comparison of two calculation approaches

Table of contents

Page

1 Introduction

This appendix presents and demonstrates the two calculation approaches used in the pilot studies. One sample model has been designed, representing a multi-unit PSA for two identical units.

2 Sample model

The sample model is a modified version of the EXPSA model that is normally installed with RiskSpectrum PSA software.

The evaluated (multi-unit) initiating event selected is LOOP.

The event tree for LOOP is presented in Figure A.1.

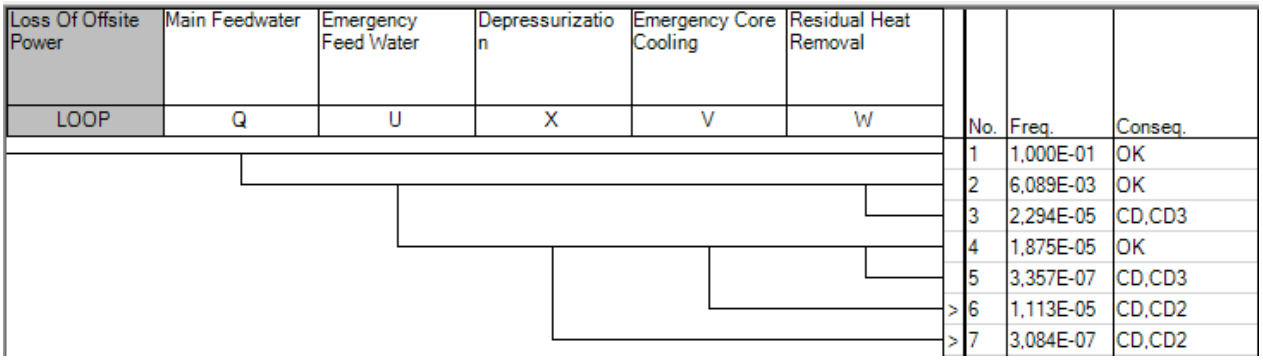


Figure A.1. LOOP Event Tree.

The main feedwater system is dependent upon a gas turbine (GT-01) in case of LOOP.

The emergency feedwater system (EFW) and the emergency core cooling (ECC) system are both relying upon diesel support (DG01 and DG02) in case of LOOP.

The depressurisation system is backed by batteries.

The residual heat removal is achieved by a RHR system (diesel backed) or it is assumed that it can be performed through a feed and bleed operation, that is performed by a system that has its own power supply (the probability is not affected by LOOP).

EFW, ECC and RHR are all relying upon the same component cooling system and corresponding service water system. EFW, ECC and RHR are two train systems.

2.1 Results of single unit PSA

The single unit PSA evaluation results in following MCS list, as in Figure A.2.

Top Event frequency F = 3,973E-06

No	Probability	%	Event 1	Event 2	Event 3	Event 4	Event 5
1	1,345E-06	33,84	!IE-LOOP	ACP-GT01-A	CCF-ACP-DG---A-ALL		
2	2,299E-07	05,79	!IE-LOOP	ACP-DG01-M	ACP-DG02-A	ACP-GT01-A	
3	2,299E-07	05,79	!IE-LOOP	ACP-DG01-A	ACP-DG02-M	ACP-GT01-A	
4	1,891E-07	04,76	!IE-LOOP	ACP-GT01-A	CCF-CCW-PM---A-ALL		
5	1,891E-07	04,76	!IE-LOOP	ACP-GT01-A	CCF-SWS-PM---A-ALL		
6	1,633E-07	04,11	!IE-LOOP	ACP-GT01-M	CCF-ACP-DG---A-ALL		
7	1,576E-07	03,97	!IE-LOOP	ACP-GT01-A	CCF-SWS-PM---D-ALL		
8	9,361E-08	02,36	!IE-LOOP	ACP-DG01-A	ACP-DG02-A	ACP-GT01-A	
9	7,844E-08	01,97	!IE-LOOP	ACP-GT01-A	CCF-RHR-PM---D-ALL	FEED&BLEED_____O	
10	4,492E-08	01,13	!IE-LOOP	ACP-GT01-A	CCF-EFW-PM---D-ALL	ECC_____O	
11	3,233E-08	00,81	!IE-LOOP	ACP-DG02-M	ACP-GT01-A	CCW-PM01-A	
12	3,233E-08	00,81	!IE-LOOP	ACP-DG02-M	ACP-GT01-A	SWS-PM01-A	
13	3,233E-08	00,81	!IE-LOOP	ACP-DG01-M	ACP-GT01-A	CCW-PM02-A	
14	3,233E-08	00,81	!IE-LOOP	ACP-DG01-M	ACP-GT01-A	SWS-PM02-A	
15	2,823E-08	00,71	!IE-LOOP	ACP-DG02-M	ACP-GT01-A	FEED&BLEED_____O	RHR-TR01-M
16	2,823E-08	00,71	!IE-LOOP	ACP-DG01-M	ACP-GT01-A	FEED&BLEED_____O	RHR-TR02-M
17	2,823E-08	00,71	!IE-LOOP	ACP-DG01-M	ACP-GT01-A	ECC_____O	EFW-TR02-M
18	2,823E-08	00,71	!IE-LOOP	ACP-DG02-M	ACP-GT01-A	ECC_____O	EFW-TR01-M
19	2,793E-08	00,70	!IE-LOOP	ACP-DG01-A	ACP-DG02-M	ACP-GT01-M	
20	2,793E-08	00,70	!IE-LOOP	ACP-DG01-M	ACP-DG02-A	ACP-GT01-M	
21	2,695E-08	00,68	!IE-LOOP	ACP-DG02-M	ACP-GT01-A	SWS-PM01-D	
22	2,695E-08	00,68	!IE-LOOP	ACP-DG01-M	ACP-GT01-A	SWS-PM02-D	
23	2,622E-08	00,66	!IE-LOOP	ACP-GT01-A	CCF-RHR-PM---A-ALL	FEED&BLEED_____O	
24	2,296E-08	00,58	!IE-LOOP	ACP-GT01-M	CCF-CCW-PM---A-ALL		
25	2,296E-08	00,58	!IE-LOOP	ACP-GT01-M	CCF-SWS-PM---A-ALL		
26	2,046E-08	00,52	!IE-LOOP	ACP-GT01-A	CCF-EFW-PM---A-ALL	ECC_____O	
27	1,914E-08	00,48	!IE-LOOP	ACP-GT01-M	CCF-SWS-PM---D-ALL		
28	1,877E-08	00,47	!IE-LOOP	ACP-GT01-A	CCF-CCW-PM---D-ALL		
29	1,341E-08	00,34	!IE-LOOP	ACP-DG01-M	ACP-GT01-A	FEED&BLEED_____O	RHR-PM02-D

Figure A.2. The single unit PSA evaluation results.

It shall be noticed that the probability of the failure to activate feed&bleed in the MCS list is its original probability (5E-2). As can be seen in the next section, this probability is increased to 2E-1 to exemplify a situation where the multi-unit risk may be affected in some specific sequences (compared to the single unit analysis).

2.2 Dependencies considered for the multi-unit evaluation

The evaluation of dependencies has resulted in Table A.1:

Table A.1. List of multi-unit dependencies to study

Multi-unit event	Modified probability in the multi-unit assessment	Comment
Diesels (failure to operate)	40% CCF is considered multi-unit CCF	Same type of equipment
EFW Pump (failure to start, failure to run)	40% CCF is considered multi-unit CCF	Same type of equipment
CCW Pumps (failure to start, failure to run)	40% CCF is considered multi-unit CCF	Same type of equipment
SWS Pumps (failure to start, failure to run)	40% CCF is considered multi-unit CCF	Same type of equipment
RHR Pumps (failure to start, failure to run)	40% CCF is considered multi-unit CCF	Same type of equipment
Gas Turbine (failure to operate, maintenance)	100% is considered multi-unit CCF	There is only one GT (shared GT). Note that the maintenance is considered also
ECC manual start, operator action	50% dependency is considered multi-unit risk	It is assumed that there is a dependency in how the operators have been trained to achieve the task
Feed&Bleed, operator action	Probability is increased to to 2E-1	Analysis: in LOOP sequences where GT fails, the technical support centre will be challenged by both units. Therefore the probability shall be increased in these sequences.

3 Presentation of the calculation approaches

3.1 Modelling of dependencies between basic events

There are two principal ways of modelling a dependency between basic events. Suppose that a basic event A_i of a single unit PSA (unit $i, i = 1,2$) has some degree of dependency between the units. One way is to split A_i into two exclusive events

$$A_i = A_i' \oplus A_c',$$

where A_i' represents the unit-specific event and A_c' the common event for both units. The simultaneous occurrence of A_i at both units is then

$$A_1 \cdot A_2 = (A_1' \cdot A_2') \oplus A_c',$$

and the probability

$$\pi' = P(A_c')/P(A_i)$$

shall correspond with the share of dependency between the units regarding this basic event.

Another way is to decompose A_i as a product of a common event and unit-specific event as follows

$$A_i = A_i'' \cdot A_c''.$$

The simultaneous occurrence of A_i at both units is in this case

$$A_1 \cdot A_2 = A_1'' \cdot A_2'' \cdot A_c''.$$

The share of dependency can be measured e.g. by the formula

$$\pi'' = P(A_1'' \cdot A_2'' \cdot A_c'')/P(A_i'' \cdot A_c'') = P(A_i''),$$

i.e., when $P(A_i'') = P(A_i)$ there is no dependency, and when $P(A_i'') = 1$ there is a full dependency. It should be noted that in this approach the basic events are assumed as independent events.

In the pilot studies two different approaches were applied. These are shortly described below and referred to as the *MCS list approach* and the *Multi-unit event combinations approach*. Sections 4 and 5 of this appendix are presenting the approaches applied on the small sample model described in section 2.

3.2 MCS list approach

In the MCS list approach, it is assumed that MCS lists of single-unit PSAs are correct representations of the combinations of basic events that lead to the top event (e.g. a core damage in level 1 PSA) for the respective unit. Correspondingly, combinations of two units' cut sets must be correct cut sets for the joint top event. The only tasks that have to be performed are the minimization of the combined cut set list and the evaluation of the frequency of each cut set combination. The first step is needed when there are full dependencies between some of the unit-specific basic events.

We denote the unit-specific minimal cut set lists as follows

$$\mathrm{TOP}^1 = \sum_{\mathrm{i}} \ \mathrm{K}_{\mathrm{i}}^1,$$

$$\mathrm{TOP}^2 = \sum_{\mathrm{j}} \ \mathrm{K}_{\mathrm{j}}^2,$$

where $\mathrm{K}_{\mathrm{i}}^1$ and $\mathrm{K}_{\mathrm{j}}^2$ are minimal cut sets for the unit-specific top events TOP^1 and TOP^2.

The minimal cut sets of the joint event TOP^{12} is directly obtained as the Boolean product

$$\mathrm{TOP}^{12} = \mathrm{TOP}^1 \cdot \mathrm{TOP}^2 = \left(\sum_{\mathrm{i}} \ \mathrm{K}_{\mathrm{i}}^1\right) \cdot \left(\sum_{\mathrm{j}} \ \mathrm{K}_{\mathrm{j}}^2\right).$$

For the quantification, we need to define rules how to treat each cut set combination $\mathrm{K}_{\mathrm{i}}^1 \cdot \mathrm{K}_{\mathrm{j}}^2$, and especially how its probability (frequency) is quantified, $P\left(\mathrm{K}_{\mathrm{i}}^1 \cdot \mathrm{K}_{\mathrm{j}}^2\right)$. In principle, one could consider numerous rules how to manipulate cut set combinations, in a similar way as, e.g., post-processing of cut sets could be done.

In the pilot study as well as in this example, we consider only one kind of rule, which takes into consideration dependencies between pairs of basic events. Let A_1 and A_2 be a pair of basic events so that A_1 appears in the MCS list 1, $\sum_i K_i^1$, and A_2 in the MCS list 2, $\sum_i K_i^2$. If there is a (positive) dependency between the events, then

$$P(A_1 \cdot A_2) > P(A_1)P(A_2).$$

The dependency rule is implemented by the second approach (see previous subsection) to model dependencies between basic events, i.e., each basic event A_i is transformed as a product of a common event and unit-specific event, $A_i = A_i' \cdot A_c'$. After the transformation of all basic events in this manner and after a Boolean reduction of the joint cut sets, a proper two-unit minimal cut set list is obtained for the joint top event. In case of more than two units, the procedure could be repeated by combining MCS lists together one by one.

Example:

Assume a multi-unit initiating event loss of offsite power LOOP with a frequency F. A multi-unit event has been identified representing the dependency of diesels (a total CCF between all the diesels on both units).

In the MCS list approach the quantification of the MCSs that contain the CCF of all diesels is defined according to the partitioning

DGi = cDG' · DGi', i = 1,2,

where DGi is the CCF event in the original, unit-specific MCS list for unit i, and cDG' and DGi' are the basic events in the multi-unit PSA MCS list. The common CCF event, cDG', represents a potential for common CCF for both units (c.f. the shock parameter in the binomial failure rate model), and the unit-specific CCF event, DGi', represents the conditional probability that the potentiality for a CCF will be realised for unit i. In a symmetrical case (CCF is equally likely for both unit), the probability of DGi' is also the conditional probability that both units have CCF of all diesels given that one unit has CCF of all diesels.

Since the initiating event, LOOPi, is a common event for both units, the unit-specific conditional probability for a LOOP, given the "potential" for LOOP is 1, i.e., P(LOOPi') =1. Therefore, LOOP, will be transformed as follows

LOOPi =cLOOP' · LOOPi' = cLOOP', i = 1,2.

Then all MCSs from the two MCS lists are joined, and Boolean reduction is performed. The Boolean reduction can be exemplified by a joint MCS, denoted MCSc', from the two MCS lists containing the diesel CCF, denoted below MCS1' and MCS2'. For that joint MCS the Boolean reduction would mean:

MCSc' = MCS1' · MCS2'

= (cLOOP' · …· cDG' · DG1') · (cLOOP' · …· cDG' · DG2') = cLOOP' · …· cDG' · DG1' · DG2'.

3.3 Multi-unit event combinations approach

In the case of two units, the MUCDF related to an initiating event (multi-unit initiator) can be re-written (from the initial formula in section 8.2) to:

$$MUCDF_{IE} = F_{IE} \times \sum_{i=1}^{n} \left(\prod_{j=1}^{M_i} P_{i,IE,j} \right) \times p(\mathrm{CDP}_{unit1} | \mathrm{IE\ \&\ i}) \times p(\mathrm{CDP}_{unit2} | \mathrm{IE\ \&\ i})$$

where:

F_{IE} is the frequency for the initiating event studied,

n is the number of combinations of multi-unit events studied for this initiating event,

M_i is the number of multi-unit events in the ith combination.

$P_{i,IE,j}$ is the probability of the jth multi-unit event of the ith combination at this initiating event, and

$p(\mathrm{CDP}_{unitx}|\mathrm{IE}\ \&\ \mathrm{i})$ is the conditional core damage probability of unit x given that the initiating event and the multi-unit events of the ith combination occur.

Using the multi-unit event combinations approach, each combination of an initiating event and multi-unit events can be considered as a separate initiator. It shall be observed that if a multi-unit event has a high probability, it may be necessary to consider the success of the event for other sequences (to avoid overestimated results). This may be thought of as an event tree, starting from the initiating event (multi-unit initiator), and including a section/branching point for each multi-unit event. Each sequence of this event tree represents a multi-unit scenario. The initiating event of a scenario is the multi-unit initiator combined with the multi-unit events that occur in the corresponding sequence. The conditional probability (for e.g. core damage) for each single-unit PSA is then analysed conditional to the occurrence of each multi-unit scenario.

It can be noticed that the multi-unit event combinations approach can be easily adopted through manually calculation of the frequency of a specific multi-unit scenario and the conditional probability for each unit of the multi-unit scenario, in a simplified form, without development of an additional calculation support.

Example:

Assume a multi-unit initiating event loss of offsite power with a frequency F. A multi-unit event has been identified representing the dependency of diesels (a total CCF between all the diesels on both units). This multi-unit event probability is denoted P.

There are two situations that need to be considered. Either the CCF between all diesels occurs with the probability P, or it does not occur (1 – P). If P is small, the success can be disregarded. Each unit PSA is evaluated for the conditional core damage probability cCDPx, with the initiating event frequency set to 1 and with the basic events representing the diesels set to Failed. The MUCDF of the scenario representing the multi-unit event is calculated as F × P × cCDP1× cCDP2.

4 MCS list approach

4.1 Analysis set-up

In the analysis, each basic event for which a dependency has been defined (Section A2.2) is decomposed into two basic events as explained in Section A3.1. The factors given in Table A.1 are assigned to the unit-specific basic events, and the common basic events receive the value

$$P(A_c') = P(A_i)/\ P(A_i').$$

Newly defined basic events are listed in Table A.2.

Table A.2. Decomposition of the dependent basic events.

Basic event ID	Description	Original P	Unit-specific P	Common event P
!IE-LOOP	Loss of Offsite Power initiating event	1,00E-01	1,00E+00	1,00E-01
ACP-GT01-A	Gas Turbine in standby supplying power to bus bar 3 fail to start	1,56E-02	1,00E+00	1,56E-02
ACP-GT01-M	Gas Turbine in standby supplying power to bus bar 3 is unavailable due to maintenance	1,90E-03	1,00E+00	1,90E-03
CCF-ACP-DG---A-ALL	Diesel generator in standby fails to start	8,60E-04	4,00E-01	2,15E-03
CCF-CCW-PM---A-ALL	Component cooling water system pumps fails to start	1,21E-04	4,00E-01	3,03E-04
CCF-CCW-PM---D-ALL	Component cooling water system pumps stops operating	1,20E-05	4,00E-01	3,00E-05
CCF-EFW-PM---A-ALL	Emergency Feed Water System pumps fails to start	2,62E-04	4,00E-01	6,55E-04
CCF-EFW-PM---D-ALL	Emergency Feed Water System pumps stops operating	5,74E-04	4,00E-01	1,44E-03

Basic event ID	Description	Original P	Unit-specific P	Common event P
CCF-RHR-PM---A-ALL	Residual Heat Removal System pumps fails to start	3,35E-04	4,00E-01	8,38E-04
CCF-RHR-PM---D-ALL	Residual Heat Removal System pumps stops operating	1,00E-03	4,00E-01	2,50E-03
CCF-SWS-PM---A-ALL	Service Water System pumps fails to start	1,21E-04	4,00E-01	3,03E-04
CCF-SWS-PM---D-ALL	Service Water System pumps stops operating	1,01E-04	4,00E-01	2,53E-04
ECC_____O	OPERATOR FAILS TO ACTIVATE ECC	5,00E-02	5,00E-01	1,00E-01

Quantification of minimal cut sets is limited to 100 most important minimal cut sets (of the single-unit PSA), which cover 92,4% (4,62E-6/yr) of the single-unit PSA's result (5,0E-6/yr).

4.2 Results

The quantification of minimal cuts sets is done both using S1-sum and Min cut set upper bound method, both yielding the same result 9,12E-7/yr. When "corrected" with the coverage error, an estimate 9,88E-7/yr would be obtained.

The multi-unit CDF results are presented in Table A.3.

