SITRON - Site risk assessment approach developed for Nordic countries

Ola Bäckström[a]*, Erik Cederhorn[b], Xuhong He[a], Jan-Erik Holmberg[b], Tero Tyrväinen[c]
[a] Lloyd's Register, Stockholm, Sweden
[b] Risk Pilot AB, Espoo, Finland
[c] VTT Technical Research Centre of Finland Ltd, Espoo, Finland

Abstract: 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 reactor accident. Within Sweden and Finland a research project called SITRON on multi-unit risk has been ongoing since 2017. This paper outlines the approach, discussed within SITRON, on multi-unit risk taking into account various dependencies between the units, combination of plant operating states and relevant risk metrics to study. The approach has been developed with aid of two pilot studies made for two Swedish sites. The dependencies between units can be caused by external hazards, which can affect multiple units at the same time, shared operational and safety systems at the site and common staff who should manage the situations. The paper also presents high level results from the two pilot studies.

Keywords: Multi-unit, Nuclear power plant safety

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.

Within Sweden and Finland a research project SITRON (SITe Risk On Nuclear installations), funded by Ringhals, Forsmark, SSM and SAFIR, has been ongoings since 2017. The first objective with 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 with 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.

The methodology for a site level risk analysis or multi-unit PSA needs to consider the dependencies between the reactor units and other radioactive sources, such as spent fuel pools and storages. The overall idea is that the site level PSA should be based on existing single unit PSA models as much as possible.
The dependencies can be caused by e.g. external hazards; shared operational and safety systems at the site; common staff who should manage the situations. Site risk analysis is not only a matter of extending current PSA:s to properly cover inter-unit dependencies in the risk assessment, but it should also provide risk insights for the site level safety management.

This paper presents the current status of the project.

2. 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 1. The scope of the single-unit PSA needs to be consistent with the selected site level PSA 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 project [1] 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.

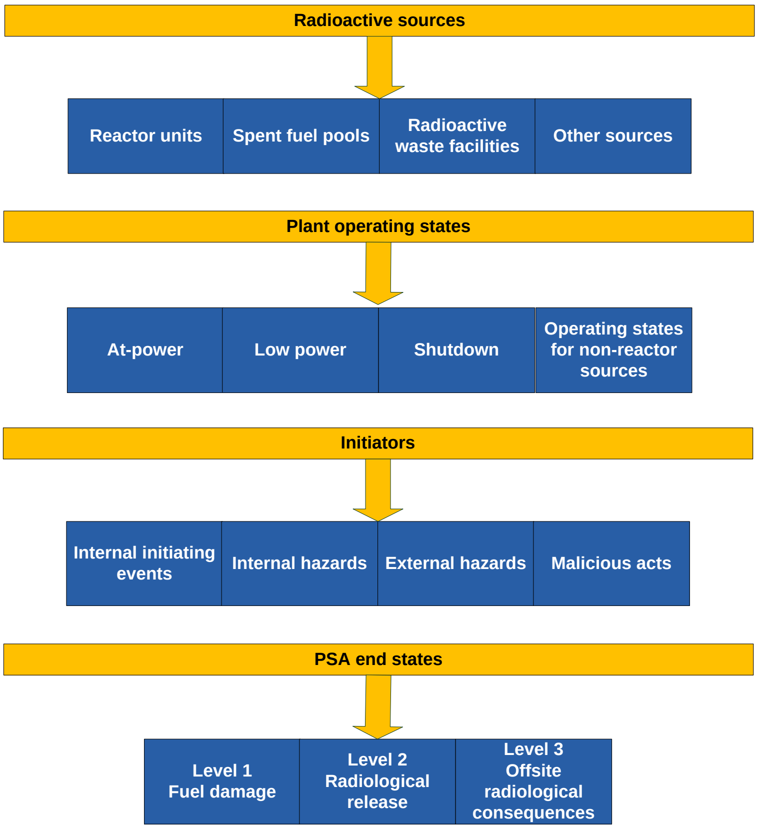
The single-unit risk metrics proposed are:

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

The multi-unit risk metrics proposed are:

- Site core/fuel damage frequency: frequency for any core/fuel damage to occur at the site per year.
- Multi-unit core/fuel damage frequency: frequency of at least two core/fuel damages occurring nearly simultaneously per site-year
- Site release category frequency: frequency of a specific site release category (considering releases from any radioactive sources) per year.

Figure 1: Selection of analysis scope for site level PSA



4. METHOD

The approach developed within SITRON considers following:

- General screening principles
- Impact of different plant operating states (POSs)
- Identification of relevant initiators
- Identification of relevant dependencies
- Data analysis
- Modelling and quantification of single-unit and multi-unit risk

The approach currently developed and discussed in this paper is mainly looking at reactor core risks and level 1 PSA. The principles should also be applicable when considering other radioactive sources to a significant extent. Level 2 PSA specific issues will be studied when the project continues.

4.1. 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. Depending on the purpose of the analysis, the screening criteria will likely need to differ. A general screening criterion for multi-unit core damage should generally be lower than a screening criterion to account for multi-unit sequences within a single-unit PSA.

