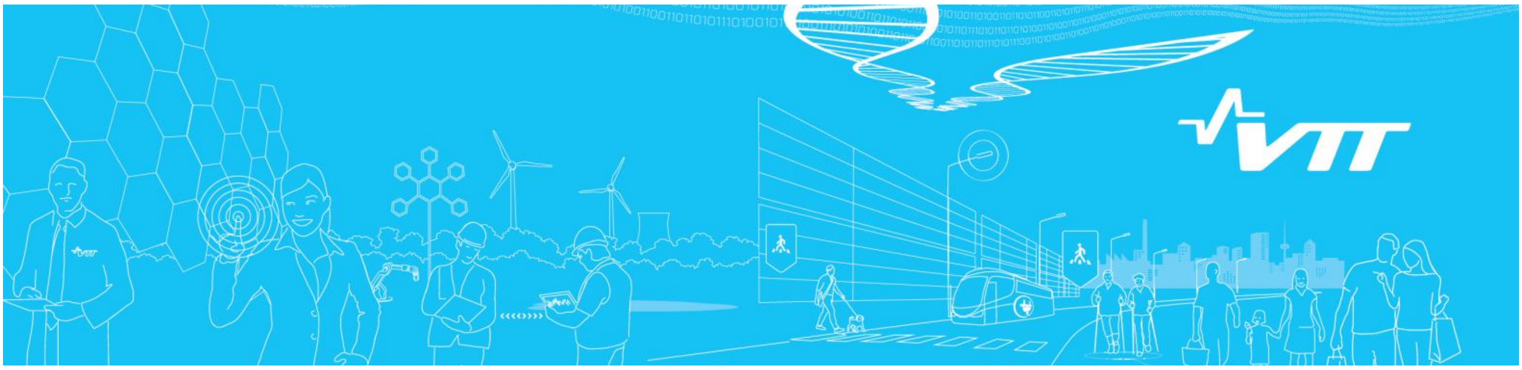

RESEARCH REPORT

VTT-R-00025-18

Requirements for site level PSA model management

Authors: Tero Tyrväinen, Kim Björkman

Confidentiality: Public

Report's title

Requirements for site level PSA model management

Customer, contact person, address VYR	**Order reference** SAFIR 4/2017
Project name Probabilistic risk assessment method development and applications	**Project number/Short name** 114491/PRAMEA
Author(s) Tero Tyrväinen, Kim Björkman	**Pages** 15/
Keywords Site probabilistic safety assessment, model management, multi-unit	**Report identification code** VTT-R-00025-18

Summary

In this report, preliminary requirements are outlined for site PSA documentation, model management and computation. First, overall requirements for site PSA are developed. Second, it is specified what information needs to be documented in different site PSA analysis steps. Third, requirements for a multi-unit dependency database and PSA model management process are listed. Finally, requirements for computation results are specified.

The requirements were mainly outlined based on method development that focused on level 1 PSA. When level 2 PSA and other radioactive sources than the fuel in the reactor core are included in the scope, some additional requirements might be needed. In addition, the overall requirements only consider PSA applications on a general level. It is therefore expected that the set of requirements will be updated when more research and development work is completed and after gaining experience from site PSA work. Guidelines for site PSA model management should also be prepared.

Confidentiality	Public

Espoo 24.1.2018

Written by Tero Ti Tero Tyrväinen, Research Scientist	**Reviewed by** Ilkka Karanta, Senior Scientist	**Accepted by** Eila Lehm 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
CCF	Common Cause Failure
MCS	Minimal Cut Set
MUCDF	Multi-Unit Core Damage Frequency
POS	Plant Operating State
PSA	Probabilistic Safety Assessment
PSF	Performance Shaping Factor
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 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 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 computation. Software tool support is also needed. This report outlines requirements for site PSA documentation, model management and computation. The purpose of the requirements is to guide site PSA development. They are not meant to be regulatory requirements. The report is closely connected to the method report [1] and it considers the same analysis phases.