Table A.3 The multi-unit risk results

Calculation	Result	Comment
S1-sum, 100 single-unit MCSs	9,12E-7	5976 joint minimal cut sets (4024 non-minimal joint cut sets)
MCUB, 100 single-unit MCSs	9,12E-7	
Adjusted S1-sum by the coverage factor	9,88E-7	100 MCSs corresponds with 92.4% of the single-unit PSA result
S1-sum when only combinations of identical MCSs are quantified	9,01E-7	Very fast and simple quantification method when identical cut set lists are combined

The 10 most dominating MCSs in the results are (the prefix "c" in the basic event ID denotes the common basic event while "1" and "2" denote a unit-specific basic event):

5,37E-07	c!IE-LOOP	cACP-GT01-A	cCCF-ACP-DG---A-ALL	1CCF-ACP-DG---A-ALL	2CCF-ACP-DG---A-ALL
7,55E-08	c!IE-LOOP	cACP-GT01-A	cCCF-CCW-PM---A-ALL	1CCF-CCW-PM---A-ALL	2CCF-CCW-PM---A-ALL
7,55E-08	c!IE-LOOP	cACP-GT01-A	cCCF-SWS-PM---A-ALL	1CCF-SWS-PM---A-ALL	2CCF-SWS-PM---A-ALL
6,54E-08	c!IE-LOOP	cACP-GT01-M	cCCF-ACP-DG---A-ALL	1CCF-ACP-DG---A-ALL	2CCF-ACP-DG---A-ALL
6,30E-08	c!IE-LOOP	cACP-GT01-A	cCCF-SWS-PM---D-ALL	1CCF-SWS-PM---D-ALL	2CCF-SWS-PM---D-ALL
2,50E-08	c!IE-LOOP	cACP-GT01-A	cCCF-RHR-PM---D-ALL	1CCF-RHR-PM---D-ALL	1FEED&BLEED_____O
	2CCF-RHR-PM---D-ALL	2FEED&BLEED_____O			
9,20E-09	c!IE-LOOP	cACP-GT01-M	cCCF-CCW-PM---A-ALL	1CCF-CCW-PM---A-ALL	2CCF-CCW-PM---A-ALL
9,20E-09	c!IE-LOOP	cACP-GT01-M	cCCF-SWS-PM---A-ALL	1CCF-SWS-PM---A-ALL	2CCF-SWS-PM---A-ALL
8,95E-09	c!IE-LOOP	cACP-GT01-A	cCCF-EFW-PM---D-ALL	cECC_____O	1CCF-EFW-PM---D-ALL
	1ECC_____O	2CCF-EFW-PM---D-ALL	2ECC_____O		
8,36E-09	c!IE-LOOP	cACP-GT01-A	cCCF-RHR-PM---A-ALL	1CCF-RHR-PM---A-ALL	1FEED&BLEED_____O
	2CCF-RHR-PM---A-ALL	2FEED&BLEED_____O			

Fussell-Vesely importances for the dependencies are calculated to:

- DG failure to operate (CCF) 67%

- SWS-A failure to start (CCF) 9%
- SWS-D failure to run (CCF) 8%
- CCW-A failure to start (CCF) 9%
- CCW-D failure to run (CCF) 1%
- EFW-A failure to start (CCF) 0,5%
- EFW-D failure to run (CCF) 1%
- RHR-A failure to start (CCF) 1%
- RHR-D failure to run (CCF) 3%
- GT-A failure to operate 89%
- GT-M Maintenance 11%
- ECC-O Manual start of ECC 2%

5 Multi-unit event combinations approach

5.1 Analysis set up

In the multi-unit event combinations approach, for each multi-unit initiator a pre-event tree is set up. The event tree is set up for branch points for all dependencies relevant for the initiator. The sequences of the event tree correspond to multi-unit scenarios, and the frequencies of the scenarios can be calculated from the event tree.

For each sequence in the pre-event tree, each single-unit model is evaluated as conditional that the multi-unit event(s) related to the dependency(ies) occur or not to calculate conditional accident probabilities, e.g. conditional core damage probabilities. When a branch-point has been passed in the pre-event tree, there are two options:

- The event related to the dependency did occur: The probability of the sequence in the pre-event tree is multiplied with the probability of the dependency. All sequences following should be evaluated conditionally that the event related to the dependency has occurred (when the separate PSA models are evaluated).
- The event related to the dependency did not occur: The probability of the sequence in the pre-event tree is multiplied with the probability of success event of the dependency. The event in the PSA model for the individual unit is set conditional success of the dependency (e.g. if the multi-unit CCF did not occur, then that probability needs to be subtracted from the individual plant event probability). The treatment of success may not be needed (conservative) if the evaluation is performed manually.

Finally, the multi-unit accident frequency of each scenario can be calculated as the frequency of the scenario (calculated from the pre-event tree) multiplied by the conditional accident probabilities of the units.

For example, if the pre event tree is evaluating that the multi-unit event failure of all diesels has occurred, then the model for each unit is evaluated with the condition that the diesels are unavailable (event is true). The results of those calculations are then multiplied with the frequency of the sequence in the pre-event tree to calculate the MUCDF of the multi-unit scenario.

The dependencies that are treated as branch points are:

- DG failure to operate
- SWS-A failure to start
- SWS-D failure to run
- CCW-A failure to start

- CCW-D failure to run
- EFW-A failure to start
- EFW-D failure to run
- RHR-A failure to start
- RHR-D failure to run
- GT-A failure to operate
- GT-M Maintenance
- ECC-O Manual start of ECC

It can be observed that grouping of dependencies may be useful to simplify the calculations (reduce the amount of branch-points).

The next step is to define the basic events in each model that represents each dependency/multi-unit event.

5.2 Results

The results are calculated with following methods:

- Min cut upper bound, MCUB (RiskSpectrum standard approach)
- Rare event approximation, REA (simplified, straight sum)
- Treatment of success with regard to dependencies not occurring
- No treatment of success with regard to dependencies not occurring

The multi-unit risk results are presented in Table A.4.

Table A.4 The multi-unit risk results

Calculation	Result	Comment
MCUB and Success	9,13E-7	This is the best estimate (see below)
MCUB and No Success	9,39E-7	
REA and Success	9,17E-7	
REA and No Success	9,44E-7	

The differences in results are not significant and all of the approaches may be considered acceptable in this case. The MCUB and Success is the best estimate because intersections between MCS are considered and success of multi-unit events not occurring is considered. The MCUB and No Success is expected to be very close to what a manual evaluation should have generated, as treatment of success may be complicated when a manual evaluation is considered.

The 10 most dominating sequences in the results are:

- 5,23E-07 Combination DG GTA
- 7,35E-08 Combination CCWA GTA
- 7,35E-08 Combination SWSA GTA
- 6,26E-08 Combination DG GTM
- 6,13E-08 Combination SWSD GTA
- 2,48E-08 Combination RHRD GTA

- 1,34E-08 Combination DG GTA ECC_O
- 8,96E-09 Combination EFWD GTA ECC_O
- 8,80E-09 Combination CCWA GTM
- 8,80E-09 Combination SWSA GTM
- 8,30E-09 Combination RHRA GTA

And the FV for the dependencies are calculated to:

- GTA 89%
- DG 66%
- SWSA 9%
- SWSD 8%
- CCWA 9%
- CCWD 1%
- EFWA 1%
- EFWD 1%
- GTM 11%
- ECC_O 4%

6 Discussion

Two different methods, both using the results from the individual PSA models, have been demonstrated and it has been shown that both methods can estimate the multi-unit risk. The difference in the methods lies in that one of the methods combines the MCS lists into one single MCS list and the other method uses an approach that can be illustrated by a pre-event tree that evaluates the combinations of multi-unit events prior to performing conditional quantifications of the single unit models.

Appendix B

Example quantification of multi-unit risk metrics

Table of contents

1 Introduction

To illustrate the risk metrics discussed in the main report, a fictive example is presented in this appendix. The example is comparable to the pilot studies in SITRON, but the presented numbers are fictive, and chosen for demonstration purposes, only. The example concerns with a site with two identical reactor units and covers one multi-unit initiating event, e.g., a multi-unit loss-of-offsite power (LOOP), as considered in the pilot studies. In the example, we only consider one plant operating state (POS) combination, i.e., both units are initially at-power. If more multi-unit initiating events and POS combinations would be considered, corresponding risk metrics can be simply obtained by summing the case specific risk metrics.

2 Definitions for risk metrics

The following risk metrics are considered in this example:

- Level 1 PSA
    - SUCDF = single-unit core damage frequency, frequency of a core damage accident of a particular unit.
    - SCDF = site core damage frequency, frequency of an accident with at least one reactor core damage at the site.
    - MUCDF = multi-unit core damage frequency, frequency of an accident with multiple (two in the example) reactor core damages at the site.
- Level 2 PSA
    - SURCF = single-unit release category frequency, frequency of an unacceptable release of a particular unit.
    - SRCF = site release category frequency, frequency of an unacceptable release at the site.
    - MURCF = multi-unit release category frequency, frequency of an unacceptable release in multiple units at the site (two in the example).

In level 2 PSA, four release categories are defined, following the definitions applied in one of the pilot studies (see Figure B.1):

- Acceptable release, which is a release less than 0.1 % of the core inventory of Cs-134 or Cs-137 from an 1800 MWt BWR (Barsebäck 1 unit). This is so called "RAMA" criterion defined in 1980's in Sweden when the decision was made to implement severe accident mitigation systems for the NPPs. (RC1).
- Unacceptable release, which is a release above the RAMA criterion. (RC2 + RC3 + RC4);
- Large release, which is a release of more than 10 % of volatile fission products of the core inventory. (RC3 + RC4);
- Large early release, which is a large release occurring prior to effective evacuation of the close-in population such that there is a potential for early health effects (RC4).

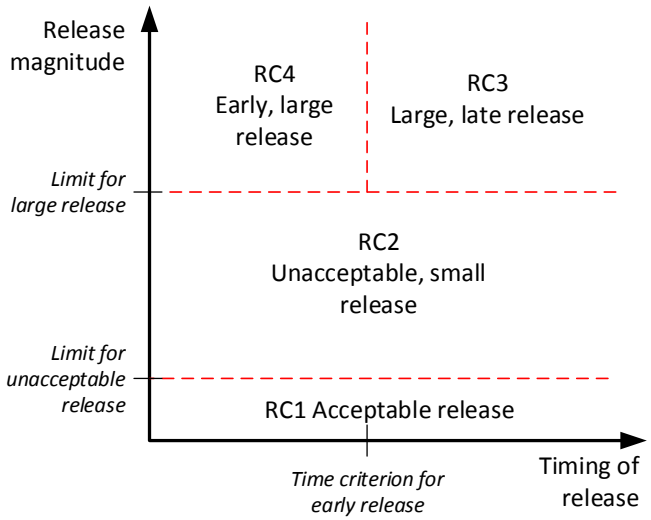


Figure B.1. Release categories (RC) of the example.

3 Single-unit PSA results

Table B.1 presents quantitative results from the single-unit PSA both for Level 1 and Level 2. It is assumed that the two units are identical so that single-unit results are identical. Single-unit CDF (SUCDF) is 3.5E-07 per year, which has been further split into plant damage state (PDS) frequencies. Here we assume that two PDSs dominate the results, i.e., high-pressure transient (HPT) and low-pressure transient (LPT).

Results for Level 2 PSA have been divided into release categories according to the usual Swedish praxis. Frequency for unacceptable release is the sum of release frequencies for small, large early and large late release, i.e., SURCF(unacceptable) = 7.9E-08 per year (= 4.0E-08 + 2.5E-08 + 1.5E-08 per year). This is the main risk metric for Level 2 PSA to be compared with the safety goal.

Table B.1. Example risk metrics for a single-unit PSA [1/year]

	Plant damage state		Sum
	HPT	LPT	
Level 1 PSA			
Core damage	2.5E-07	1,0E-07	**3.5E-07**
Level 2 PSA			
Acceptable release	2.0E-07	7.5E-08	**2.7E-07**
Small release	2.8E-08	1.2E-08	**4.0E-08**
Large late release	1.6E-08	8.6E-09	**2.5E-08**
Large early release	1.0E-08	4.4E-09	**1.5E-08**
Sum	**2.5E-07**	**1.0E-07**	**3.5E-07**

SUCDF

SURCF (Unacceptable release)

HPT = high-pressure transient,
LPT = low-pressure transient

4 Multi-unit level 1 PSA results

Next, a multi-unit analysis is performed, i.e., combinations of scenarios for units 1 and 2 are studied taking into account dependences between the units such as common systems, operator actions dependences and inter-unit CCFs. Table B.2 shows the results for plant damage state combinations. From this table, multi-unit risk metrics for Level 1 PSA can be calculated, such as

- SCDF (site core damage frequency) = 6.5E-07 per year. This is sum of all PDS-combinations minus "OK-OK". This is slightly less than twice the single-unit CDF (2 × 3.5E-07 per year = 7.0E-07 per year). The difference is equal to MUCDF.
- MUCDF (multi-unit core damage frequency) = 5.0E-08 per year. This is sum of HPT-HPT, HPT-LPT (twice) and LPT-LPT combinations.

Table B.2. Example multi-unit plant damage state frequencies [1/year].

Plant damage state unit 2		Plant damage state unit 1		
		OK	HPT	LPT
OK	No core damage	1.0E-02	2.2E-07	8.0E-08
HPT	High-pressure transient	2.2E-07	3.0E-08	1.0E-10
LPT	Low-pressure transient	8.0E-08	1.0E-10	2.0E-08
Sum		**1.0E-02**	**2.5E-07**	**1.0E-07**

SDF
SUCDF
MUCDF

5 Multi-unit level 2 PSA results

To calculate multi-unit release frequencies, release categories for combinations of single-unit releases need to be determined. In the pilot studies, we have assumed that each minimal cut set of the single-unit PSA is associated with a certain source term so that the combination of two minimal cut sets can be associated with the combination of corresponding source terms. Therefore, the determination of multi-unit release category is straightforward.

Based on findings from the pilot studies, it can be concluded that a combination of two acceptable releases will be most likely an acceptable release. Similarly, a combination of two small releases will be most likely a small release. Combination of two large late releases cannot be an early large release. As a conclusion, multi-unit release categories can be thus defined as simply as illustrated in Figure B.2. This simplification has been applied in the pilot studies for the method demonstration purposes.

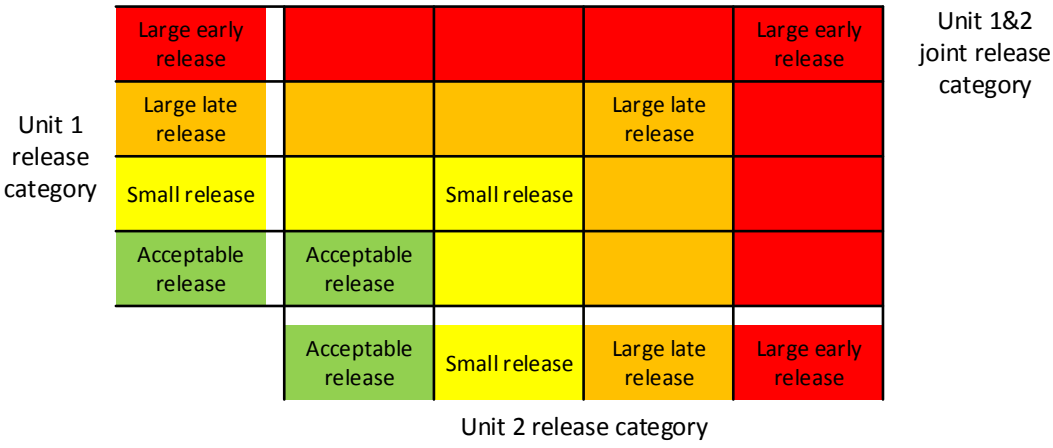


Figure B.2. Simplified determination of the multi-unit release category

Release frequencies for various plant damage state combinations must be solved. In principle, many PDS-combinations may need to be evaluated, depending on the number of non-significant PDSs. In this example, there are eight PDS-combinations to be considered, but only five cases need to be solved due to symmetries. In addition, preliminary findings from the pilot studies indicate that, in practice, many PDS-combinations can be shown to be insignificant, which makes the multi-unit Level 2 assessments manageable. In fact, if the aim is just to assess the frequency for an unacceptable release at the site level, only one "new" quantification is needed. This is the scenario where both units experience an unacceptable release. The site level (two-unit) frequency regarding unacceptable release is

SRCF(unacceptable) = 2 × SURCF(unacceptable) – MURCF(unacceptable).

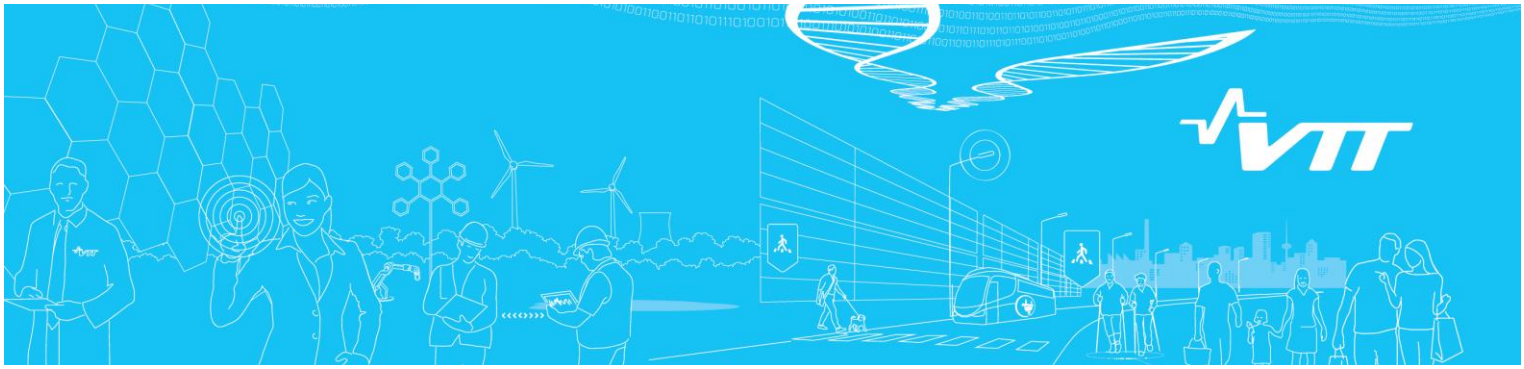
Table B.3 presents example multi-unit Level 2 PSA results. The numbers in the right-most column are the site release frequencies for this initiating event. For instance, the site level frequency for an unacceptable release SRCF(unacceptable) = 1.53E-07 per year (= 7.7E-08 + 4.8E-08 + 2.8E-08), which is slightly lower than twice the corresponding single-unit frequency (2 × 7.9E-08 per year = 1.58E-07 per year). The difference is MURCF(unacceptable) = 5E-09 per year.

Table B.3. Example multi-unit release category frequencies [1/year].

Release category	Multi-unit plant damage state (Unit 1 - Unit 2)								
	OK-HPT	HPT-OK	OK-LPT	LPT-OK	HPT-HPT	LPT-LPT	HPT-LPT	LPT-HPT	**Sum**
Acceptable release	1.7E-7	1.7E-7	5.7E-8	5.7E-8	2.5E-8	1.8E-8	5.0E-11	5.0E-11	**5.0E-7**
Small release	2.6E-8	2.2E-8	1.1E-8	1.1E-8	2.0E-9	6.0E-10	1.2E-11	1.2E-11	**7.7E-8**
Large late release	1.5E-8	1.5E-8	8.0E-9	8.0E-9	1.5E-9	8.0E-10	2.6E-11	2.6E-11	**4.8E-8**
Large early release	9.0E-9	9.0E-9	4.0E-9	4.0E-9	1.5E-9	6.0E-10	1.2E-11	1.2E-11	**2.8E-8**
Sum	**2.2E-7**	**2.2E-7**	**8.0E-8**	**8.0E-8**	**3.0E-8**	**2.0E-8**	**1.0E-10**	**1.0E-10**	**6.5E-7**

Appendix C – WP3 Site PSA model management

Tyrväinen, T., Björkman K. 2019. SITRON — Site PSA model management, VTT-R-06885-18, VTT, Espoo.