Following criteria have been suggested:

- Multi-unit CDF: Scenario (a combination of multi-unit events) frequency estimated to be less than 1E-08/year. If the contribution to the CDF is less than 1E-08/year for any of the units, the contribution to a multi-unit release is expected to be insignificant.
- Single-unit CDF: Contribution from potential multi-unit sequences is less than 1 % of single-unit CDF. A less strict screening criterion can be used since these sequences must have potential to influence that specific unit’s CDF.

4.2. 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, the approach suggests that:

- 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.

4.3. 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. 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).

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

Single-unit events 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.

4.4. 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
- Spatial dependencies
- Human and organizational dependencies
- Simultaneous maintenance

The dependencies related to SSCs, components (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 sequences causes damage that would affect an adjacent unit. Simultaneous maintenance is likely possible to screen out (for example simultaneous scheduled maintenance).

The identification process is suggested to be done in two steps, qualitative screening and selection of dependencies.

4.4.1. 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

Dependencies ranked as ‘very important’ or ‘important’ in the qualitative analysis are expected to also be important from a quantitative aspect.

4.4.2. Selection of dependencies

The selection of relevant dependencies can be done in several ways. Two ways are suggested in this approach:

- Qualitative analysis of MCS list to identify and characterize the dominating combinations
- Selection of relevant dependencies through quantitative screening and characterization

The qualitative approach selects relevant dependencies by analysing the MCS list. All relevant MCSs above certain threshold (or cut-off) are studied. The MCSs that contain events that could represent a dependency are highlighted for further analysis. All highlighted MCSs represent one or multiple dependencies. The dependencies are then grouped and characterized for further analysis.

The quantitative screening approach is studying all relevant initiators. For each initiator, dependencies identified in the qualitative screening are analysed based on the Fussell-Vesely importance of the basic events related to each dependency (in the single unit MCS lists). The maximum contribution from the dependency can then be evaluated and compared with the screening threshold. The selected dependencies are then further analysed and potential combinations of dependencies are identified by studying the MCSs that contain the identified dependency.

If the selection of dependencies does not identify dependencies that were ranked as ‘very important’ or ‘important’ in the qualitative analysis, then the single-unit PSAs should be reviewed to ensure that it properly accounts for the dependency.

4.5. 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.

Below the estimate of CCF data on multi-unit context and HEPs are discussed further.

4.5.1. Common cause failure

Inter-unit CCF can be defined in the same way as normal CCF, see e.g. [2]. The only difference is that components fail in multiple units instead of a single unit. Currently, Inter-unit CCF data are scarce, and inter-unit CCF probabilities become very uncertain. Therefore, a simplified and conservative modelling approach is chosen where the only inter-unit CCFs considered are CCFs with failure of all identical components at the site (excluding identical components that appear in different systems), e.g. all identical diesel generators.

For simplicity, the only inter-unit CCF considered is a complete CCF of all nm (components there are m components in each of n units). The probability for this CCF is estimated as

$$Q^{m,n} = \varphi Q^{m},$$

where φ is the probability that all nm components fail given that m components fail in one unit. The parameter φ should be possible to estimate based on operating data. Such data may be hard to find, but [3] is discussing multi-unit CCF events and compare it with single unit CCF events.

If the parameter φ cannot be estimated from operating data covering multi-unit cases, a conservative estimation based on single-unit CCF data can be considered. The parameter φ can then be represented as

$$\varphi = \frac{Psg(mn)}{Psg(m)},$$

where $Psg(m)$ is the probability that at least m specific components fail, in this case m components in one unit. Therefore, $Psg(mn)$ and $Psg(m)$ should be estimated for example based on impact vectors.

4.5.2. Human reliability analysis

For multi-unit risk, HRA will continue to play an important role in the analysis. A few pilot studies have been performed [4], [5] or are being performed for multi-unit HRA issues [6]. 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.

In general, HRA methodologies developed and used in internal events analysis 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.

In the multi-unit accident scenarios, the existing human actions should be re-evaluated considering the site conditions, unit status and the challenging PSFs. 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.

The selected approach described in the current phase of the project document is the *Penalty approach.* One may, however, have to explicitly consider dependencies between HFEs for different units. Such dependency assessment in addition to the Penalty approach is not further analysed yet.

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 [5]. EDF proposed the use of a penalty factor with 3 levels for the risk significant human actions. The penalty factor X is estimated by expert judgement based on a number of arguments.

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

- X=1 (none). No need to increase HEP.
- X=2 (low). The influence is low
- X=5 (medium). The influence is medium based on the additional challenges
- X=10 (high). The influence is high.
- HEP=1. The influence is extremely high and the action is considered as impossible.

The preliminary penalty factors in this project are based on following information:

- Who performs the action: MCR staff, shared supervision staff, field or local staff
- Where is the action performed: In MCR or outside MCR (locally)
- The types of human actions: EOP actions, recovery or repair actions

4.6. Quantification

The multi-unit core damage frequency for a specific initiator 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.