Risk metrics for site PSA have been outlined in [3]. The main site risk metrics for level 1 PSA are the multi-unit core damage frequency (MUCDF) and the site core damage frequency (SCDF). 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 at least two units nearly simultaneously. 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 other fuel locations 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 methods developed in [1], and Section 3 discusses the challenges related to site PSA analysis and model management. Section 4 outlines the requirements for PSA documentation, model management and computation. The conclusions of the report are presented in Section 5.

2. Method description

Guidance for evaluating the site risk for nuclear installations using already existing single-unit PSA models is presented in [1]. The method is partly based on the preliminary probabilistic multi-unit risk assessment approach outlined in [2]. This section summarizes the method in order to provide basic information as a link to the requirements for PSA documentation, model management and computation.

The method consists of the following steps:

- **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.

- **Analysis of POS impact:** Site PSA needs to account for the units’ various combinations of possible plant operating states (POS). The availability of safety systems and recovery actions as well as success criteria differ between POSs and is really the reason for having different POSs. Sufficiently similar POSs should be grouped as much as possible, e.g. outage POSs with approximately the same plant configuration from the residual heat removal point of view. POS groups and combinations of POS groups are screened in order to focus the analysis on the set of most risk relevant POS combinations. It should be noted that POS importance is partly dependent on the considered initiating event.

- **Identification of multi-unit dependencies:** This step consists of the following phases:
    - Identification of multi-unit initiators: The initiators that can cause a multi-unit sequence are identified. The initiators can be categorized into different groups: multi-unit initiating event, partial multi-unit initiating event and initiating event caused by accident in another unit.
    - Identification and selection of dependencies: The dependencies for the identified initiators need to be identified. The dependencies can be shared systems, structures, and components (SSC), identical components, proximity dependencies, human and organizational dependencies, and simultaneous maintenance.

      Qualitative screening is used to rank dependencies in categories 'very important', 'important', 'less important' and 'insignificant'. After the qualitative analysis of dependencies, the relevant dependencies are selected. For the selection, e.g. qualitative analysis of MCS list or quantitative screening and characterization can be used.
- **Data analysis**: During this step, the probability parameters related to multi-unit dependencies are estimated, e.g. inter-unit common cause failure (CCF) probabilities.
- **Human reliability analysis**: This step consists of the following phases:
    - Identification of relevant operator actions for identified initiators,
    - Identification of new human actions,
    - Identification of the influence factors in multi-unit scenarios, and assessment of dependencies between human actions.
- **Quantification of multi-unit risks:** This step can include the following parts:
    - Extending single-unit PSA models, i.e. complementary modelling of multi-unit scenarios in the single-unit PSA. The modelling is done from the risk metrics perspective.
    - Computing site specific risk metrics. Two alternatives can be utilized in the calculation of the MUCDF: combination of MCS lists of different units, or quantification based on multi-unit event combinations.

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 documentation procedures are therefore needed to manage the site 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. Even some new software tool functionality might be needed.

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. 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.

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. Requirements for model management

The purpose of the requirements specified in the following sub-sections for site PSA model management is to guide site PSA development and maintenance. They should not be considered as strict requirements in that sense that some authority would require that they would have to be fulfilled. The idea is that by fulfilling them site PSA can be managed in a consistent manner. Same objectives may also be achieved in different ways without fulfilling these requirements. The requirements are a basis for the development of site PSA model management guidelines. The guidelines should specify how to cover the requirements in practise.

4.1 Overall requirements for site PSA

- Site PSA shall analyse the contribution of multi-unit accidents to site level risk.
- Site PSA shall include analysis of
    - all initiating events that can affect multiple units and appear in single-unit PSAs, such as external hazards and loss of offsite power,
    - all systems that are shared between units and appear in single-unit PSAs,
    - common cause failures between identical components if the components are important risk contributors in single-unit PSAs,
    - human actions in multi-unit accident scenarios.
- Site PSA shall provide risk insights for site safety management with regard to severe accident management, emergency preparedness, and design, operation and maintenance of shared systems.
- Site PSA shall analyse the impact of different plant operating states.
- Site PSA shall identify the most important site risk contributors.