RESEARCH REPORT

VTT-R-06885-18

SITRON - Site PSA model management

Authors: Tero Tyrväinen, Kim Björkman

Confidentiality: Public

Report's title SITRON - Site PSA model management	
Customer, contact person, address VYR, NKS, FKA, RAB, SSM	**Order reference** SAFIR 4/2018
Project name Probabilistic risk assessment method development and applications	**Project number/Short name** 110223/PRAMEA
Author(s) Tero Tyrväinen, Kim Björkman	**Pages** 25/
Keywords Site probabilistic safety assessment, model management	**Report identification code** VTT-R-06885-18

Summary

In site probabilistic safety assessment (PSA), a nuclear power plant site is analysed as a whole considering all reactor units and other facilities with radionuclide sources. Site PSA especially focuses on dependencies between different units and locations of the radionuclide sources. Most PSAs are unit specific and there are no well-established methods for site PSA.

Besides general method development, procedures are needed for documenting the site PSA, managing possible modifications made to the single-unit PSA models, and managing the data and computation. This report provides guidance for site PSA model management and discusses the needs for a site PSA database. This report is closely connected to a site PSA method described in a separate report and it considers the same analysis phases.

The report discusses single-unit PSA models from site PSA perspective, site PSA documentation and the database for site PSA. Guidelines for site PSA documentation and model management tasks in different analysis phases and in the maintenance phase are given. The focus of the report is on level 1 issues, but also level 2 aspects are covered.

Confidentiality	Public

Espoo 18.1.2019

Written by	**Reviewed by**	**Accepted by**
Tero Tyrväinen, Research Scientist	Ilkka Karanta, Senior Scientist	Eila Lehmus, Research Team Leader

VTT's contact address
VTT, PL 1000, 02044 VTT

Distribution (customer and VTT)
SAFIR reference group 2, FKA, RAB, SSM, Lloyds Register, Risk Pilot AB, VTT archives

Contents

Abbreviations

Acronym	Description
CCDP	Conditional Core Damage Probability
CSTP	Conditional Source Term category Probability
CCF	Common Cause Failure
MCS	Minimal Cut Set
MUCDF	Multi-Unit Core Damage Frequency
MUIE	Multi-Unit Initiating Event
MUSTF	Multi-unit Source Term category combination Frequency
POS	Plant Operating State
PSA	Probabilistic Safety Assessment
SCDF	Site Core Damage Frequency
SSC	Systems, Structures and Components

1. Introduction

In site probabilistic safety assessment (PSA), a nuclear power plant site is analysed as a whole considering all reactor units and other facilities with radioactive sources. Site PSA especially focuses on dependencies between different units and locations of the radioactive sources. For example, an external hazard can affect multiple reactor units or facilities at the same time, and then resources shared between the units might not be available for all units to manage the accident. Most PSAs are unit specific, and there are no well-established methods for site PSA.

Site PSA methods have been studied in separate research reports [1-2]. In addition to methods, procedures are needed for documenting the analysis, managing possible modifications made to the PSA models, and managing the data and computation. This report provides guidance for site PSA model management and discusses the needs for site PSA database. The work is partly based on the requirements presented in [3]. The report is closely connected to the method report [1] and it considers the same analysis phases.

The selection of the risk metrics to be calculated is the starting point for the site PSA. Risk metrics for site PSA have been outlined in [4]. The main site risk metrics for level 1 PSA are the site core damage frequency (SCDF) and the multi-unit core damage frequency (MUCDF). The SCDF is the frequency for any core damage to occur at the site per site-year. The MUCDF is the frequency of core damage occurring in multiple units nearly simultaneously. The MUCDF can be calculated for a specific combination of units, and also the total MUCDF can be calculated as the frequency of core damage occurring in at least two units taking into account all the units at the site. Computation of risk importance measures with regard to different risk metrics is also an important part of site PSA. MUCDF and SCDF can be generalised to concern fuel damage instead of core damage when radioactive sources other than reactor cores are included in the analysis. The main risk metrics for level 2 PSA are the frequencies of site release categories.

Section 2 summarises the method developed in [1] and introduces some basic concepts. Section 3 discusses the challenges related to site PSA analysis and model management. Single-unit models are discussed in Section 4, site PSA document is outlined in Section 5, and database for site PSA is discussed in Section 6. Section 7 goes through the whole site PSA analysis process from the model management point of view. Maintenance of site PSA is briefly discussed in Section 8. The conclusions of the report are presented in Section 9.

2. Method description

Method for evaluating the site risk for nuclear installations using already existing single-unit PSA models is presented in [1]. This section summarizes the method in order to provide basic information as a link to the site PSA model management.

Site PSA mainly concerns three types of analysis elements:

- plant operating states
- multi-unit initiators
- multi-unit dependencies.

A multi-unit initiator is an event that can initiate an accident in multiple units. A multi-unit dependency is a dependency that can cause an event to affect multiple units or dependent events in multiple units. Dependencies related to multi-unit initiators are not included in the category “multi-unit dependencies” here, because they are considered separately.

Based on [1], the following analysis steps can be identified:

1. **Selection of analysis scope and risk metrics:** In this step, the scope of the site PSA is selected. The following issues should be considered in the selection: different radioactive sources, possible operating states, initiators, and PSA end states. The scope of the site PSA needs to be consistent with the scope of the single-unit PSA.

2. **Analysis of POS impact:** Site PSA needs to account for the units' various combinations of possible plant operating states (POSs). The POSs come directly from single-unit PSAs and they concern only one unit. POS groups are created based on individual POSs that are sufficiently similar. POS groups also concern only one unit. Then, POS groups of different units are combined to create POS group combinations that include one POS group from each unit included in the analysis. POS groups and POS group combinations are screened so that only the most relevant POS group combinations are included in the quantification.

   Figure 1 illustrates the creation of POS group combination with four POSs and two units. The POS groups with POS D are screened out, as well as the POS group combination with POSs B and C coming from both of the units.

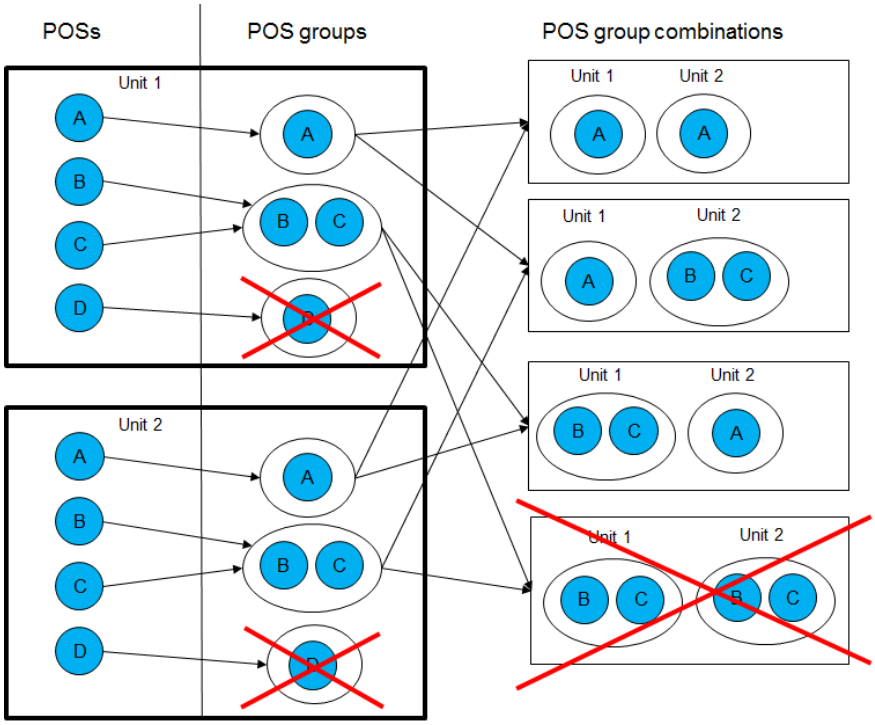


Figure 1: Illustration of the creation of POS group combinations.

3. **Identification of multi-unit initiators:** There are three types of multi-unit initiators:

   - Multi-unit initiating events (MUIEs, that affect always multiple units)
   - Partial multi-unit initiating events (that may affect one or multiple units)
   - Propagating events: Accident starts in one unit and propagates later to another unit.

   Partial multi-unit initiating events are divided into multi-unit initiating events and single-unit initiating events, and the multi-unit initiating events are included in the further analysis.

The multi-unit initiators are screened, and the most relevant ones are selected for quantification. Relevant combinations of multi-unit initiators and POS group combinations are identified for the analysis. Let a pair of a multi-unit initiator and POS group combination be called a *multi-unit analysis case*.

Figure 2 illustrates how multi-unit analysis cases are constructed based on multi-unit initiators and the POS group combinations which were screened in previously. Propagating event PE (the orange block) is screened out. Based on partial multi-unit initiating event, new multi-unit initiating event MUIE3 is created. Multi-unit initiating event MUIE2 is not relevant for POSs B and C, and the corresponding analysis cases are thus not created. Analysis cases with MUIE1 and POS group combinations A-BC and BC-A are also screened out. Five multi-unit analysis cases are left for further analysis.

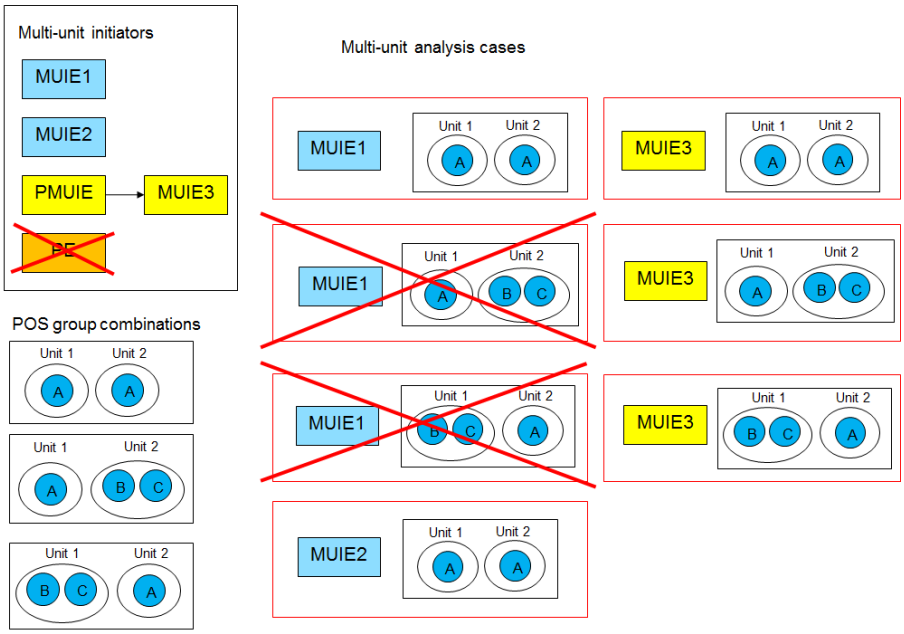


Figure 2: Illustration of the creation of multi-unit analysis cases.

4. **Identification and selection of dependencies:** Different types of multi-unit dependencies include

    - shared systems, structures, and components (SSC)
    - identical components
    - spatial dependencies
    - human and organizational dependencies
    - containment and vessel design
    - simultaneous maintenance
    - phenomenological uncertainty (e.g. epistemic uncertainty related to severe accident phenomena can be common for two units).

Identified multi-unit dependencies are screened qualitatively. Single-unit basic events associated with the screened in multi-unit dependencies are identified. Multi-unit

dependencies are screened quantitatively based on the single-unit basic events. For each multi-unit analysis case, the relevant multi-unit dependencies are identified.

Figure 3 illustrates the screening process of multi-unit dependencies. One dependency is screened out qualitatively, and one dependency is screened out quantitatively. Then, relevant multi-unit dependencies are identified for each multi-unit analysis case.

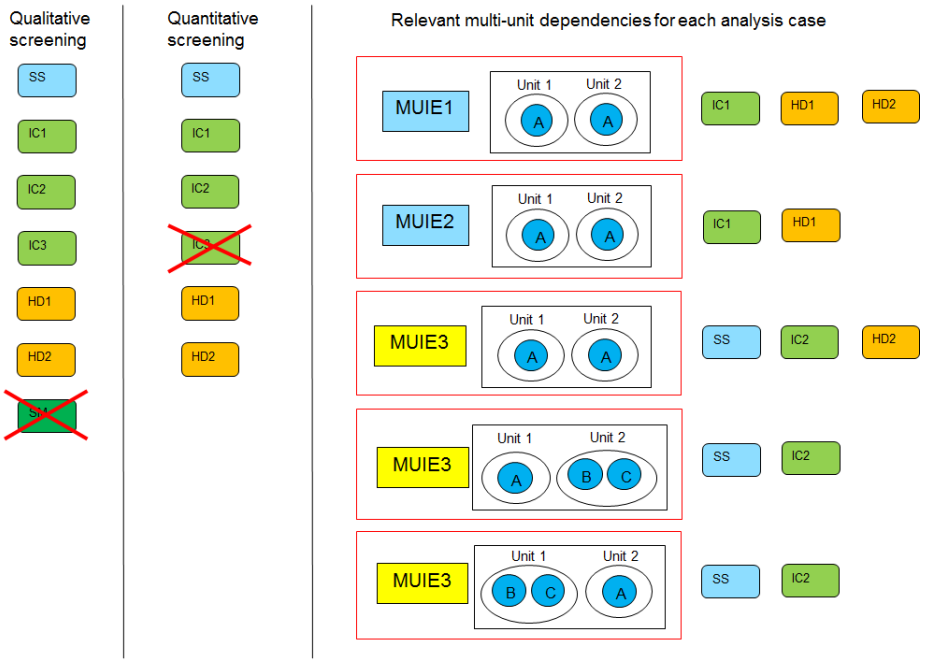


Figure 3: Screening of multi-unit dependencies.

From the screened in multi-unit dependencies, multi-unit basic events are selected. A multi-unit basic event is a set of dependent events in multiple units or an event affecting multiple units. One or multiple multi-unit basic events can be selected based on a multi-unit dependency. For each multi-unit analysis case, the relevant multi-unit basic events are identified.

5. **Analysis of source terms:** This step is relevant only when level 2 analysis is considered. Source term categories are analyzed to determine which of them are relevant for the screened in MUIEs. Screening of source terms can be performed based on single-unit PSA results. Then combined source terms are studied to examine how the source term combinations are mapped into site release categories. Finally, the relevance of source term combinations for multi-unit analysis is assessed. Relevance of a source term combination is dependent on the applied risk metrics. Final selection of release categories to be analyzed can also be made at this point.

6. **Data analysis**: The frequencies of multi-unit initiators and the probabilities of multi-unit basic events are estimated in each multi-unit analysis case.

7. **Quantification of multi-unit risks:** The analyst can select one of the two following approaches:

    a. **Multi-unit event combinations approach:**

    A multi-unit scenario is defined as a combination including

    - a POS group combination
    - a multi-unit initiator

- zero, one or multiple multi-unit basic events.

Multi-unit scenarios are created for the quantification based on the multi-unit analysis cases and multi-unit basic events relevant for each analysis case. In an analysis case, all possible combinations of relevant multi-unit basic events, i.e. all possible multi-unit scenarios, are considered.

The frequency of each multi-unit scenario is calculated as the frequency of the initiator multiplied by the probabilities of multi-unit basic events. The conditional core damage probability (CCDP) or conditional source term category probabilities (CSTPs) of each multi-unit scenario are also calculated. The MUCDF of a multi-unit scenario is then the frequency of the multi-unit scenario multiplied by the CCDP values. Similarly, the multi-unit source term category combination frequency (MUSTF) is the frequency of the multi-unit scenario multiplied by the CSTP values corresponding to source term category combination. The risk metrics and risk importance values are calculated based on the MUCDF or MUSTF values of the multi-unit scenarios.

b. **Minimal cut set list approach:**

The minimal cut set (MCS) lists of different units are combined, and the risk metrics and risk importance values are calculated based on the combined MCS list(s). The quantification is in principle similar to single-unit PSA quantification.

3. Challenges

Site PSA introduces new challenges for documentation, PSA model management and computation tools. Site PSA involves information and data from many different sources, use of multiple PSA models, and several analysis steps, which are potentially applied to a large set of dependencies between units. Systematic data management and documentation procedures are therefore needed to manage the site level analysis process as a whole.

Single-unit PSA models need to be extended to include significant multi-unit dependencies if they have not been modelled before. In addition to documentation, this can be a challenge for PSA model configuration management and change tracking point of view. In addition, some specific scenarios may require special calculations with a single-unit PSA model, e.g. to determine the probability that a shared system is used. This may require creation of new special versions of single-unit PSA models.

Multi-unit risk is estimated based on the information from the different units, which means that risk metrics and risk importance measures are not obtained directly from a single PSA model like in single-unit analyses. Total site calculations need to combine somehow the results from different PSA models.

The maintenance of a site PSA is also more challenging than the maintenance of a single-unit PSA. When a modification is made to one unit, site results need to also be updated. PSAs should also be updated in parallel for site PSA, not one by one. Site PSA could even be maintained as living PSA.

4. Single-unit PSA models

4.1 Requirements for single-unit PSA models

In the site PSA method [1], it is assumed that single-unit PSA covers all scenarios and events that can significantly affect single-unit risk, including multi-unit accident scenarios. It has to be possible to calculate the conditional core damage probability of a multi-unit scenario (defined in Section 2) correctly using a single-unit model. In other words, the consequences of multi-unit events have to be modelled correctly in single-unit PSAs.

Risk-significant shared systems need to be taken correctly into account in the site level quantification. The unavailability of a shared system due to its use in another unit has to be included in the single-unit models as discussed in Section 4.2.

When the analysis includes level 2, it needs to be possible to calculate the conditional source term category probabilities of multi-unit accident scenarios. If release categorisation is changed/simplified compared to the single-unit PSA (e.g. one release category for unacceptable release is used instead of splitting it into multiple release categories), there might be a need to change the release categorisation in the versions of the single-unit models used in site PSA.

If spent fuel pool belonging to a reactor unit is included in the scope of the analysis, the single-unit PSA should cover both the reactor risks and the spent fuel pool risks. It is not necessary to include them in the same PSA model as long as conditional fuel damage probabilities and conditional source term category probabilities of multi-unit scenarios can be calculated.

4.2 Modelling multi-unit aspects in single-unit models

Some multi-unit scenarios may need to be modelled in single-unit models, particularly scenarios involving a shared system or human actions. Separating multi-unit events, particularly multi-unit initiating events, from single-unit events in single-unit models can make modelling of site dependencies easier, since human error probabilities or unavailabilities of shared systems can be different in different scenarios. Easy identification of multi-unit events would also be useful. An identifier could e.g. appear in the name or comment of a multi-unit event.