This evaluation can be performed in different ways. 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.

The total MUCDF can be calculated by summing the MUCDF values of different initiating events:

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

4.6.1. MCS list approach

The modelling of inter-unit dependencies is implemented by transforming each basic event, A, into a product of a common basic event, cA, and a unit-specific basic event, iA (i=1,2) for a site with two units.

$$\mathrm{A} = \mathrm{cA} * \mathrm{iA}$$

All basic events can be categorised into three groups as follows:

- No dependency: P(iA) = P(A), P(cA) = 1
- Full dependency: P(cA) = P(A), P(iA) = 1
- Partial dependency: P(A) < P(cA), P(iA) < 1.

The minimal cut sets of the multi-unit core damage are directly obtained as the Boolean product of the MCS lists of the two units. Through Boolean reduction the common probability will be only accounted for once in each MCS.

$$\overline{\mathrm{K}}^{12} = \overline{\mathrm{K}}^{1} \cdot \overline{\mathrm{K}}^{2} = \sum_{\mathrm{i}} \mathrm{K}_{\mathrm{i}}^{1} \cdot \sum_{\mathrm{j}} \mathrm{K}_{\mathrm{j}}^{2},$$

Where $\mathrm{K}_{\mathrm{i}}^{1}$ and $\mathrm{K}_{\mathrm{j}}^{2}$ are minimal cut sets core damage in units 1 and 2.

The multi-unit CDF for one multi-unit initiating event is then evaluated by calculating the joint MCS list.

$$MUCDF_{IE} = f(\overline{\mathrm{K}}^{12})$$

It should be noted that if there are full dependencies between basic events, then some MCS combinations may no longer be minimal and they must be removed from the equation.

4.6.2. Multi-unit event combinations approach

The multi-unit event combinations approach uses what can be looked upon as a pre-event tree. In the pre-event tree the dependencies are considered individually or as combinations. Each sequence then represents a specific state that is resolved for each unit separately. This can be represented by following equation:

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

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 i:th combination.

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

$p(\mathrm{CD}_{unitx} | \mathrm{IE} \ \&\ \mathrm{i})$ 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 event(s) then needs to be conditionally quantified using the single-unit PSA models. This is typically achieved by setting the conditional probability to 1.0 for the dependencies studied in this particular sequence. It may also mean, in addition, that specific probabilities for certain dependencies (for example human dependencies) may be applied in that specific sequence (if increased HEP is to be applied in some sequences).

5. PILOT STUDIES

5.1. Introduction to the pilot studies

In the SITRON project, two Swedish pilot studies are made, one for the Forsmark nuclear power station [7] and second for the Ringhals nuclear power station [8]. 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).

In 2017, the pilot studies have included a qualitative analysis of unit dependencies and a quantitative analysis of the multi-unit initiating event loss-of-offsite power (LOOP). The pilot studies were limited to 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 for both sites.

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.

5.2. Identification of initiating events and POS combinations

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.

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.

5.3. Identifications of dependencies

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 common cause failure groups could be considered potential inter-unit CCF groups. It was also noticed that the CCF analysis may need to be extended to components that are single in a single unit perspective but can form a CCF group in the multi-unit perspective. Assessment of relevant CCF groups was limited to the example scenario, LOOP.

Following types of dependencies were finally considered in the evaluation:

- CCFs: Batteries, diesels, component cooling pumps, service water pumps, auxiliary feedwater pumps
- HRA: Operator actions that may involve technical support center or performed locally
- Other: house load supply, simultaneous loss of 130 kV (main is 400 kV)

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

5.3. Quantification of MUCDF

The MUCDF assessment has been very simplified, and includes several uncertainties (particularly inter-unit CCF probabilities). Conditional probability of a double-unit core damage given one core damage is 10-20% in one of the pilot studies and around 1-2% in the other. The main contributor to the MUCDF is the probability of inter-unit CCF.

6. 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.

There are different approaches for selecting the relevant dependencies to study in more detail. Which approach to choose is to some extent dependent on the degree of similarity between existing single-unit PSAs, but also on the types of dependencies. Given relevant reliability data, the quantification of site level core damage frequency is straightforward and can be achieved by for example quantifications of conditional core damage probability for each unit, considering the initiator and the dependencies.

The pilot studies conducted indicates that the MUCDF may not be negligible and that the outlined approach is possible to follow.

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).

References

[1] Holmberg, J.-E. "*SITRON - Risk metrics*", Report 14124-R005, Risk Pilot AB, Espoo

[2] 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

[3] 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)

[4] 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

[5] 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

[6] 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

[7] Cederhorn, E., Holmberg, J.-E., "*SITRON Pilot study Forsmark 1 and 2*", Report 14124-R007 u1, Risk Pilot AB, Espoo

[8] Bäckström, O., "*SITRON – Pilot Study – Project Report Ringhals 3&4*", Report 212634-R-003 v1.0, Lloyds Register Consulting, Stockholm