The level of documentation and quality assurance of site PSA should generally be similar to the documentation and quality assurance of single-unit PSAs. General quality requirements of single-unit PSA should also be applied to site PSA. It is recommended that site PSA is developed and maintained according to quality assurance procedures specified in a quality assurance plan. Applicable parts of relevant PSA guidelines, such as the IAEA documents on quality assurance programme for PSA, guidance for development and application of level 1 PSA and living PSA [4-6], should be taken into account.

The following sections provide more detailed requirements on site PSA documentation, model management and computation. Table 1 outlines anticipated documentation and model management tasks related to different analysis phases. The process will be developed further in 2018.

Table 1: Documentation and management tasks in different analysis phases.

Analysis phase	Documentation	Model and database management
Preparations before analysis	Documentation of source materials and PSA model versions	
Selection of analysis scope and risk metrics	Documentation of the scope and risk metrics	
Analysis of POS impact	Documentation of the POS analysis results	Addition of individual POS groups and POS group combinations to database
Identification of multi-unit dependencies	Documentation of the dependency screening results	Addition of multi-unit initiators and dependencies to database, screening of dependencies with the models
Data analysis	Documentation of the data analysis results	Systematic analysis of those multi-unit initiators and dependencies that were screened in using the database, addition of frequencies of initiating events and probability parameters related to dependencies to the database
Human reliability analysis	Documentation of the human reliability analysis results	Addition of human failure events and their probabilities to database
Quatification of multi-unit risks	Documentation of the results	Computation with the models and database, management of files used in computation
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

4.2 Requirements for documentation

This section specifies the information that shall be documented during site PSA development. The requirements are grouped according to the analysis phases, mostly corresponding to the analysis steps in [1] summarized in chapter 2.

Source materials

- Available source documents shall be listed.
- If some important information is missing, it shall also be documented to make the limitations of the analysis clear.
- The version of each single-unit PSA model used in the analysis shall be documented.

Selection of analysis scope and risk metrics

- The scope of the study shall be described:
    - Radioactive sources that are considered
    - PSA levels included in the analysis
    - Types of initiators considered
    - Operating states considered
    - The scope of SSCs considered including the fixed date for the plant (site) configuration being analysed
- The selected risk metrics shall be listed.

Analysis of POS impact

- POS groups shall be listed.
- For each **individual** POS group, the following information shall be documented:
    - Specific POSs belonging to the group
    - Justification for the grouping
    - Estimated time share
    - Time window for core/fuel damage in case of loss of residual heat removal
    - Screening decision and justification
    - List of relevant multi-unit initiating events
- For each identified POS group **combination**, the following information shall be documented:
    - Screening decision and justification
    - Effects on system and human dependencies
- For each multi-unit initiating event, the following information shall be documented:
    - POS dependency category
    - Season dependency
    - POS group combinations to be included in the analysis and justification

Identification of multi-unit dependencies

- For each identified multi-unit initiator, the following information shall be documented:
    - Identifier (Name)
    - Category (multi-unit initiating event, partial multi-unit initiating event or single-unit event that propagates to another unit)
    - Description

  - Frequency
  - Screening decision and justification
  - Source documents
  - The corresponding initiating events in the PSA models
- The identified multi-unit initiators shall be listed.
- For each identified dependency, the following information shall be documented (if applicable):
  - Identifier (Name)
  - Dependency category (shared SSC, identical components, spatial dependency, human dependency, organizational dependency or simultaneous maintenance)
  - Description
  - Qualitative ranking and its justification (reasoning behind it)
  - Screening decision and justification
  - Source documents
  - The units to which the dependency is related, if there are more than two units
  - Basic events related to the dependency in the PSA models
- The identified dependencies shall be listed for each multi-unit initiator.

Data analysis

The following requirements apply to those multi-unit events and dependencies that have not been screened out.