The probability that a shared system is needed in another unit needs to be considered in single-unit PSA. The probability may need to be calculated using the PSA model of the other unit. The probability can be assumed to be multi-unit initiator specific. A special version of the corresponding event tree can be created so that the end points of the event tree represent conditions where the shared system is needed. The initiating event frequency can be set to 1, and then the probability that the shared system is used can be calculated directly from the event tree. Some probabilities related to multi-unit dependencies, such as identical components, may also need to be adjusted. The event tree does not need to be used, if the unavailability of the shared system can be determined without it, e.g. if the case is very simple. The basic event can then be added to the other single-unit model. There can be basic events representing the same shared system with different probabilities for different multi-unit initiators. A house event or an attribute can be used to select the correct basic event for each multi-unit initiator.

If there is no priority logic for the use of a system shared between two units, it could be reasonable to divide the calculated probabilities by 2, because the system could be used in either of the units. For example, if probability p_1 is calculated for the scenario that the shared system is also needed in the other unit, probability $p_1/2$ can be used in the PSA model. In

addition, the system has a failure probability p_2. It needs to also be scaled by $1 - p_1/2$. The failure can be modelled as a separate basic event.

It can be stated with some justification that human error probabilities are higher in some multi-unit scenarios. Detailed considerations of human error probabilities in multi-unit scenarios can be found in [1]. The modelling is straightforward, if multi-unit scenarios can be separated from single-unit scenarios in the model, e.g. as separate accident sequences or in the post-processing of minimal cut sets.

Initiating events induced by an accident in another unit need to be taken into account. If such event is found significant, it can be modelled as a separate initiating event or included in the frequency of the corresponding single-unit initiating event. The model of the originating unit may need to be used in the computation of frequency. In addition, the probability of the propagation between units needs to be estimated.

4.3 Updating single-unit models based on multi-unit analysis

It is possible that a need to update single-unit models is noticed when performing multi-unit analysis. It is important to keep the single-unit models up-to-date both from the single-unit and multi-unit analysis point of view. The best option is to perform the correction right away when a need to update (e.g. due to a defect or improvement with regard to increase in realism) is noticed. It also needs to be judged if the analyses performed before the observation need to be revised, e.g. quantitative screening.

It is very case specific what may need to be updated. The update can e.g. be the addition of a new basic event, or the change of a probability or frequency. Modelling of shared systems and human error events are the areas that could most likely require updates from the multi-unit perspective.

5. Site PSA documentation

Site PSA needs to be documented comprehensively. The following chapter titles are recommended to be used in the document:

- Selection of analysis scope and risk metrics
- Data sources and models
- Analysis of POS impact
- Identification of multi-unit initiators
- Identification and selection of dependencies
- Analysis of source terms (level 2 only)
- Data analysis
- Quantification of multi-unit risks
- Documents and files used in the analysis

Section 7 of this document specifies what information should be documented under these chapters.

6. Database for site PSA

A database system is needed to manage the analysis process. It can be just a set of Excel sheets, but since many of the analysis elements are interrelated, a more advanced database system could be considered, e.g. Microsoft Access.

Analysis elements that could be included in the database are presented in Table 1, along with possible data fields. Section 2 contains information on how different analysis elements are linked to the analysis phases. For some data fields, Section 7 provides some further explanation.

Table 1: Site PSA elements.

Element	Description	Possible data fields
Plant operating state	Plant operating state as defined in single-unit PSA	Identifier, description, time share, status of primary circuit, status of the core cooling system, status of the residual heat removal system, status of spent fuel pool, multi-unit initiators
POS group	Group of sufficiently similar POSs for site PSA purposes concerning a single unit	Identifier, POSs belonging to the group, justification for the grouping, time share, time window for core/fuel damage in case of loss of residual heat removal, screening decision, justification for the screening decision, multi-unit initiators
POS group combination	Combination of POS groups (including one group from each unit)	Identifier, the POS groups included in the combination (with correspondence to units), time share, screening decision, justification for the screening decision, multi-unit initiators
Multi-unit initiator	Initiating event that can potentially cause accident in multiple units (including accident propagation to another unit)	Identifier, category, description, frequency, screening decision, justification for the screening decision, source documents, the corresponding initiating events in the single-unit models, relevant POSs, POS dependency, season dependency, POS group combinations to be included in the analysis, justification for the selection of POS group combinations, affected unit combination, data sources, frequency estimation method, frequencies in different POS group combinations
Partial multi-unit initiating event	Initiating event that may affect one or multiple units	Multi-unit initiating events created based on this partial multi-unit initiating event, data sources, frequency estimation method used in single-unit PSA, frequencies in single-unit models, summary of operating data, qualitative analysis, frequency estimation methods for site PSA, new frequencies

Element	Description	Possible data fields
Multi-unit analysis case	A pair of a multi-unit initiator and POS group combination	Identifier, multi-unit initiator, POS group combination, relevant multi-unit dependencies, relevant multi-unit basic events, frequency of the multi-unit initiator in the POS group combination
Multi-unit dependency	A dependency that can cause an event to affect multiple units or dependent events in multiple units (initiating event dependencies excluded)	Identifier, category, description, qualitative ranking, justification for the qualitative ranking, source documents, related units, related basic events in the single-unit models, Fussell-Vesely in each multi-unit initiating event in each unit, maximum contribution from potential multi-unit sequences in each unit, screening decision
Multi-unit basic event	A set of dependent events in multiple units or an event affecting multiple units	Identifier, description, related multi-unit dependency, source documents, related units, related basic events in the single-unit models, relevant multi-unit analysis cases, probability in each relevant multi-unit analysis case
Inter-unit CCF	A CCF where components fail in multiple units (subcategory of multi-unit basic event)	Identifier, component type, failure mode, units, group size, CCF combination, data sources, probability of the corresponding single-unit CCF in each unit, summary of operating data, model used in estimation, parameters used in estimation, probability of the inter-unit CCF
Multi-unit human error event	A human error event affecting multiple units or dependent human error events in multiple units (subcategory of multi-unit basic event)	Identifier, description, related basic events in the single-unit models, probabilities of the basic events in single-unit models, qualitative assessment from multi-unit point of view, probability estimation procedure, penalty factor/dependency category in each relevant multi-unit analysis case, probability in each relevant multi-unit analysis case
Source term	Source term as defined in single-unit PSA	Identifier, description, release size, release timing, other release characteristics, screening decision and justification
Source term combination	Combination of single-unit source terms (including one source term from each considered unit)	Identifier, the source terms included in the combination, associated release category, screening decision, justification for screening and how the combined source terms are associated in the release category
Release category	Group of accident sequences with a similar source term at the site level	Identifier, description, source term combinations

Several analysis elements are connected. A POS group combination consists of POS groups, and a POS group consists of POSs. Inter-unit CCFs and multi-unit human error events are multi-unit basic events with specific properties. Multi-unit basic events originate from multi-unit dependencies. A partial multi-unit initiating event is a multi-unit initiator with special properties. Some new multi-unit initiators are also created based on a partial multi-unit initiating event.

Multi-unit initiators are also associated with specific POSs, POS groups and POS group combinations. Practically, POS groups and POS group combinations inherit the relevant multi-unit initiators from individual POSs. A multi-unit analysis case consists of a multi-unit initiator and a POS group combination.

In a database these connections can be presented as relationships (i.e. one table has a foreign key that references the primary key of another table). For example, the POS data field (foreign key) of a POS group is linked to the respective POS table based on the POS element identifier (primary key).

The database should include one or more tables for each analysis element type. Some functionality that could be useful includes:

- Data could be inherited from an analysis element to another one. E.g. a POS group combination could automatically inherit multi-unit initiators from the POS groups participating in the combination.

- It would be useful to sort tables according to different attributes.

- It could be useful to customize tables, because some of analysis elements include many data fields and the user may be interested only on specific fields at a time. In addition, some analysis elements, like multi-unit dependencies and multi-unit initiators, go through multiple analysis phases and only some of the data fields are relevant for a single analysis phase. It could be useful to have different header sets or tables for different analysis phases.

- Filtering of data could be useful. For example, the user could want to view only those multi-unit dependencies that are screened in for further analysis.

- Since several analysis elements are connected, data links could be used so that it would be possible to e.g. jump from the data of multi-unit initiator to the data of an associated POS group combination.

- Convenient ways for viewing data need to be considered. For example, it might be useful to view data only related to a single multi-unit analysis case because there are a lot of data connected to an analysis case (considering also the data of the multi-unit initiator and POS group combination of the analysis case).

- Search functions would be useful (available in normal Excel application).

- It should be possible to export selected tables to the site PSA document.

- Since some computations need to be performed with the data, the computation formulas could be built in into the database system. For example, some inter-unit CCF probability estimation formulas could be useful.

- Some data, like some initiating event frequencies and single-unit CCF probabilities, come from the databases of single-unit PSAs. Functionality to facilitate such data imports can be considered.

It can be useful to extend the database with a new analysis element: multi-unit scenario, which has been defined in Section 2. It is needed if the multi-unit event combinations approach (see Section 2) is used in quantification, and could be of interest also otherwise. A multi-unit scenario could have the following data fields:

- Identifier
- POS group combination
- Multi-unit initiator
- Multi-unit basic events
- Frequency
- The related initiating/basic events in the single-unit PSA models
- The CCDP in each unit (given the multi-unit initiator, POS group combination and multi-unit basic events)
- The MUCDF of the scenario (for each combination of units if there are more than two units)

The multi-unit scenarios could be created automatically based on the multi-unit analysis cases. An event tree presentation of a multi-unit analysis case could also be created. The multi-unit basic events would be the nodal questions in such event tree, and each sequence would represent a multi-unit scenario.

If the minimal cut set list approach (see Section 2) is used in the computation, the combined minimal cut set list needs to be treated with a set of rules to ensure correct quantification. The database could support the practical implementation of such rules. For example, rules could be created automatically based on the multi-unit initiators and multi-unit basic events in the database or the database could directly serve as a set of rules if it was integrated with the computation tool. A typical example of a rule would be that two single-unit basic events related to the same multi-unit basic event are identified in the same minimal cut set, and the frequency of the minimal cut set is increased according to the probability of the multi-unit basic event.

If minimal cut set lists are combined in the site PSA, different units cannot contain single-unit events with the same names. If there are same names, the names need to be changed to unit specific at some point. The change of names can take place when the minimal cut sets are pre-processed for the combination in site PSA. The database needs to contain information on the correspondence between the names used in the single-unit PSA and site PSA.

The quantification of the minimal cut sets could also utilise the site PSA database. Alternatively, relevant initiating event and basic event data from the site PSA database could be imported to the software tool used. In this latter case, an interface between the database system and the software tool would need to be developed.

7. Guidelines for site PSA model management

Table 2 presents the main documentation and model management tasks in different analysis phases and in the maintenance phase. In this section, the whole analysis process is gone through from the documentation and model management point of view.

Table 2: Documentation and management tasks in different analysis phases.

Analysis phase	Documentation	Model and database management
Selection of analysis scope and risk metrics	Documentation of the scope and risk metrics	
Preparations before analysis	Documentation of references and PSA model versions	
Analysis of POS impact	Documentation of the POS analysis process and results	Insertion of POSs, POS groups and POS group combinations to the database
Identification of multi-unit initiators	Documentation of the initiator screening process and results	Insertion of multi-unit initiators to the database
Identification and selection of dependencies	Documentation of the dependency screening process and results	Insertion of dependencies to the database, screening of dependencies with the single-unit models, insertion of multi-unit basic events to the database
Analysis of source terms (level 2 only)	Documentation of the source term analysis process and results	Insertion of source terms, source term combinations and release categories to the database
Data analysis	Documentation of the data analysis process and results	Systematic analysis of those multi-unit initiators and basic events that were screened in using the database, insertion of frequencies of initiating events and probability parameters related to multi-unit basic events to the database
Quantification of multi-unit risks	Documentation of the results	Computation based on the single-unit models and database
Maintenance of site PSA	Update of relevant parts of the documentation when needed, documentation of changes	Process for updating site PSA, model configuration management, version control, verification and validation of model changes

Besides the above listed analysis phases, for level 2 purposes, it might be necessary to dedicate a step for the assessment of multi-unit plant damage states.

7.1 Selection of analysis scope and risk metrics

The analysis starts with the selection of scope and risk metrics. Recommended risk metrics have been documented in [4]. In the selection of the scope at least the following issues should be considered:

- Radionuclide sources that are considered
- PSA levels and end states included in the analysis
  - Release categories need to be selected if the analysis covers level 2. The release categories can be the same as in single-unit PSAs, but the analysis can also be simplified by creating larger release categories and not considering release timings in the release categorisation. It is possible to consider only one release category of large or unacceptable release, which is considerably simpler than the analysis of multiple

smaller release categories. Release categorisation may also be decided later after the analysis of source term combinations.

- Types of initiators considered
- Operating states considered
- The scope of SSCs considered including the fixed date for the plant (site) configuration being analysed.

These selections are documented in the chapter Selection of analysis scope and risk metrics in the site PSA document.

7.2 Preparations before the analysis

PSA model versions that are used in the analysis are selected and documented. It is possible to make some adjustments to the model versions before the analysis, e.g. concerning release categorisation or modelling of multi-unit aspects as discussed in Section 4.2.

The main source documents are listed in the site PSA document.

7.3 Analysis of POS impact

Analysis of POS impact is performed in the following steps:

1. Review POSs to obtain basic information on their differences. Pay particularly attention to the status of the primary circuit and available core cooling and residual heat removal systems.

   Steps 2-5 concern an individual unit. If the units are similar with regard to POSs, the procedure can be performed only for one unit, but otherwise it needs to be performed for each unit separately.

2. Make a table of POSs e.g. with the following headers: POS identifier, description, time share, status of primary circuit, status of the core cooling system, status of the residual heat removal system and status of the spent fuel pool. The relevant systems to be included here are plant specific and more headers should be included if there are more systems.

3. Merge together those POSs that are sufficiently similar to form POS groups. The grouping can be based on the configuration of residual heat removal systems as discussed in Section 4.2 of [1].

4. Make a table of the **individual** POS groups with the following headers:

   a. POS group identifier

   b. Specific POSs belonging to the group

   c. Justification for the grouping

   d. Estimated time share

   e. Time window for core/fuel damage in case of loss of residual heat removal

   f. Screening decision and justification

Add the POS group table to the site PSA document.

5. Estimate the time shares of POS group **combinations**. Consider only the POS groups that have been screened in.

6. Make a table of POS group combinations with the following headers:

    a. POS group combination identifier

    b. For each unit, the POS group included in the combination

    c. Estimated time share

    d. Screening decision and justification

    Add the POS group combinations table to the site PSA document.

7.4 Identification of multi-unit initiators

1. Go through the initiating events in the single-unit PSA models and categorize them in the following groups:

    - single-unit initiating event
    - multi-unit initiating event
    - partial multi-unit initiating event

2. Analyse the possibility that a single-unit accident introduces an initiating event in another unit (or that a multi-unit accident of two units introduces an initiating event in third unit, etc.). Make a list of potential cases.

3. Make a table of multi-unit initiators (including partial multi-unit initiating events and propagating accidents) e.g. with the following headers:

    a. Identifier

    b. Category (multi-unit initiating event, partial multi-unit initiating event or single-unit event that propagates to another unit)

    c. Description

    d. Frequency (may not be available at this point for all events)

    e. Screening decision and justification

    f. Source documents

    g. The corresponding initiating events in the PSA models

    h. Relevant POSs

    i. POS dependency

    j. Season dependency

    k. POS group combinations to be included in the analysis and justification

4. Divide each partial multi-unit initiating event into multi-unit initiating events corresponding to different unit combinations and into single-unit initiating events. Add the information on this process to the database and site PSA document. Add the new multi-unit initiating events to the previous table. The category for these events is a 'multi-unit initiating event that originates from a partial multi-unit initiating event.' The other data, except the frequency, can be inherited from the original partial multi-unit initiating events.

   Add the multi-unit initiator table to the site PSA document.

5. Make a table of the multi-unit analysis cases. For each analysis case, at least the following information needs to be included (possible to complement with information related to the initiator or POS group combination):

   a. Identifier

   b. Multi-unit initiator

   c. POS group combination

   List the multi-unit analysis cases in the site PSA document.

7.5 Identification and selection of dependencies

7.5.1 Qualitative analysis

1. Identify all multi-unit dependencies. Some guidance can be found in Sections 5.2 and 6 of [1]. The identification of human action dependencies is specifically discussed in Sections 8.2-3 of [1].

2. Make a table of multi-unit dependencies with e.g. the following headers:

   a. Identifier (name)

   b. Dependency category (shared SSC, identical components, spatial dependency, human dependency, simultaneous maintenance or phenomenological uncertainty)

   c. Description (e.g. systems and components involved)

3. Analyse each dependency qualitatively and define the qualitative ranking according to the categories defined in Table 5.1 of [1].

4. Add the following information of each dependency to the dependency table (if applicable):

   a. Qualitative ranking and its justification (reasoning behind it)

   b. Source documents

   c. The units to which the dependency is related, if there are more than two units

   d. Basic events related to the dependency in the single-unit PSA models

   Add the multi-unit dependency table to the site PSA document.

7.5.2 Quantitative screening

1. Screen each previously screened in multi-unit dependency quantitatively based on single-unit basic events as presented in Section 5.2.2 of [1]. For each dependency, add the following information to the database and site PSA documentation:

    a. Fussell-Vesely in each multi-unit initiating event in each unit

    b. The increase factor (defined in [1]) in each multi-unit initiating event in each unit

    c. Maximum contribution from potential multi-unit sequences in each unit

    d. Screening decision

    Note that if the analysis covers level 2, at least the level 2 dependencies need to be screened on the basis of release category frequencies. It is possible to perform the screening for multiple release categories separately.

2. For each screened in dependency, identify the relevant multi-unit initiating events. The previously calculated Fussell-Vesely values can be utilised. Make a table of the multi-unit analysis cases specifying the relevant multi-unit dependencies for each analysis case.

3. Based on each screened in multi-unit dependency, define one or more multi-unit basic events. Make a table of the multi-unit basic events e.g. with the following fields:

    a. Identifier

    b. Description

    c. Related multi-unit dependency

    d. Source documents

    e. Related units (if there are more than two units)

    f. Related basic events in the single-unit models

4. Make a table of the multi-unit analysis cases specifying the relevant multi-unit basic events for each analysis case based on the relevant dependencies.

7.6 Analysis of source terms (level 2 only)

1. Review source terms of individual units. Determine which source terms are relevant for the screened in MUIEs. Make a table of source term categories, with the following headers: Source term category identifier, description, screening decision (based on relevance for selected MUIEs and possibly based on single-unit level 2 PSA results) and justification. The description header can be split into several headers describing specific characteristics of the source term category.

2. Analyse combined source terms from individual units and how they are associated in different release categories. Assess the relevance of source term combinations for multi-unit analysis. Screen out insignificant combinations. Make a table for source term combinations with headers: Group identifier, associated release category, screening decision, and justification for screening and how the combined source terms are associated in the release category.

3. Review selected release categories based on analysis results. Make a table of release categories with headers: identifier, description, source term combinations.

4. Add the source term combinations table to the site PSA document. If release categories have been changed, update the Selection of analysis scope and risk metrics chapter in the site PSA document accordingly.

7.7 Data analysis

7.7.1 Initiating events

1. Go through each partial multi-unit initiating event. If at least one multi-unit initiating event that has been created based on the partial multi-unit initiating event has been screened in, estimate the corresponding frequency/frequencies as discussed in Section 7.2.2 of [1].

   Write the following information of each partial multi-unit event in the site PSA document if applicable:

   - Data sources
   - How the frequencies have previously been estimated for individual units
   - The frequencies used in single-unit PSAs
   - Summary of operating data
   - Qualitative analysis including
     - different causes for the event and how they affect units
   - How the new frequencies are estimated for multi-unit analysis
   - The frequencies of the new multi-unit initiating events.

   A database table with the above information for each partial multi-unit event can also be made.

2. Make a table of all multi-unit initiators that have been screened in. The headers of the table can be e.g.:

   a. Identifier

   b. Affected unit combination (if there are more than two units)

   c. Data sources

   d. How the frequency is estimated

   e. Frequency (total annual frequency)

   Add the table to the site PSA document.

3. Estimate the frequency of each multi-unit initiating event in each POS group combination that is relevant for the initiating event (if not already available). If an initiating event has no POS dependence, the annual event frequency can be multiplied

by the POS group combination time share. If an initiating event depends on POSs, it is expected that POS specific frequencies can be found in the single-unit analyses.

4. Make a table of multi-unit initiating events and POS group combinations. Each cell of the table specifies the frequency of the corresponding initiating event in the corresponding POS group combination. Add the table to the site PSA document.

7.7.2 Multi-unit basic events

1. Estimate the probability of each inter-unit CCF that has been screened in according to formulas presented in Section 7.3 of [1].
2. Make a table for inter-unit CCFs including the following information for each CCF if applicable:
    a. Identifier
    b. Component type
    c. Failure mode
    d. Units (if more than two units are analysed)
    e. Group size
    f. CCF combination (or combinations if multiple combinations are merged)
    g. Data sources
    h. Single-unit CCF probability in each unit
    i. Summary of operating data
    j. Model used in the estimation
    k. Parameters used in the estimation
    l. Probability of the inter-unit CCF

    Add the table to the site PSA document.
3. Estimate the probability of each multi-unit human error event. Section 8.4 of [1] provides instructions for two different estimation methods.
4. Make a table of multi-unit human error events e.g. with the following headers:
    a. Identifier
    b. Description
    c. Related basic events in the single-unit models
    d. Probabilities of the basic events in the single-unit models
    e. Qualitative assessment from the multi-unit point of view
    f. Multi-unit probability estimation method

g. Multi-unit penalty factor or dependency category [1] in each multi-unit analysis case

h. Probability in each multi-unit analysis case

Add the table to the site PSA document.

5. If other types of multi-unit basic events have been screened in, their probabilities also need to be estimated and documented (possibly separately for each multi-unit analysis case). Section 7 of [1] provides some guidance on the data analysis of different types of multi-unit dependencies.

7.8 Quantification of multi-unit risks

Two methods for the quantification of multi-unit risks are presented in [1]. One is based on computation of conditional core damage probabilities of multi-unit event combinations, and the other one is based on combination of the minimal cut sets of the units. They are discussed separately in the following subsections.

7.8.1 Multi-unit event combinations approach

For each multi-unit analysis case (multi-unit initiator and POS group combination) that has been screened in:

1. Create an event tree with relevant multi-unit basic events.

2. Calculate the frequencies of the multi-unit scenarios based on the event tree.

3. For each multi-unit scenario that has a frequency larger than the selected screening threshold (e.g. 1E-8/year for level 1 and 1E-9/year for level 2), calculate the CCDP in each relevant unit. If there is no advanced computation support available, the calculations can be performed in the following way:

    a. Set the initiating event frequency to 1 and the probabilities of the basic events related to the multi-unit basic events to 1 (or statuses to “failed”). If needed, select also the correct POS. For example, if there is a basic event representing the time share of the POS, its probability needs to be set to 1.

    b. Make sure that other initiating events do not skew the result. It should be possible to focus on the initiating event specific results. Even if multiple initiating events appear in the same event tree, the result can be calculated by multiplying the total frequency with the Fussell-Vesely of the initiating event. Alternatively, the frequencies of other initiating events can be set to 0.

    c. Successes of multi-unit basic events can also be taken into account (optional). It should be noticed that even though a multi-unit basic event does not occur, a related single-unit basic event may occur. A portion of the probability of the single-unit basic event comes from the multi-unit event. This portion can be subtracted from the probability of the basic event to make the computation more accurate.

    d. Calculate the event tree in the single-unit model, or reminimize and recalculate the corresponding minimal cut set list to get the conditional core damage probability.

If the analysis covers level 2, the CSTP is calculated for each considered source term category in each relevant unit.

The following concerns all multi-unit analysis cases together.

4. Make a table of the multi-unit scenarios (can be initiating event specific or cover all initiating events). For each multi-unit scenario, it can include the following information:

    a. identifier of the multi-unit initiator

    b. Identifiers/names of the multi-unit basic events

    c. The POS group combination

    d. The frequency of the scenario

    e. The related basic events in the single-unit PSA models

    f. The CCDP in each unit

    g. The MUCDF of the scenario (for each combination of units if there are more than two units)

    If the analysis covers level 2, the CSTP value of each source term category in each unit, and the MUSTF of each source term category combination (for each combination of units if there are more than two units) are included.

    Add the table(s) to the site PSA document.

5. For each unit combination (if there are more than two units), calculate the MUCDF by summing the MUCDF values (related to the analysed unit combination) of all multi-unit scenarios. Report the calculated MUCDF values in the site PSA document.

    If the analysis covers level 2, calculate the MUSTF of each relevant source term category combination for each unit combination.

6. Calculate the SCDF.

    If the analysis covers level 2, calculate the site level frequencies of release categories.

7. Calculate and document relevant risk importance measure values.

8. Make conclusions on the results and write them to the site PSA document.

7.8.2 Minimal cut set list approach

1. Pre-process minimal cut sets of individual units if needed. If different units have single-unit events with the same names, the names of the single-unit events need to be made unit specific.

2. Combine minimal cut sets of different units to make the minimal cut set list(s) needed for the quantification. One option is to make a minimal cut set list for “site level core/fuel damage”, i.e. a list containing the minimal cut sets of all units. Another option is to create a minimal cut set list for “multi-unit core/fuel damage” by multiplying the minimal cut sets of different units (according to Boolean algebra). If there are more than two units, minimal cut sets lists can be created for different unit combinations. Both options can be used to calculate the site core/fuel damage frequency. The needed minimal cut set lists depend on the selected risk metrics.

If the analysis covers level 2, one option is to make a minimal cut set list for each analysed release category at the site level. Alternatively, minimal cut set lists can be generated for different source term combinations, and the risk metrics can be calculated based on the frequencies of the combinations.

3. Prepare the database and rules for the quantification of the minimal cut sets (if not ready already based on the previous analysis phases).

4. Calculate the selected risk metrics from the minimal cut set lists.

5. Calculate relevant risk importance measure values from the minimal cut set lists and document them.

6. Make conclusions on the results and write them to the site PSA document.

8. Maintenance of site PSA

It is recommended that the names and locations of documents and files used in the analysis are listed in the site PSA document chapter Documents and files used in the analysis. All files and documents should also have version numbers.

To maintain the site PSA, a log of changes needs to be maintained. All changes in site PSA input data need to be documented in the log. The model changes need to be documented so that they can be traced back to the inputs. Single-unit models need to always be updated before site PSA. When the site PSA is updated, it is recommended that the whole analysis procedure and site PSA document are gone through with the list of changes, and the relevant parts of the database, site PSA document and calculations are updated step by step. Summary of those updates should also be added to the log. New versions of modified documents and files should be created.

If special versions of single-unit models are needed for site PSA, it is likely better to create the special versions based on the current single-unit models every time when the site PSA is updated, instead of maintaining alternative versions of the single-unit models along with the main versions.

9. Conclusions

In this report, guidance for site PSA model management is given and requirements for a site PSA database are specified. This report follows the developed site PSA approach [1] and it considers the same analysis phases.

Site PSA's requirements for single-unit PSA models are discussed, and documentation and database needs for site PSA are presented. Analysis phase by phase guidelines for site PSA documentation and model management tasks are given. Also site PSA maintenance is discussed. The guidelines can also guide the performance of the actual analysis and serve as a checklist. The focus of the report is on level 1 issues, but also level 2 aspects are covered.

The guidelines presented in this report are meant to support the developed site PSA approach [1] and they are not applicable as such to alternative approaches. These guidelines need to be kept up-to-date with possible method updates and modifications.

References

1. Bäckström, O., He, X., Holmberg, J-E, Tyrväinen, T. SITRON – Method development. Report 212634-R-001 Draft v1.09, Lloyd's Register, 2018.

2. Tyrväinen, T., Häggström, A., Bäckström, O., Björkman, K. A methodology for preliminary probabilistic multi-unit risk assessment. VTT-R-00086-17, VTT Technical Research Centre of Finland Ltd, Espoo, 2017.

3. Tyrväinen, T, Björkman, K. Requirements for site level PSA model management. VTT-R-00025-18, VTT Technical Research Centre of Finland Ltd, Espoo, 2018.

4. Holmberg, J.-E. SITRON — Risk metrics. Report 14124_R005, Risk Pilot Ab, Espoo, 2017.

Appendix D – WP5 Technical support centre

Massaiu, S. 2019. Decision-making during severe and multi-unit accidents: Technical Support Centers and Emergency Response Organizations at Nordic Countries, IFE/F-2018/189, Institute for Energy Technology, Halden.

IFE/F-2018/189

Decision-making during severe and multi-unit accidents: Technical Support Centers and Emergency Response Organizations at Nordic Countries

<table>
<tr><td>Report number
IFE/F-2018/189</td><td colspan="2"></td><td>Availability:
Public</td></tr>
<tr><td>Date:
December 2018</td><td>Revision:</td><td>DOCUS ID:
30326</td><td>Number of pages: 30</td></tr>
<tr><td colspan="4">Client: Nordisk Kjernkraftsikkerhet (NKS)</td></tr>
<tr><td colspan="4">Title:
Decision-making during severe and multi-unit accidents: Technical Support Centers and Emergency Response Organizations at Nordic Countries</td></tr>
<tr><td colspan="4">Summary:
Site-level risk analysis needs to evaluate the likelihood that actions taken by plant personnel will prevent, reduce, or delay, large radioactive releases that may follow single or multi-source severe fuel damage accidents. In these accidents almost all safety issues are resolved through operator actions which serve as preventive measures. The Emergency Response Organization (ERO) and the Technical Support Center (TSC) have thus a crucial role.

This report describes the ERO/TSCs at Nordic nuclear power plants for identifying functional characteristics that might impact operational decisions during severe and multi-unit accidents. These include the roles, responsibilities and the allocation of accident mitigation tasks, including the criteria for activation and location of the TSCs, their interactions and communications with the main control room personnel and other plant personnel, as well as the staff competence building. Plants' self-assessed general and specific operational challenges to their TSCs/EROs in severe/multi-unit accidents are reported.

The report also compares how the different plants credit the TSC role in Probability Safety Analyses (PSA) for multi-unit events. The TSC is not modeled in detail as this is assumed to have a limited impact on the HRA accuracy and the PSA results.

The report thus provides a concise reference source of generic and plant-specific information related to the TSC role in responding to severe and site-level accidents, a necessary first step for including it in PSA/HRAs and, possibly, a useful complement for further progress on severe accidents preparedness.</td></tr>
<tr><td colspan="4">Prepared by (digitally signed): Salvatore Massaiu</td></tr>
<tr><td colspan="4">Reviewed by (digitally signed): Xuhong He</td></tr>
<tr><td colspan="4">Authorised by (digitally signed):</td></tr>
</table>

Institute for Energy Technology
P.O. Box 40, NO-2027 Kjeller, Norway / P.O. Box 173, NO-1751 Halden
Telephone: +47 63 80 60 00/ +47 69 21 22 00
http://www.ife.no / firmapost@ife.no

Acronyms and abbreviations

Acronym	Description
BWR	Boiling water reactor
DLC	*Driftledningcentralen*. Unit-level operation management center at Plant C NPPs
EC	Emergency center. Also ERC, ECC.
ECC	Emergency command center. Also EC, ERC.
EM	Emergency manager. Also, ERO director, EPM.
EOP	Emergency operating procedure
EPM	Emergency preparedness manager. Also, EM, ERO director
EPO	Emergency preparedness organization
ERC	Emergency response center. Also EC, ECC.
ERO	Emergency response organization
FCV	Filtered containment venting
HEP	Human error probability
HFE	Human Failure Event
HORAAM	Human and Organizational Reliability Analysis in Accident Management
HRA	Human reliability analysis
KC	*Kommandocentralen*. Emergency Command Center, ERC at Plant C NPP
LOCA	Loss of coolant accident
LOOP	Loss of outside power
LUHS	Loss of ultimate heat sink
MCR	Main control room
NPP	Nuclear power plant
OL	*Områdesledare*. ERO director at Swedish NPPs
OSSA	Operating Strategies for Severe Accidents
PSA	Probability safety analysis
PWR	Pressurized water reactor
SACRG	Severe accident crew guidelines. Element of Westinghouse plants' SAMGs
SAM	Severe accident management
SAMG	Severe accident management guidelines
SPAR-H	Standardized plant analysis risk-Human reliability analysis method
STUK	*Säteilyturvakeskus*. Radiation and Nuclear Safety Authority of Finland
THAL	*Teknisk handbook för anläggningsledning*. Plant C NPP's SAMGs
THERP	Technique for human error-rate prediction
TS	Technical support
TSC	Technical support center
UDM	Ultimate decision maker
VHI	*Vakthavande ingenjör*. Engineer on duty at Swedish NPPs
VVER	Water-water energetic reactor

Contents

1 Introduction

Most nuclear power stations sites house more than one reactor unit as well as other nuclear facilities such as spent fuel pool storage. After the Fukushima Daiichi accident in March 2011 general interest has increased in assessing the site/multi-unit risk, and not only the risk of a single reactor, as traditionally done. One of the new issues posed by assessing the site-level risk is to evaluate the role of the emergency response organization (ERO)[1] in nuclear power plant multi-unit scenarios, and more specifically the impact of the decisions of the technical support center (TSC), the operating unit responsible to prevent, reduce, or delay large radioactive releases that may follow single or multi-unit severe core damage.

1.1 Objectives and methodology

This report describes functional characteristics of Nordic nuclear power plants' TSCs (and key elements of the broader EROs) that might impact on operational decisions during severe and site-level accidents. This report also compares how the different plants credit the TSC role in Probability Safety Analyses (PSA) for multi-unit events. The report is intended to serve as quick-reference source for supporting the qualitative phase of site-level and level-2 PSA analysis.

The report includes a brief literature review on: (a) the TSCs and EROs roles in making operational decision during severe, site-level accident mitigation activities: (b) how the TSC role is addressed in Human Reliability Analysis (HRA); and (c) on the currently acknowledged challenges faced by the TSCs and EROs' decision makers.

Based on the literature reviews a semi-structured questionnaire has been developed and sent to ERO specialists and PSA analysts at the five Nordic power plants with nuclear reactors in operation. Four of these have answered and the responses have been elaborated and summarized here.

1.2 Severe accidents and Technical Support Centers

All nuclear power plants in the Nordic countries have an emergency plan which activates an emergency response organization (ERO) on certain predefined criteria (Jaworska, 2002). The ERO includes actors at the plants, utilities, and local as well as national authorities (for the Nordic EROs see Drøivoldsmo, Porsmyr, & Nystad, 2011). The technical support center is the part of the ERO that is in charge or will contribute to operational decisions at the plant during a severe accident. TSC tasks may include: (a) determining the plant damage state; (b) evaluating and selecting strategies to bring the plant to a controlled stable state; (c) organizing components and systems repairs; and (d) directing actions to be performed by the Main Control Room (MCR) operators and other personnel outside the TSC.

The exact tasks as well as the specific implementation of TSC is utility or even site-specific. While in the United States the responsibility for handling the plant in severe accidents is brought outside the main control room (Vayssier, 2012) some plants in Europe maintain the authority to take actions in the control room, e.g., by having the main control room operators implement (part of) severe accident management guidelines (SAMGs) or by locating the TSC in the main control room building. Central TSC characteristics, such as its functional role, location, available technology, as well as its interaction with the main control room and with the ERO director (typically named Emergency Manager, EM) for ultimate decision making, vary from plant to plant.

[1] Also called emergency preparedness organization (EPO).

1.3 TSC/ERO challenges

The ERO and TSC are activated for the most serious emergencies at nuclear power plants. These include severe accidents, that is core-melt accidents, events most plants were not designed to control (and hence called beyond design-basis accidents). Until the Three Mile Island unit 2 (TMI-2) accident in 1979 emergency operation (the prevention of core melt) was the last frontier of reactor safety (Sehgal, 2016). Severe accident research started immediately after the TMI-2 accident in order to establish whether the installed plants required substantial backfits to prevent the initiation and mitigate the consequences of severe accidents (id.). European countries focused on hardware changes to increase the existing reactors safety, while the United States Nuclear Regulatory Commission (U.S. NRC) in addition started the Accident Management Program for developing SAMGs (Vayssier, 2012).

In severe accidents the role of the ERO and TSC is crucial as "almost all of the severe accident safety issues are being resolved through operator actions during the severe accident management, which serve as preventive measures" (Sehgal, 2012). Examples are the timing and extent of water addition as a prevention measure for elimination of the possibility of containment failure with Direct Containment Heating in a high-pressure accident, or igniter activation/operation in hydrogen control processes.

The main challenge for the ERO/TSC is constituted by the fact that severe accident phenomena are much more complicated than design-basis accidents. They describe the interactions of core melt with water and reactor structures that may lead to vessel/containment integrity failures and large radioactive releases, interactions "not easy to comprehend by an operator or even by a practicing severe accident expert" (id.)(Vayssier, 2016). As most plants were not designed against severe accidents events, the mere application of SAMGs may not prevent large releases, although it can delay or reduce these (Vayssier, 2012).

Specific challenges for the ERO and TSC are identified by research, analysis of real events and by observation of ERO emergency drills (Vayssier, 2014)(Kaarstad et al., 2016)(Liinasuo & Koskinen, 2017). Examples are:

- Command and control issues:
    - Unclear understanding of own role and responsibilities in the accident.
    - Mistrust between groups.
    - Over-centralization of decisions.
    - MCR staff acceptance of "losing" authority.
    - Unclear understanding of roles and responsibilities in accidents involving disruption of communication lines / relocation of control centers.
    - Unclear ERO/TSC/MCR authority over operations on the field.
- Communication and coordination issues:
    - Multiple actors and control centers spread in different locations on-site and off-site.
    - Unfamiliarity with communication protocols (e.g., phonetic alphabet, three-way communication).
    - Workload due to "bureaucratic" work.
    - Interaction with multiple parties providing conflicting information/advice.
    - Delays in information transmission / unsynchronized groups.
- Decision making issues:
    - MCR willingness to leave the (more familiar) EOPs.
    - Unclear criteria to enter SAMGs / degraded indications on the criteria.
    - Use of generic SAMGs not adapted to own plant.
    - SAMGs not indicating the details of restoring systems, supporting systems and the time windows of repair actions.
    - Evaluating instruments reliability; dealing with degraded/failed indications.

  - Evaluating/quantifying negative consequences of action alternatives on the fly, under the stress of the ongoing accident.
  - Time needed to understand the causes of an abnormal plant behavior vs. time available for timely operator actions.
  - Use of emergency mobile equipment in the mitigating domain (after core melt).
- Training issues:
  - Lack of realistic training with simulators reproducing chaotic and stressful severe accidents conditions.
  - Lack of feedback on the effects of operational decisions on the accident evolution in emergency drills.
  - Lack of training with lost communication infrastructure and/or inhabitability of control centers.
  - Lack of training to sudden complications and deviations from pre-analyzed paths and decision making that deviate from guidelines (i.e., training to switch between compliance and initiative).
  - Emergency drills that last significantly less than the simulated emergencies.
  - Lack of training on shift takeover.
  - Training not simulating communication both inside and outside the plant.