- For each multi-unit initiating event, the following information shall be documented:
  - Data sources
  - How the frequency is estimated
  - Frequency
- For each partial multi-unit initiating event, the following information shall be documented:
  - 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
    - New frequencies
- For each inter-unit CCF, the following information shall be documented:
    - Data sources
    - How single-unit CCF probabilities have been estimated
    - Summary of operating data
    - How the probabilities are estimated
    - Parameter values used in the estimation, e.g. the probability of complete CCF inside one unit and φ from [1]
    - Inter-unit CCF probabilities

Concerning correlated fragilities of components and accident propagation between units, similar type of information needs to be documented. However, requirements are not outlined at this point, because data analysis procedures have not yet been developed.

Human reliability analysis

- For each multi-unit initiating event, list the human failure events modelled in current PSAs.
- For each relevant human failure event and multi-unit initiator combination, the following information shall be documented:
    - Identifier (Name)
    - Description
    - Basic events representing the human failure event in the current models
    - Human failure probabilities in the current models
    - Qualitative assessment from multi-unit scenario point of view
    - If single-unit models are modified with regard to this human failure, how they are modified
    - Human failure probability in multi-unit scenario
- New human actions identified for multi-unit accident scenarios shall be listed.
- For each new human action identified for multi-unit accident scenarios, the following information shall be documented:
    - Identifier (Name)
    - Description
    - Qualitative assessment (including dependencies between this and other human actions)
    - How it is modelled in single-unit PSA models (if it is modelled at this point)

  - Human failure probability

Quantification of multi-unit risks

- The computation of risk metrics and the results shall be documented in detail.
- Comprehensive conclusions shall be written based on the results.
- Comprehensive discussion on the limitations of the analysis shall be written.
- Most important basic events and initiating events with regard to selected risk metrics shall be listed according to selected risk importance measures.
- Most important multi-unit dependencies with regard to selected risk metrics shall be listed according to selected risk importance measures.

Documents and files

- For each document and file used in the analysis, the following information shall be documented:
  - Name of the document/file
  - Location (directory on network drive/computer/workspace, etc.)

4.3 Requirements for managing the PSA models

In this section, requirements are outlined for managing the database for dependencies and for managing the PSA model. Basically, two types of requirements are outlined:

1. Procedures for managing the PSA models.
2. Features that the database or the PSA model itself should support.

The focus will be on the procedures. PSA model development and management guidelines should specify how to perform systematically different steps to meet the outlined requirements. For example, in the guidelines it can be specified how model updates should be performed.

The requirements for managing the PSA model are also closely related to the documentation (see Section 4.2) and computation requirements (see Section 4.4). Many of the requirements are meant to facilitate either the documentation or the computation of the site PSA.

The outlined requirements do not directly specify requirements for PSA software. However, certain PSA software functionality can help in meeting the requirements in practice. For example, PSA software can facilitate the documentation, traceability of model changes and of results, and the database management of multiple single unit PSAs.

4.3.1 Database for dependencies

A database is recommended for the management of site dependencies. This database should be separate from the databases of single-unit PSA models, unless the single-unit PSAs have a common database. The use of the database is not necessary if the data can be managed otherwise, but given that the database is used in the analysis, the following requirements should be considered in its development:

- Each identified dependency shall be added into a database.

- The database shall contain data fields that correspond to documentation requirements in Section 4.2, e.g.:
  - Basic dependency information, e.g., the identifier, category and description for an identified dependency.
  - Screening information, e.g. qualitative screening rank and screening decision.
  - Information for data analysis, e.g. fields for different parameter values.
- It shall be possible to sort and search dependencies in the database according to different attributes.
- For each analysis phase listed in Section 2 (except selection of analysis scope and risk metrics, and possibly analysis of POS impact), the database shall contain tables representing the results of the phase (i.e. the information listed in Section 4.2), or it shall be possible to generate such tables based on the database.