1.4 Human Reliability Analysis and Technical Support Centers

Historically the main focus for Human reliability Analysis (HRA) has been on supporting Level 1 Probability Safety Assessment (PSA), that is, to estimate the likelihood of the main control room 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 Fukushima accident has reminded the importance of and renewed the interest for conducting HRA also for Level 2 PSA, that is, with accidents scenarios after core damage has occurred (i.e. severe accidents) and for conditions involving multi-unit events.

Human actions in severe accidents are considered to differ from emergency actions covered by Level 1 PSA in several respects (Arigi, Kim, Park, & Kim, 2018), (Park, Ham, D. H., & Jung, W. J., 2018); (St Germain, Boring, Banaseanu, Akl, & Xu, 2016); (Fauchille, Bonneville, & Maguer, 2014); (Cooper, Xing, & Chang, 2013); Raimond et al., 2013):

- Decision-making responsibility shifts from the MCR to the ERO/TSC;
- The formalized guidance for severe accidents is provided by Severe Accident Management Guidelines that differ from EOPs in a number of ways, including goals and priorities, rules for compliance, and skills required for making complex evaluations and decisions;
- Decisions involve trade-offs between positive and negative consequences, novel and out of ordinary actions, as well as strategies contrary to conventional knowledge;
- Instrumentation reliability is less accurate, e.g., loss of instrument precision when exposed to extreme environmental conditions, loss of critical instrumentation during station blackout;
- Different temporalities, with time windows for SAMG actions spanning from several hours up to 72 hours.

Multi-unit or multi-source accidents pose additional issues. First, the decisions and responses are more complex and less supported by SAMGs than in single unit level 2 PSA. Second, decisions on shared resources create dependencies between units (Bareith, 2018). Yet positive dependencies can also occur, insofar lessons learned by one unit can be passed on to other affected units. This happened at Fukushima when procedural actions, timing for actions (e.g., how long it took to perform an operation), requirements (preconditions for action), and challenges encountered were passed on from unit to unit (Kaarstad et al., 2016).

Despite these important differences, HRA methods developed for Level 1 PSA are applied to PSA Level 2 (especially THERP and SPAR-H) by using expert judgment in the quantification of each HFE (Raimond et al., 2013).

HORAAM (Human and Organizational Reliability Analysis in Accident Management) is a HRA method specifically developed for treating the Human Error Probabilities (HEPs) of the actions contained in the SAMGs. HORAAM predicts human error probabilities based on a decision tree structure, in which 7 influence factors are characterized as “favorable”, “medium” or “unfavorable”. The factors consider aspects such as:

- the decision-time available;
- the availability of correct information;
- the severity of decision consequences;
- the adequate representation of the plant state;
- the necessary compromises in the decision;
- the availability of experts in the TSC and their ability to make good decisions based on their understanding.

The possible values of the influencing factors along the branches of the decision tree results in Human Error Probabilities (HEPs) that vary from 1E-4 to 1. A combination of several “unfavorable” modes rapidly leads to a failure probability of 1. Conversely, if all the influence factors take the “favorable” mode, the failure probability is 1E-4.

The qualitative analysis of the Influencing Factors in HORAAM can consider organizational factors impacts of site-wide accidents in internal event PSAs (LUHS/LOOP), e.g., one safety engineer for twin units, long time aspects (Dupuy, 2018). Yet, the qualitative analysis is sensitive to user’s differences and fully developed user’s guide is not available. Furthermore, the existing catalogue of influencing factors does not fully cover the decision-making dimensions of severe accident tasks (Park, 2018), so that the method has limits also as a simple checklist for aiding expert judgment elicitation.

Operator actions generally considered in Level 2 PSA for different reactor types are listed in Table 1 below (Raimond et al., 2013). However, there is no general analysis of the effect of SAMG actions in current PSAs (Vayssier, 2016).

Table 1. Examples of PSA Level 2 operator actions

Reactor Type	Severe accident management actions
Gen II PWR	Depressurization of the primary circuit Core reflood (may include recovery of AC power) Containment spraying Containment venting Containment water filling for reactor cavity flooding Hydrogen risk management Manual closure of containment isolation valves Isolation or feeding of an affected steam generator
Gen II BWR	Depressurization of the primary circuit Core reflood (may include recovery of AC power) Boration to prevent recriticality Containment spraying Containment venting Lower drywell flooding Containment water filling – cooling of reactor pressure vessel from outside Manual closure of containment isolation valves

2 Technical Support Centers implementations at Nordic sites

There are 12 nuclear power units in operation in the Nordic countries. Four are in Finland (two sites) and eight in Sweden (three sites). One plant in Sweden has not answered to the survey and will not be covered by this report.

2.1 Plant A

At Plant A power plant the TSC is located outside the plant site (at the company headquarters, at far distance from the site). However, a Technical Support (TS) group is present on site. TSC functions are thus distributed in two different locations: within the power plant premises and at the company headquarters.

The Ultimate Decision Maker in an emergency is the Emergency Manager at the on-site Emergency Center (EC) supported by the TS personnel located both on-site and off-site. The EC and the TS groups are shared by the two power units.

2.1.1 Roles, responsibilities and accident mitigation tasks

The emergency organization at Plant A can mobilize 180 manpower. In case of Severe Accident (SA) situation the Severe Accident Management (SAM) expert (in the TSC) provides recommendations regarding the implementation of SAMGs to the Emergency Manager who maintains ultimate authority on the decisions (e.g., ultimate decisions maker). Figure 1 describes the emergency organization at Plant A.

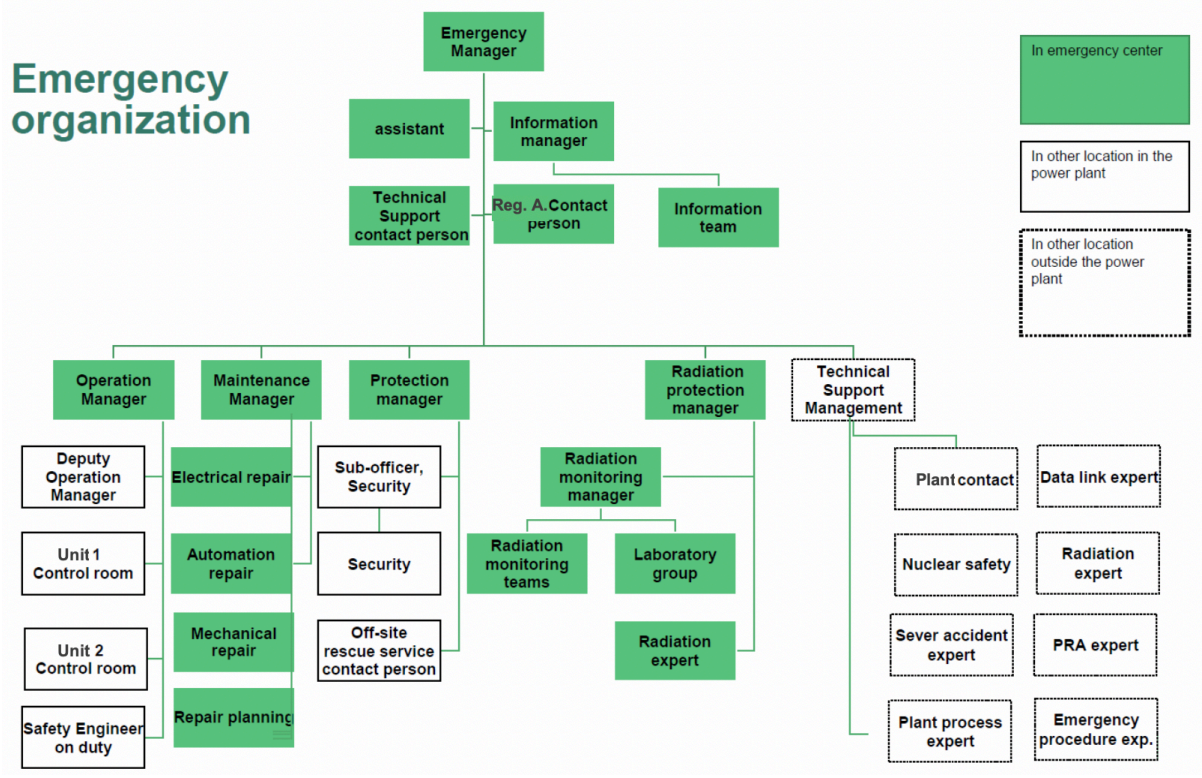


Figure 1. Emergency Organization at Plant A NPP. The site Emergency Center is supported by the Technical Support Center located off-site at the company's headquarters.

2.1.2 Activation and Location

TSC activation depends on the declared state. The emergency guidelines include criteria for declaring a state of alert, site emergency or general emergency. Emergencies are classified into three levels:

- Alert: the emergency organization is alerted to ensure the plant safety;
- Site emergency: safety deteriorates or is in danger of deteriorating significantly;
- General emergency: there is a hazard of a radioactive release that may require protective measures in the vicinity of the NPP.

The following events will trigger the activation of TSC:

1. **Alert:**
   - Leak from secondary circuit;
   - Fire e.g. at the main transformer area or turbine hall;
   - Sub-zero sea water temperatures (may lead into spontaneous freezing of water in cooling water tunnels which could cause blockage of water flow);
   - Small leakage within containment;
   - High sea water level (Plant A NPP has had one alert situation due to high sea water level in 2005).
2. **Site emergency:**
   - Primary coolant leakage during maintenance;
   - Primary-Secondary leakage;
   - Loss of coolant;
   - Loss of heat sink.
3. **General emergency:**
   - Situation where the reactor core outflow temperature exceeds 450 ˚C.

Location
The TSC is located outside the plant site (at the company headquarters, far from the site). A Technical Support group is also present at the site. Therefore, the operating company considers the TSC as distributed in two different locations: within the power plant premises and at the company headquarters.

2.1.3 MCR-TSC interaction and communication

The MCR shift supervisor acts as head of the TSC until he/she is relieved from that duty when the head of emergency preparedness organization arrives in TSC.

The MCR is responsible for directing the field operators (MCR personnel also include a field operator). The TSC groups can directly dispatch plant personnel to obtain local measurements and information (without asking the MCR). The MCR and TSC should coordinate about the operations at the plant. In case of disagreement the TSC has the authority can overrule decisions made by MCR operators.

The MCR mainly communicates with TSC. This happens through MCR and TSC dedicated contact persons. Not all TSC members can access the MCR, but the Emergency Manager can arrange needed permissions if needed. The TSC communicates also to other organizations.

Communication formats exist for communications between the site and the corporate headquarters. Technical jargon is forbidden in the web-based log tool notes. It is encouraged to avoid unnecessary technical jargon in other communication as well (e.g. via phone or email) but not prohibited.

Technology
The TSC on-site disposes of process computer display that shows basically all plant process variables, radiation levels from various locations within the power plant and from surrounding nearby

environment, as well as weather measurements near the power plant. This data also includes alarms and past log data. Process computers also include computational aids, like core performance and leak monitoring. The TSC off-site (corporate headquarters) has only essential information directly available.

The TSC's process computer data has worked well in emergency drills. However, the information provided by the plant simulator is only a sub-set of all the information that would be available in a real situation. These 'missing' variables include e.g., weather measurements, environmental radiation monitoring (dose rate) measurement and some radiation monitoring at the plant. Use of such 'missing' information is not practiced.

For communication between TSC and MCR fixed-line phones are used. Other communication means are: conference/video calls, mobile phones, satellite phones, chat, email, web-based log tool, Microsoft OneNote log tool, VIRVE network and fax. The TSC has also whiteboards to assist local communication.

2.1.4 Competence building

All new ERO members receive basic training on their role. Every member in the TSC's organization gets refresher training of few hours every year. Deepening training is provided when necessary. Before a person can officially be part of the TSC's emergency preparedness organization he/she needs to observe an emergency preparedness drill. Each position has a senior member who is responsible of taking care of that position's training (basic training, refresher training and deepening training).

2.2 Plant B

At Plant B the Emergency Response Center (ERC) led by the Emergency Preparedness Manager (EPM) is the ultimate decision maker responsible for operational decisions and actions at the plant. The ERC is located in the immediate proximity of the Main Control Room (MCR). The concept is that operating personnel, security personnel, radiation teams and maintenance teams carry out the actions at the plant units and inside the site area under the lea of the EPM. The ERC is thus in charge of functions that at the international level are normally assigned to the TSC, while at Plant B the TSC is a distinct support group that receives tasks and assignments from the Emergency Preparedness Manager and tries to focus on e.g., possible action plans, evaluation of radiological consequences, technical assessments, long term strategies as well as monitoring, reporting and evaluation of the events and plant status. Local authorities (rescue services) have the overall management and responsibility of the situation outside the site area and are responsible for e.g. evacuation activities and public communication.

2.2.1 TSC role in the Emergency Response Organization

The Emergency Preparedness Manager leads the ERO and is the ultimate decision maker. The ERO gathers in the immediate proximity of the affected main control room, inside the site area. The emergency response organization also comprises the Operation Manager, the Maintenance Manager, the Service and Evacuation Manager and the Radiation Protection Manager.

The TSC is a separate support group that gathers inside the site area, but not in the immediate proximity to the main control room. Its function is to assist the ERO managers. The TSC group carries out the tasks appointed by the EPM and issues recommendations to the EPM on the required operation and maintenance procedures. The TSC negotiates with the regulator STUK the required actions and procedures and assists the company management and communication center in acquiring the information that is to be presented to the media. It also initiates the planning of post-accident procedures and restoration procedures.

The Emergency Preparedness Manager is entirely responsible for the activities of the emergency organization in the event of an accident. Work appointed by the Emergency Preparedness Manager is considered emergency work. The Operation Manager in charge of the MCR activities and the work carried out in the field (which is supervised by the MCR). The MCR also manages other plant operations in the field in co-operation with the Maintenance Manager and the Operation Manager. Repair teams are assembled by the Maintenance Manager. The Service and Evacuation Manager handles the personnel transfers, food rationing, and communication links.

The Radiation Protection Manager supervises the radiation safety of personnel and releases to environment by monitoring personnel radiation doses and by estimating emissions and radiation doses to the environment.

The Emergency Preparedness Manager is also responsible for determining the emergency preparedness category and making the necessary alerts/notifications to the company headquarters and the authorities.

2.2.2 TSC activation and location

The MCR Shift Supervisors declare an emergency situation independently or in consultation with their superior. Alternatively, the Plant Meeting can also decide on initiating the emergency situation procedure. The decision is based on process information, radioactive emission information, and other relevant information.

The emergency preparedness categories are:

1. Alert
    - An alert is a situation where the safety level of the nuclear power plant needs to be ensured due to abnormal conditions.
    - Some other event which requires the emergency response organization to be activated as a precaution.
2. Site area emergency
    - A site area emergency is a situation where the safety of the nuclear power plant is significantly reduced, or is at risk of being significantly reduced
    - For example: Loss of coolant accidents, control rod inoperability during transients, preventing the reactor from being completely shut down by normal procedures and loss of external power supply and in-house emergency power systems, making operation according to normal procedures impossible.
3. General emergency
    - A general emergency is a situation during which there is danger of radioactive substance releases that may require protective measures in the vicinity of the nuclear power plant.
    - Measured or estimated dose rates outside the plant are more than 5 mSv/h to the whole body or more than 20 mSv/h to the thyroid gland.

Location

The ERO gathers inside site area and in immediate proximity to the main control room. The TSC gathers inside site area, but not in immediate proximity to the main control room. There is also an alternative location outside site area (about 20 km away from the site area).

2.2.3 TSC interactions and communications

After the alert has been given and sufficient amount of TSC personnel has arrived, the Emergency Preparedness Manager claims command of the situation. He/she typically visits the MCR to get the latest status update and to notify the MCR the command turnover. The Emergency Preparedness Manager then delegates tasks and communicates with the other managers.

The MCR keeps an active role and is likely to suggest actions to the Operation Manager. The Operation Manager keeps a close communication with the MCR for mitigation of the accident. The MCR can also proceed according to the instructions when available. Prioritization of actions can be decided by the ERO management and suggested by the TSC.

The MCR typically commands the field operators, together with the Operation Manager. Maintenance personnel work in close collaboration with the MCR and the Maintenance Manager. Many activities at the plant need the supervision, coordination and control of the MCR. The Maintenance Manager communicates with the repair teams.

Regular status updates and briefings are organized, e.g. every 30 minutes between the ERC and support group (TSC) so that everybody can stay up to date and share views of the situation. Regular status briefings typically follow a common format. Submittal of information to local nuclear regulator utilizes predefined written forms. Status updates to local nuclear regulator follow typically a schedule that has been agreed with the regulator. Brief updates and communications will also be written in the electronic emergency diary so that a common written log of the events and actions remains that can be accessed by all the involved parties.

Technology
Communication technology includes whiteboards, phone/radio, special phone system used by local authorities, telefax and electronic emergency diaries (one used by the company, some used mainly by the local authorities, access privileges arranged so that all relevant parties can read and follow the information given).

The Emergency Response Center has access to main process and system data, including alarms, coming from the affected unit (each unit has a separate ERC room). The room occupied by the TSC (support group) has access to such data from all three units. Separate screens (data panels) have been designed for emergency situations collecting together data relevant for accident situations (e.g. temperatures and radiation levels inside containment, operational status of systems needed for residual heat removal, etc.). For the two units in operation the data sent to the ERC and the TSC (support group) is limited, so not all measurement data is available. For the unit under construction almost all data available in the MCR is sent. Some plant data is also sent directly to the nuclear regulating authorities.

2.2.4 Competence building

Staff belonging to the emergency organization are nominated based on their experience and work activities. The idea is to include both experienced people and younger people who can learn from the senior members. The different roles are described in written instructions. One emergency exercise for the whole emergency organization is organized once a year. In addition to that there are 1-2 training lectures for the whole group every year and smaller training sessions and drills organized separately for different teams (e.g. radiation measurement teams, teams responsible for media communications).

2.3 Plant C

At plant C the Site Emergency Director (OL) at the Emergency Command Center (ECC) leads the ERO and is responsible for the whole site. The ECC is located inside the site area and not in the proximity of the units' main control rooms. Operational decisions at the unit level are taken at the Operation Management Center (DLC) where also the TSC gathers, in control centers specific for the units (outside the MCR at units 1 and 2, in the MCR at unit 3).

2.3.1 Roles, responsibilities and accident mitigation tasks

The Emergency Response Organization at Plant C is made of four groups:

- Emergency Command Center (KC)

- Operation Management Center (DLC)
- Technical Support Center (TSC)
- Main control room (MCR).

When summoned, the Emergency Command Center (ECC) deals with issues at site level. The ECC is staffed by managers, specialists and coordinators. The Site Emergency director (OL) leads the KC and is the “Ultimate Decision Maker”. This role is rotated among a small number of senior managers/experts at Plant C NPP.

When summoned, the Operation Management Center (DLC) deals with issues at the unit level for the affected unit. The DLC is staffed by unit managers and other personnel with operation experience and works in close cooperation with the main control room (MCR). A senior operation manager with the assigned role “DL2” heads the DLC.

When summoned, the TSC deals with issues at the affected unit level. The TSC is staffed by work supervisors in the areas of maintenance, radiation protection and chemistry. The TSC implements the decisions taken by the DLC.

Immediate severe accident mitigation actions are mostly covered by procedures (EOPs, AOPs, SAMGs) handled by the MCR with support from DLC/TSC/KC when these have summoned. The main control room (MCR) initiate the transition from the EOPs to the severe accident management guidelines (called THAL) when core melt starts, according to criteria in the EOPs. The EOPs handle early mitigation actions that often are included in SAMGs internationally. The engineer on duty (VHI) or the MCR shift supervisor takes the decision to transfer from EOPs to SAMGs (THAL). At this point the engineer on duty (VHI) takes command until the Emergency Command Center (KC) is summoned.

When turnover of command and control from the MCR to the Emergency Command Center (KC) has happened, the KS will have the strategic responsibility at the site level while the DLC at the unit level. Nuclear safety specialists will be present at the command center (KC) helping to diagnose plant conditions and assessing damage state. Specialists from the plant owner will also support from an emergency situation room at the utility headquarters far from the plant.

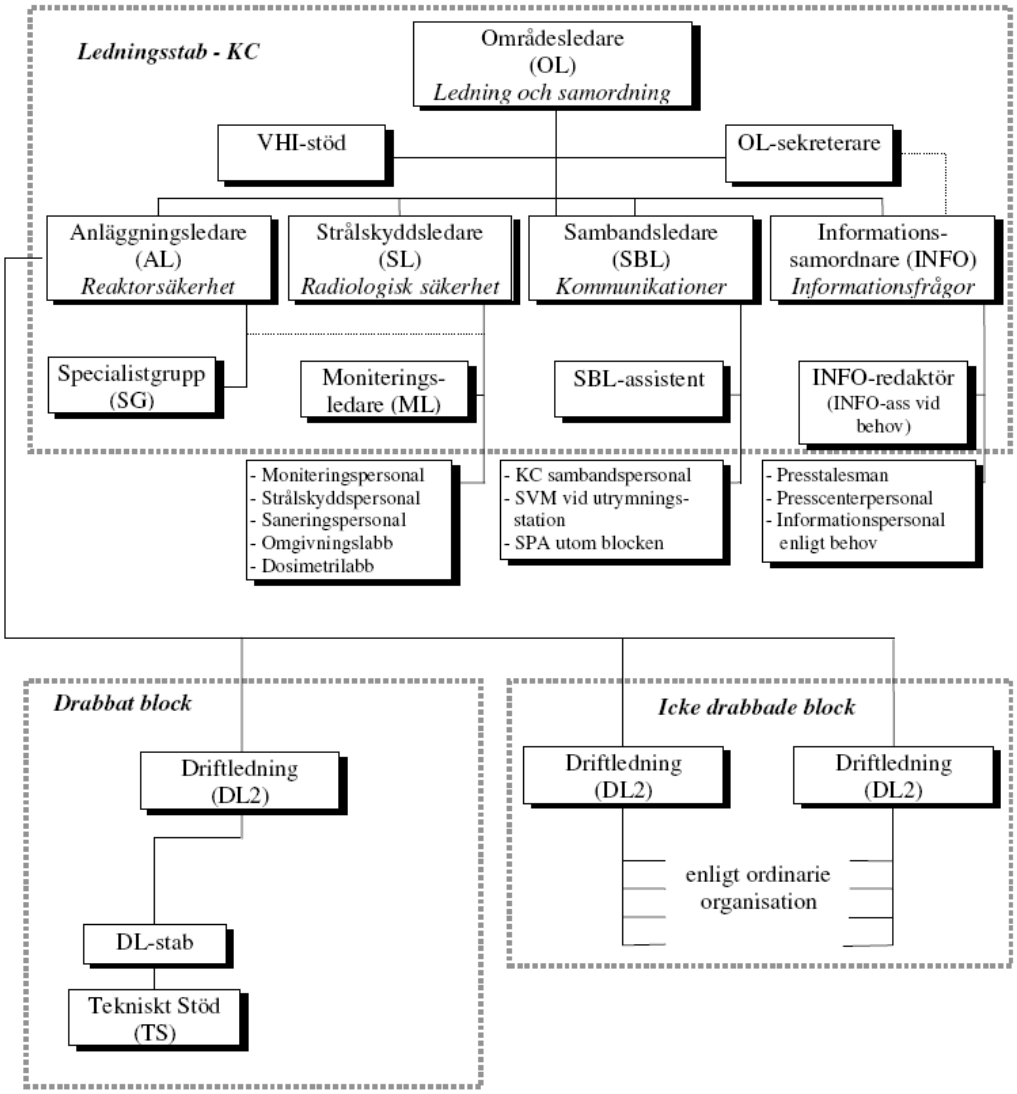


Figure 2. Emergency Response Organization at Plant C NPP

The MCR remains in charge of managing plant personnel meaning that the KC and DLC cannot dispatch plant personnel without asking the MCR. However, the KC can dispatch fire fighters and the DLC can dispatch maintenance personnel via the TSC of the affected unit. To by-pass the MCR regarding their own personnel would not be the normal procedure.

Work is ongoing at Plant C NPP at developing SAMGs consistent with international standards. This may change responsibilities to some extent. Today the Emergency Command Center (KC) is responsible for implementing the "THAL" during an accident situation, which is a document corresponding to the SAMG.

2.3.2 Activation and Location

There are three different alarm levels (preparedness classes) at Plant C NPP:

- Plant C site preparedness (FAB)
- Elevated preparedness (höjd beredskap)
- Accident alarm (haverilarm)

The Emergency Command Center (KC), the Operation Management Center (DLC) and the Technical Support Center (TSC) are summoned on all three alarm levels. Staffing is dependent on the level of

severity: in the less severe events (FAB), for instance, the number of required persons in the KC is lower.

Location
The Emergency Command Center (KC) is located inside the site area and not in the proximity of the main control room (MCR). There is also an alternative KC location outside the evacuation zone (far away from the site). The DLC and the TSC are on site: at Plant C units 1 and 2 these are outside the MCR, while in the MCR at Plant C unit 3. The alternative locations for the DLC and TSC at Plant C units 1 and 2 are the respective MCRs.

2.3.3 MCR-TSC interaction and communication

In a severe accident the MCR will be performing actions covered by the operating procedures (EOPs, AOPs, LeOH). According to criteria in the EOPs at indication of core melt the engineer on duty (VHI) or the MCR shift supervisor will order to transfer from the EOPs to the SAMGs (THAL). At this point the engineer on duty (VHI) will takes command until the Emergency Command Center (KC) is summoned. At that point the MCR will execute the directions obtained from the KC and the Operation Management Center (DLC). The MCR will maintain command and control of field operators and maintenance personnel.

Communication between the various control centers KC, DLC and TSC, and between the KC, DLC, TSC and the MCR has proven to be challenging. One action has been to locate the DLC and the TSC in the MCR at Plant C 3. In case of multi-unit events no personnel can be assigned the same role at several units.

Technology
Communication technology used at the plant includes peer-to-peer, telephone, radio, RAKEL (satellite radio), video, and whiteboards. There are dedicated roles for communicating and coordinating the TSC with other actors and communication protocols are followed.

2.3.4 Competence building

The training courses consists of both basic and repetition training. There are accident exercises where the participants can apply the insights from the courses. These are:

- The “Unit exercise” involving the unit manager, DLC, TSC and KC at one unit at Plant C NPP.
- The “Function exercise” training specific parts of the accident and the unit preparedness.
- The “Joint exercise” involving specific parts of the accident and unit preparedness as well as external organizations
- The “Total exercise” organized by the County Administrative Board every 4-6 years involving the entire ERO (DLC, TSC and KC) and all relevant external organizations.

The training and accident exercises are reviewed based on predetermined criteria and on the demands for the different roles in the accident organization.

2.4 Plant D

The description of Plant D organization applies to two reactor units. In these units the TSC is located in the rear part of the Main Control Room of the corresponding unit. The Unit Manager supported by the TSC commands actions to the MCR, but the ultimate decisions maker is the Site Emergency Director, head of the Emergency Response Organization located at the Emergency Command Center (Kommandocentralen), a different building on-site.

2.4.1 Roles, responsibilities and accident mitigation tasks

The Plant D Emergency Response Organization (ERO) consists of the Emergency Command Center (ECC), the TSC, and the ERO Field organization.

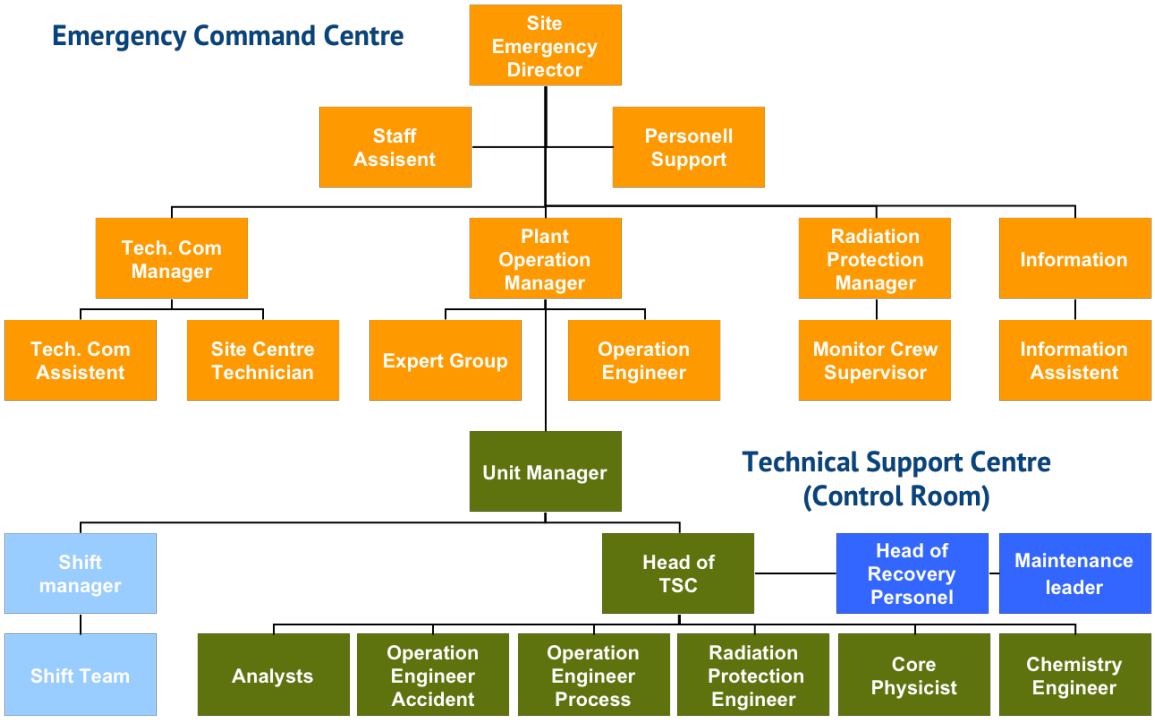


Figure 3. TSC within the ERO at Plant D

The ECC goal is to protect the public and make recommendations whether protective actions like evacuations, in-door stay, intake of stable iodine should be undertaken. Such recommendations are based on judgements about the current status of the plant and anticipated development, estimation of current source terms based upon comparison with source-terms from pre-calculated accident scenarios, and projection of doses to the public through simplified atmospheric spreading calculations. The ECC performs the Core Damage Assessment (CDA) in order to give a source term for assessment of potential doses to the public. It may cooperate with the TSC in order to get plant parameters as input to the CDA.

The TSC supports the Unit Leader (Block Leder) and the MCR in the efforts to return the plant to a stable state and minimize releases to the environment. This is done through using the SAMG procedures and evaluating whether unconventional alignments or equipment should be put in place.

The Analyst and the Operations Engineer in the TSC have the responsibility for the SAMGs, whereas the Unit Leader commands the decisions to the MCR. The TSC informs the ECC about the plant status, planned actions and anticipated development of plant status. Especially actions which will cause deliberate releases (e.g. activation of FCV) has to be agreed upon with the ECC before such actions are performed.

The ultimate decision maker is the Site Emergency Director (Områdesledare) who is the Emergency Response Organization lead at Plant D (Haveriberedskapsorganisation).

2.4.2 Activation and Location

The Engineer on Duty (VaktHavande Ingenjör - VHI) decides if the criteria for calling out the ERO are met. There are 4 alarm levels:

1. **Information**. ERO (with ECC and TSC) is not activated, but existing personnel at the plant, especially communications personnel, is prepared to communicate with authorities, news media, etc.
2. **Activation.** According to the two units, alarm criteria for this level include:
    1. Identification of a design-basis accident (e.g. LOCA) through the EOPs (Emergency Operating Procedures).
    2. Certain fuel handling accidents.
    3. Other situations like:
        a. Indication of a primary break in the auxiliary building
        b. Identification of a bomb
        c. Large fire in areas with safety systems that cannot be extinguished within 15 minutes
        d. Other event that can be a threat to safety, e.g., flooding in areas with safety systems or rising temperature in the spent fuel pools
        e. Consistent high activity in the chimney
        f. Failure/leakage of decay tank with potential radioactive release.
3. **Alert** (Höjd beredskap).
    1. The plant deviates from expected response at disturbed operation - at least 2 barriers are broken or challenged
    2. The plant is exposed to threats where the consequences are not analyzed or not easily predictable.
4. **General Emergency** (Haverilarm). Certain parameters exceed certain values, e.g. containment pressure greater than design pressure, core exit thermocouple temperatures greater than allowed, Steam Generator Tube Rupture, dose rates in containment and/or chimney exceeds certain values, etc.

The TSC is activated at alarm-levels 2, 3 and 4. The criteria for alarm-level 2 are considered to be fairly benign, no immediate danger: the intention is that the TSC normally should be activated well before levels 3 and 4 occurs.

Location
The Emergency Command Center is inside the site area in a building with additional equipment for power supply, communication systems, air filtration, etc., in order to endure harsh conditions.

The TSC is located in the immediate proximity to the MCR in the rear part of the MCR (main control room), behind the back panels.

2.4.3 MCR-TSC interaction and communication

When the ERO is in place the direction of the whole plant is transferred to the Site Emergency Director in the Command Center. In the early stages of the accident the MCR shift crew works on operational response according the SACRG-1. As soon as the TSC is available command and control over the damaged plant is transferred from the MCR to the TSC according to the SACRG-2. The TSC uses the SAMG procedures and perform the decision process in these procedures. The work in the TSC is lead by the Head of Technical Support (in Swedish cTS) who is trained in staff operations. The Unit Manager acts as the link between the TSC and the MCR shift crew.

At the damaged unit maintenance personnel and field operators are coordinated by the Head of recovery Personnel (cIP) in the TSC. The TSC will always cooperate with MCR, but the Unit Manager might directly dispatch personnel to obtain local measurements, as well as to locally repair or activate equipment. Resources outside the damaged unit are coordinated by the Command Center, who also interacts with other plant staff and the authorities.

The communication between the TSC and Command Center (CC) occurs via regular information meetings (recommended to occur every hour) and through contacts between different resources, e.g., the Operations Engineer Emergency Preparedness (OEEP). The Head of Technical Support (cTS) in the TSC and the Staff Assistant (SA) in the CC are trained on how to plan meetings between Unit Leader, CC and TSC.

In case of conflicts (e.g., conflicts on strategies, direction of plant staff) the Unit Manager has the authority to prioritize and resolve. This is done with support from the TSC. Some actions, like containment vent system manual activation, need approval by the Site Emergency Director. The Site Emergency Director also resolves conflicts about use of resources shared by different units.

Technology
The TSC is located in the MCR and has access to all MCR-information. It is mainly the Operation Engineer Processes that would go the MCR to get this information. In addition, the TSC has own computers with access to Process Information System (PIS) where a large number of process parameters are available in near real-time with historical trending capability.

The CC has access to the PIS system and the control room "Block Computers", but might cooperate with the Operation Engineer Processes in the TSC in order to get additional process information. The CC has additional information from radiation monitoring systems both inside and outside the site.

Information technology available in the TSC are: phones, video, whiteboards, a computer diary, and emails.

2.4.4 Competence building

All Plant D emergency preparedness employees take basic and role-specific courses on emergency response preparedness course.

Every second year there is a unit-level exercise in which the complete ERO and external parties train together. Not everyone in the ERO takes active part (since there are several persons having the same role) but most have a role, e.g. as observers.

The cooperation between the TSC and a simplified MCR are practiced in so called "Training of sub-function" on specific tasks, and at sessions at the plant training simulator.

Twice a year there are an unprepared call-out exercise, normally outside normal office hours, when the ERO is called out and established. The goal is that 80% of all roles should be established within 2 hours.

2.5 Summary comparison of operational decision authority at Nordic plants

The survey reveals that the Emergency Response Organizations and the role of the TSC in the Nordic countries NPPs differ, sometimes also units within the same site have differences regarding, for instance, the location and instrumentation of the different control centers. A common trait is that at all four NPPs the ultimate decision maker is the Emergency Manager (EM), who has the responsibility for the entire site. Apart from Plant D, the Nordic plants' role and functions of the TSC and the procedural guidance systems depart in significant ways from the more well-known U.S. approach (Safety Data Integration Group, 1981).

Table 2 summarizes how decision making authority in severe accidents is distributed within the EROs of the four Nordic NPPs.

Table 2. Summary table of operational decision authority at Nordic Plants

	Plant A	Plant B	Plant C	Plant D
Ultimate decision maker	EM (on-site, outside MCR)	EM (on-site, immediate proximity of the affected unit MCR)	EM (on-site, outside MCR)	EM (on site, outside MCR)
Discontinuation of EOPs / Immediate actions in SAMGs	MCR	MCR	MCR	MCR
SAMG use	TSC (off-site) recommends actions to EM. Has direct access to essential plant information only, needs to contact on-site TSC for full plant data.	EM (TSC can support on EM assignment. TSC is on-site but not in immediate proximity to the MCR)	DLC (Operation Management Center, outside MCR at Units 1 and 2, in MRC at Unit 3)	TSC (on-site, immediate proximity of the affected unit MCR)
Direction of actions not contained in, or contrary to, procedures or guidelines	TSC	EM (TSC can support on EM assignment)	EM	TSC
Initiation of strategies/actions involving intentional release of fission products	TSC	EM (TSC can support on EM assignment)	EM	TSC (with EM consent)
Command of plant personnel	MCR and TSC	EM (with Operation Manger and Maintenance Manager. MCR supervises plant personnel work)	MCR (EM can dispatch fire fighters, DLC maintenance personnel via the TSC of the affected unit)	TSC (MCR cooperates)
Request of mobile or off-site equipment	TSC	EM	DLC and EM (to some extent MCR)	TSC
Command over systems/resources shared by multiple units	MCR as per procedures, TSC if situation not covered by procedures. TSC can overrule MCR	EM	EM	TSC
Direction of personnel from different units	TSC	EM	EM	EM

EM = Emergency Manager; TSC = Technical Support Center; MCR = Main Control Room; ERO = Emergency Response Organization; DLC = Operation Management Center (Plant C NPP)

3 TSC/ERO challenges at Nordic plants

The questionnaire has asked the respondents to identify challenges the TSC and the wider ERO could face in a severe/multi-unit accident. The questions have concentrated on challenges to information

acquisition & exchange, task allocation & teamwork, and on specific operational challenges. This section summarizes the answers received, the plants' self-assessed strengths and potential weaknesses in severe site-level accidents (see Appendixes 1-3 for the original questions and answers).

Self-reported TSC challenges in information accessibility and exchange

The plants generally consider the access to relevant plant information for decision making to be good. One plant mentions possible issues in case of multi-unit events, another high communication requirements across distant command centers, and yet another the lack of training on some information systems due to simulator's limitations. Table 3 summarizes the plants' answers on information access and exchange challenges.