4.3.2 PSA models

- The dependencies that have been selected for modelling based on screening shall be gone through systemically to ensure that all of them are included in the analysis.
- It shall be easy to identify basic events and initiating events representing multi-unit events in a PSA model.
  - This can be achieved, for example, by an identifier in the name or a multi-unit dependency data field.
- Each dependency modelling case shall be verified and validated.
- If special versions of PSA models or additional models for supporting calculations are created in the modelling process, they shall be named clearly and backed-up.
- All files used to perform calculations, such as spreadsheet files, shall be subject to version control.
- It shall be possible to trace different model elements back to the inputs.
- A process for updating site level PSA shall be defined:
  - There shall be comprehensive and clear guidelines for updating the site level PSA.
  - All single unit PSA models shall be kept up-to-date.
  - It shall be possible to keep track of model changes.
  - It shall be possible to trace model changes back to the inputs.
- If site level calculations are performed using different model configurations than normal PSA calculations, model configuration changes shall be based on a predefined process.
  - There shall be clear guidelines for changing the configuration.
  - It shall be possible to save the model configuration for reuse.

  - It shall be possible to keep track of model configuration changes.

4.4 Requirements for computation

This section defines requirements for computation results and computation process.

- It shall be possible to calculate the selected risk metrics. They can include
  - MUCDF or multi-unit fuel damage frequency,
  - SCDF or site fuel damage frequency,
  - frequencies for site release categories.
- Each computation case shall be repeatable (logging of analysis case settings).
- It shall be possible to trace the site results back to the PSA models of individual units.
- The computation tools shall support the documentation task for computation and results (see Section 4.2).
- It shall be possible to calculate selected risk importance measures for basic events and initiating events with regard to selected risk metrics.
- It shall be possible to identify the unit of each single-unit basic event and initiating event that appears in site level results.
- It shall be possible to calculate selected risk importance measures for multi-unit dependencies with regard to selected risk metrics.
- It shall be possible to calculate the contributions of different plant operating states to site level risk metrics.
- It shall be possible to calculate the contributions of multi-unit dependencies to the core/fuel damage risk related to a specific plant operating state.
- It shall be possible to calculate the contributions of different groups of events to selected risk metrics. For example, it shall be possible to calculate the contribution of
  - multi-unit initiators,
  - failures of components in a particular system,
  - human errors.
- It shall be possible to perform sensitivity analyses with regard to model parameters.

Possibility to calculate uncertainty distributions for the risk metrics would also be useful. In site uncertainty analysis, correlations of uncertainty distributions between units should be taken into account.

5. Conclusions

In this report, preliminary requirements for site PSA documentation, model management and computation are outlined. First, overall requirements for site PSA are developed. Second, the information that needs to be documented during the different site PSA analysis steps is specified. Third, requirements for a multi-unit dependency database and PSA model management process are listed. Finally, requirements for computation results are specified.

Some of the requirements might not be applicable in all cases. The set of applicable requirements depends, e.g., on the scope of the analysis, and whether the site PSA shall be kept updated. Additionally, the required level of the documentation and the scope of the single unit models can affect the extent of applicable requirements. The requirements were outlined considering a comprehensive site PSA that is updated on a regular basis.

The requirements were mainly outlined based on the presented methods [1]. The method development focused on level 1 PSA. When level 2 PSA and other radioactive sources than the fuel in the core are included in the scope, some additional requirements might be needed. In addition, the overall requirements only consider PSA applications on a general level. It is therefore, expected that the set of requirements will need updateing when more research and development work is completed and after gaining experience from site PSA work. Guidelines for site PSA model management should also be prepared.

References

1. Bäckström, O., Häggström, A., He, X., Holmberg, J-E, Tyrväinen, T. SITRON – Method development. Report 212634-R-001, 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. Holmberg, J.-E. SITRON — Risk metrics. Report 14124_R005, Risk Pilot Ab, Espoo, 2017.

4. International Atomic Energy Agency. A framework for a quality assurance programme for PSA. IAEA-TECDOC-1101, Vienna, 1999.

5. International Atomic Energy Agency. Development and application of level 1 probabilistic safety assessment for nuclear power plants. Specific safety guide SSG-3, Vienna, 2010.

6. International Atomic Energy Agency. Living probabilistic safety assessment (LPSA). IAEA-TECDOC-1106, Vienna, 1999.