Table 3. Self-assessed potential TSC challenges on information and communication

Plant A	Plant B	Plant C	Plant D
The TSC obtain process computer data, and this arrangement has worked well. In emergency preparedness drills the TSC members do not get all process and other information from the plant simulator (including weather, environmental radiation monitoring, dose rate), which limits the scope of the exercises.	The main challenge is that the ERO gets data only from the MCR unit in which it is gathered. Only the support group outside the plant gets data from all three NPP units. In multi-unit situations the ERO can move to the support group facilities if decided by the Emergency Preparedness Manager. Reliability of the data connections in accident situations involving possible loss of I&C and electrical systems is always uncertain. Plant overview is maintained by status boards (big paper boards on the wall) where main systems availabilities will be marked manually.	The different groups comprising the ERO (KS, DLC, TSC, MCR) are located in different places and need a lot of communication and coordination. Because of this, DLC and TSC are co-located in the MCR at Plant C unit 3 (not yet in units 1 and 2).	The TSC has good access to plant information as it is in the same room as the MCR. The availability of the PIS system is considered to be of great value.

Task allocation and teamwork

All plants believe their EROs possess the technical competence required in severe and site-level accidents and that the different control-centers/decision-makers interact well, as shown in and reinforced through drills and exercises. They see potential improvements in more precise task definitions for the TSC (one plant) and communication and cooperation (three plants), e.g., time lags and lack of coordination between decision makers at distant locations. The plants have addressed the issue of multi-unit accidents by not assigning ERO staff the same role at several units, but there remain issues related to procedures (one plant), resource conflicts (one plant) and high workload for the ultimate decision maker (one plant). One plant reminds that the basic ERO configuration was designed for single-unit events (see table 4 for details).

Table 4. Self-reported evaluation of task allocation and teamwork within the EROs

	Plant A	Plant B	Plant C	Plant D
Best practices/what works well	Authority distribution works well. MCR may ask questions from TSC and TSC will provide answers.	TSC and support group have good and versatile technical and operational competence.	The ERO (KC, DLC and TSC) works well, e.g. the meeting procedures.	Drills involving a simplified MCR and the TSC have improved the communication between the TSC and MCR.
Challenges/ potential for improvement	None, the task allocation between TSC and MCR has worked well.	Communication between groups of people located at different facilities is always challenging and time consuming. Information sharing could be improved. The support group could have more precise tasks and assignments with given deadlines.	Communication between KC, DLC and TSC and between these and the MCR has proven to be challenging, especially at units 1 and 2 where the DLC is located outside the MCR.	There can be a delay before information reach the ultimate decision maker in the command center KC. It can be difficult to find time to keep KC/TSC up to date on what the other part is doing.
Multi-unit specific aspects. (e.g., staff and resource conflicts during multi-unit accidents?)	For every TSC position there are more than one person. TSC may also gather all available resources to support its work, e.g. experts that are not officially part of TSC but have needed expertise.	Management of multi-unit accidents would be challenging. The basic configuration of the emergency organization has been created for one-unit situations. The update of procedures for multi-unit situations is ongoing. Resource conflicts might occur.	There has been an increased focus on multi-unit events. None is assigned the same role at several units, which was the case in some instances before.	Drills have been performed with manning two TSCs for two damaged units. The load on KC can be high in such a situation.

Operational challenges in multi-unit scenarios

The questionnaire asked the plants to evaluate specific operational challenges in severe site-level accidents (see Appendix 3). All plants recognize (a) command and control risks due to poor task definition, allocation, lack of training and on actions not described in procedures; and (b) the risk of trying to use equipment damaged by or not qualified for the environmental conditions. Most plants also consider the risk of (a) not achieving a global situation awareness; (b) of setting wrong priorities and not updating these timely; and (c) of following the procedures based on current parameters without insights in actual plant conditions and without evaluating pros and cons of actions. The plants had different views on the risks of (a) failing to maintain core/debris cooling of the unit(s) uninterruptedly and (b) failing to maintain a complete list of all available recourses for water and power. Most plants considered unlikely the risks of (a) improper transfer from EOPs to SAMGs, and (b) of failing to consider instruments' reliability due to environmental conditions. See the summaries of the individual answers in Table 5 below.

Table 5. Self-evaluation of potential EROs challenges in multi-unit scenario

Possible issue	Plant A	Plant B	Plant C	Plant D
Improper EOP-SAMG transition	Unlikely. Entry criteria to SAMG are explicit (exact limit values). Some SAM domain actions are contained in the EOPs. Both EOP and SAMG are MCR procedures/guidelines.	Unlikely. The instructions to be used in the loss of AC power situations are clear and recovery of AC power would be a clear goal for MCR. SAM actions would only take place, if AC power could not be recovered quickly enough.	Yes, possible.	Unlikely. The criteria for SAMGs entry are clearly defined.
Complete and updated list of available resources for water and/or power for the units not created and maintained	Unlikely.	To certain degree yes. List of possible AC power sources is clear, also list of possible water sources is clear, but in some complex multi-unit situations the focus might be lost and priorities might not be that clear.	Yes, possible.	Each unit has its own resources, which should not create additional problems about available resources for water and/or power in multi-unit accidents.
Trying to use equipment that has been damaged by the accident or that is not qualified for the prevailing environmental conditions	Might happen. Operators follow procedures in which actions are based on usage of qualified equipment and measurements. However, exceeding qualification limits is not considered in guidance. Safety engineer monitors the state of the plant in parallel. The TSC decides and prioritizes the repair actions.	Not very likely but possible. The understanding of the overall situation (big picture) might be degraded in a complex multi-unit situation. Depends also on the severity of the situation: if severe accident has already taken place, then the situation would be much more complicated and much more difficult to manage without good communication and good training on procedures.	Yes, possible.	Can happen.

Possible issue	Plant A	Plant B	Plant C	Plant D
Not considering the impact of the severe accident environmental conditions for the instruments which are read to initiate severe accident guidelines	Plant A has specified SAM systems and equipment and the SAM strategy considers environmental conditions and instrumentation. Communication with TSC is required before executing the main actions. There is a SAM specialist in the TSC.	Not very likely but possible. The main actions are to be initiated before onset of severe core degradation. Therefore, the instruments should not be affected yet.	Yes, possible.	The SAMG contains cautions and recommendations about instrument availability and reliability.
Not achieving a global situation understanding: not understanding time windows, actions consequences, or not integrating various sets of procedures	The guidance should ensure actions in correct time window and prevent wrong actions.	Very likely. Phenomena related to severe accidents are complicated and not that well known. The management of the overall situation would be very challenging.	Yes, possible.	Can of course happen.
Delay in updating operating strategies / wrong priorities between important actions	The situation evolves slowly which helps communication. The MCR uses procedures that include communication points with TSC for important actions. The guidance should ensure timely action and prevent wrong actions.	Possible. The good coordination between TSC and MCR would be important.	Yes, possible.	Can of course happen. Some scenarios are tricky and requires quick actions which have to be trained.
Parameter-based procedures following without insights in the plant damage conditions and/or not balancing plusses and minuses	The safety engineer follows the status of the plant in parallel and decides recovery actions. The TSC assists. The guidance should ensure actions in correct time window and prevent wrong actions.	Very likely. Phenomena related to severe accidents and beyond design events are complicated and not that well known. The management of the overall situation would be very challenging. Proper prioritization of the actions would be challenging.	Yes, possible.	Can of course happen. Yet, the WOG-SAMG have a clear structure where each strategy has a list of “Pro/Con”, i.e. “plusses and minuses”, where potential impact from plant damage conditions is considered.

Possible issue	Plant A	Plant B	Plant C	Plant D
Core/debris cooling of the units not maintained uninterruptedly	Not applicable, core debris cooling is a passive function after SAM actions which are executed in EOPs and checked in SAMG.	Probably yes, complicated and challenging situation.	Yes, possible.	Actions like evacuations and externals calls are handled by the KC and should not distract from core/debris cooling.
Poor command and control for actions not well trained or included in current procedures	Actions in guidelines have been trained. Struggling may occur in situations which are outside of procedure scope.	Probably yes, complicated and challenging situation.	Yes, possible.	Can of course happen.
Poor ERO command and control due unclear tasks definition, allocation, training, and shift transfer training.	Might be possible.	Probably yes, complicated and challenging situation.	Yes, possible.	Can of course happen.

4 TSC treatment in Nordic plants' PSA/HRAs

The Nordic countries Level 2 HRAs are conducted by using methods developed for Level 1 HRA (THERP-based methods and extensions) and/or by using expert judgment in the quantification of HFEs, as it is also the case internationally (Raimond et al., 2013). The TSC is given limited consideration in the PSA/HRA due to high-level (not detailed) and indirect modelling of TSC actions, and the uncertain gain of doing otherwise (assumed limited impact on the HRA accuracy and PSA results), although one plant analyst recognizes that "the more serious the situation is, the more important is the role of the TSC". The individual plants' treatment of the TSC in their PSAs is given in Table 6 (Plants A and B) and Table 7 (Plants C and D).

Table 6. TSC treatment at Plants A and B HRAs

	Plant A	Plant B
HRA Method used	A modified version of ASEP.	Expert judgment.
HFE identification	MCR and TSC actions considered as Category C actions. When estimating the probability it is taken into account that the TSC supports the main control room.	The human actions that are part of the mitigation strategy and could affect the estimation of source term (magnitude, timing, composition) are considered. **A) Units 1 and 2**: The TSC is considered but the significance is small. Certain operator actions during SA are included in the Level 2 PRA model. They are, however, initiated by the MCR staff based on their written instructions. The role of the TSC is not focal for the initiation of the human actions modelled in the L2 PRA, but TSC can supervise and guide the MCR staff and make sure that proper actions will be carried out. The influence of the TSC has been taken into account in the estimation of the success probabilities of a couple of operator actions (modelling of PSFs). **B) Unit 3**: During SA the mitigation actions follow OSSA guidelines (Operating Strategies for Severe Accidents) and the TSC has a central role in the management of such actions. The role of TSC is included in the event and fault tree modelling used for the level 1 – level 2 interface model.
TSC PSFs	Not considered specifically.	Depends on the unit (PRA model), but stress level, available instructions, amount of training, feedback from the process and the familiarity of the situation are among the factors considered.
Quantification	Especially for some recovery actions (usually no procedures available) the ASEP-HRA method cannot directly be used but the probability is estimated by expert judgement taking into account the role of the TSC.	Values from literature and the method are used, supported by expert judgment. Some values also use information gathered from specific simulator tests and training sessions.
TSC impact to HRA	The TSC has a role in the PSA/HRA. It is hard to tell exactly how important and in which situations it is important but in general it can be said that the more serious the situation is, the more important the role of the TSC. For example, in level 3 PSA the role would be important but only Level 1 and 2 PSAs have been carried out for Plant A NPP.	TSC is important for actions that cannot be based on straightforward instructions but require careful consideration and estimation of the overall situation.

Table 7. TSC treatment at Plants C and D HRAs

	Plant C	Plant D
HRA Method used	The usual PSA and HRA methodologies used at Plant C for HRA. The Human reliability analysis method description (Holmberg 2016) is the main reference. It is a THERP-based HRA methodology.	The TSC is mentioned in the qualitative argumentation for some actions to support that the operators will perform them in time.
HFE identification	EM and DLC actions are not modelled in detail, but implicitly considered in PSA/HRA for longer time windows. The main focus for the HRA is the work in the MCR and by maintenance personnel. EM/DSC actions are part of the understanding of the handling of an event, but not modelled separately.	The TSC is mentioned for actions performed more than two hours after core damage, e.g., when the TSC is assumed to be in place.
TSC PSFs	Not considered specifically.	THERP is used for the plant HRA. If TSC actions would be re-analysed today Plant D current HRA method would apply five calibration factors covering instructions, training, coordination, stress and HSI.
Quantification	EM and DLC actions are not modelled in detail, but can be included in broader HFEs. These actions are part of the understanding of the handling of an event, but not modelled separately. No experience database is used.	Today the TSC is only credited indirectly.
TSC impact to HRA	It may be of interest to model EM and DLC actions in more detail. However, HRA in general contains many uncertainties and it is not certain that more detail in this case will be the most efficient way to enhance the HRA accuracy in the PSA studies.	TSC role not important in the current PSA. The main contributor in the current PSA level 2 is basemat failure in situations where there is water in the pit, but despite this coolability could not be assured due to epistemic uncertainties in the understanding of coolability. In this situation there are no actions the TSC could perform to improve the situation. Plant D is investigating whether the risk for basemat failure is realistic. If it could be assessed as lower, other problems might be dominating, e.g. SGTR in Severe accident conditions. Such an event might be more demanding on manual actions.

5 Conclusions

This report has described the Nordic plants' TSCs and other EROs staff that have a role on operational decisions during severe and site-level accidents. The Emergency Response Organizations and the role of the TSC in the Nordic countries NPPs differ, sometimes also reactor units within the same site have differences regarding, for instance, the location and instrumentation of the different control centers. A common trait is that at all four NPPs the ultimate decision maker is the Emergency Manager (EM), who has the responsibility for the entire site. Apart from Plant D, the Nordic plants' role and functions of the TSC as well as the procedural guidance systems differ in significant ways from the more well-known U.S. approach.

The plants have self-assessed challenges that the TSC and the wider ERO could face in a severe/multi-unit accident. The plants generally consider the access to relevant plant information

(instrumentation in the control centers) for decision making to be good. All plants believe their EROs possess the technical competences and the organizational skills and capabilities required in severe and site-level accidents, as shown in and reinforced through drills and exercises. Potential improvements are spotted in more precise task definitions for the TSC (at one plant) and in communication and cooperation (three plants). The plants have addressed the issue of multi-unit accidents by not assigning ERO staff the same role at several units, but there remain issues related to procedures (one plant), resource conflicts (one plant) and high workload for the ultimate decision maker (one plant). One plant reminds that the basic ERO configuration was designed for single-unit events.

All plants recognize the possibility that specific operational challenges could arise in severe site-level accidents to various degrees. The most acute risks relate to command and control (risks due to poor task definition, allocation, lack of training and on actions not described in procedures) and on trying to use equipment damaged by or not qualified for the environmental conditions. Medium risks are poor situation awareness, wrong priorities, lack of insights in actual plant conditions and lack of consequences evaluation. Only half of the plants repute credible the risks of failing to maintain core/debris cooling of the unit(s) uninterruptedly and of failing to maintain a complete list of all available recourses for water and power. Most plants considered unlikely the risks of improper transfer from EOPs to SAMGs and of failing to consider instruments' reliability due to environmental conditions.

The report has also described how the different plants credit the TSC role in Probability Safety Analyses (PSA) for multi-unit events. The Nordic countries Level 2 HRAs are conducted by using methods developed for Level 1 HRA (THERP-based methods and extensions) and/or by using expert judgment in the quantification of HFEs. The TSC is given limited consideration in the PSA/HRAs (not detailed / indirect modelling of TSC actions) and it is assumed that a detailed treatment will have a limited impact on the HRA accuracy and the PSA results.

There is therefore a disconnect between PSA/HRA practice (both at Nordic sites and internationally) and the fact that in site-level accidents almost all safety issues are resolved through TSC decisions to prevent, reduce, or delay large radioactive releases that may follow single or multi-source severe fuel damage accidents. The report provides a concise reference source of generic and plant-specific information related to the TSC role in responding to severe and site-level accidents, a necessary first step for including it in PSA/HRAs and, possibly, a useful complement for further progress on severe accidents preparedness.

References

Arigi, A. M., Kim, G., Park, J., & Kim, J. (2018). Human and organizational factors for multi-unit probabilistic safety assessment: Identification and characterization for the Korean case. *Nuclear Engineering and Technology*.

Bareith, A. (2018, July). *An initiative towards site-level risk assessment For NPP Paks*. Presented at the WGRISK Workshop on Status of Site Level PSA, Munich, Germany.

Cooper, S., Xing, J., & Chang, Y. (2013). What HRA needs to support site-wide, multi-hazard level 2 PRA. In *PSA 2013 International Topical Meeting on Probabilistic Safety Assessment and Analysis, September 22-26*.

Drøivoldsmo, A., Porsmyr, J., & Nystad, E. (2011). *Preparedness organisations at Nordic nuclear power plants* (No. NKS-250). Nordisk Kernesikkerhedsforskning.

Dupuy, P. (2018, July). *Safety of Multi-Unit Sites in France*. Presented at the WGRISK Workshop on Status of Site Level PSA, Munich, Germany.

Fauchille, V., Bonneville, H., & Maguer, J. Y. (2014). Experience feedback from Fukushima towards human reliability analysis for level 2 probabilistic safety assessments. In *Proceedings of the 12th Probabilistic Safety Assessment and Management Conference, Paper PSAM-167* (pp. 1–9).

Jaworska, A. (2002). *Nuclear emergency preparedness in the Nordic and Baltic Sea countries* (No. NKS-76). Nordisk Kernesikkerhedsforskning.

Kaarstad, M., Massaiu, S., Strand, S., Holmgren, L., Skjerve, A. B., & Bye, A. (2016). *Workshop Meeting on Accident Management and Operation* (No. HWR-1146). Halden, Norway: Halden Reactor Project.

Liinasuo, M., & Koskinen, H. (2017). *Principles and practices of emergency exercises* (No. VTT-R-00618-17) (p. 45). Espoo, Finland: VTT Technical Research Centre of Finland Ltd.

Park, J., Ham, D. H., & Jung, W. J. (2018). Characterizing Decision-Making Tasks Included in SAMGs. Presented at the International Workshop on Status of Site Level PSA, Munich, Germany.

Raimond, E., Durin, T., Rahni, N., Meignen, R., Cranga, M., Pichereau, F., … Mildenberger, O. (2013). *Best-practices guidelines for L2PSA development and applications. Volume 2-Best practices for the Gen II PWR, Gen II BWR L2PSAs. Extension to Gen III reactors* (No. ASAMPSA2/WP2&3/ 2013-35).

Safety Data Integration Group. (1981). *Functional Criteria for Emergency Response Facilities* (No. NUREG-0696). Washington, DC: Division of Emergency Preparedness Office of Inspection and Enforcement U.S. Nuclear Regulatory Commission.

Sehgal, B. R. (2012). *Nuclear safety in light water reactors severe accident phenomenology*. Amsterdam; Boston: Elsevier/Academic Press.

Sehgal, B. R. (2016, August). *The Tyranny of Severe Accident Management*. Presented at the NUC Workshop “Accident Management: Emerging R&D Needs and Approaches,” Raleigh, NC.

St Germain, S., Boring, R., Banaseanu, G., Akl, Y., & Xu, M. (2016). *Modification of the SPAR-H method to support HRA for Level 2 PSA*. United States: Idaho National Lab (INL), Idaho Falls.

Vayssier, G. (2012). Severe Accident Management Guidelines (SAMG). In *Nuclear Safety in Light Water Reactors* (Sehgal Bal Raj, pp. 520–549). Amsterdam: Elsevier.

Vayssier, G. (2014). Benefits and Limitations of the New Consolidated PWROG Severe Accident Management Guidance (SAMG)-A Review of Some Critical Issues. *International Journal of Performability Engineering*, *10*(7).

Vayssier, G. (2016a). Severe Accident Management Guidance: Lessons Still to be Learned after Fukushima-The Need for an Industrial Standard. *International Nuclear Safety Journal*, *5*(1), 8–20.

Vayssier, G. (2016b, August). *Research Needs for Severe Accident Management - A Personal Perspective*. Presented at the NUC Workshop “Accident Management: Emerging R&D Needs and Approaches,” Raleigh, NC.