Framatome's lessons learned on Multi-Unit PSA

Jean-Yves Brandelet[a], Hervé Brunelière[b], and Pierre Lacaille[c]
[a] Framatome, Courbevoie, France
[b] Framatome, Courbevoie, France
[c] Framatome, Courbevoie, France

Abstract: To date, when conducting a Probabilistic Safety Assessment (PSA), each reactor of the site is in most cases considered individually. Multi-unit accidents are not systematically considered in PSA, and there is sometimes an implied assumption that the reactor is properly protected and does not participate in accident sequences impacting any other reactor at the site. The Fukushima Daiichi accident in 2011 reinforced the importance of multi-unit risk assessment. In this frame and for R&D perspective, Framatome is currently developing a multi-unit PSA and investigates the problematic specific to it. This paper presents Framatome's lessons learned on multi-unit PSA modeling as well as differences between a single unit and a site PSA.

Keywords: PSA, Multi-Unit, methodology, modeling.

1. INTRODUCTION

To date, when conducting a Probabilistic Safety Assessment (PSA), each reactor of the site is in most cases considered individually. Multi-unit accidents are not systematically considered in PSA, and there is sometimes an implied assumption that the reactor is properly protected and does not participate in accident sequences impacting any other reactor at the site. The Fukushima Daiichi accident in 2011 reinforced the importance of multi-unit risk assessment by demonstrating the possible occurrence of accidents causing core damages in more than one reactor at the same site. In fact, there is a possibility of multi-unit accident sequences involving unusual challenges to the safety systems and components and to the human resources and infrastructures that should perform the mitigating actions at each reactor. Initiating events, like external hazards or internal fire and floods in areas with shared equipment, or their potential combination may lead to accident sequences affecting multiple units alongside. Core damage or a release from one unit could also compromise the protection means of other units at the site, which is called "domino effects". Moreover, the different units on the same site often share a common electrical grid, ultimate heat sink and sometimes shared systems and structures that provide vital safety functions.

Accordingly, the probability of preventing and mitigating an accident on one unit cannot be assessed without considering the status of the other site units. And knowing that most Nuclear Power Stations worldwide host more than one single reactor and that the frequency of an accident on a multi-unit site is proportional with the number of its units, this emphasizes the importance of expanding current PSAs to account for initiating events or accident sequences that could affect multiple reactors, either simultaneously or sequentially.

Thus, international community is willing to expand current PSAs to account for accident sequences that could affect multiples reactors, either simultaneously or sequentially. Special recommendations regarding multi-unit already exist, and are included in safety standards and PSA guides to address multi-unit PSA issues (e.g. IAEA SSG-3, ASME/ANS RA-Sb-2013).

In this frame and for R&D perspective, Framatome is currently developing a multi-unit PSA and investigates the problematics specific to it.

2. DIFFERENCES BETWEEN SINGLE UNIT PSA AND SITE PSA

Some differences between a single unit PSA and a site PSA exist and may influence the results. The aim of this section is to present some of these differences and to expose the retained solutions to solve them.

2.1. Initiating Events

In order to model and observe the changes that could occur when advancing from a single unit to a multi-unit PSA, the initial list of initiating event needs to be re-screened in order to sort them as initiating event impacting only one unit at a time or as initiating event having the potential for a site accident.

It has to be noted that most initiating events, even those defined as "single unit initiating event" can impact additional units. Indeed, after a spurious reactor trip at one unit, there might be a risk of consequential loss of offsite power which could potentially impact the entire site. However the contribution of these events is expected to be low and is neglected in a first approach.

2.2. Common Cause Failures

In a single unit PSA model, Common Cause Failures (CCF) are generally considered for identical components of the unit, operating in the same conditions. In a multi-unit PSA, two types of CCF are to be considered – intra-unit CCF, as for a single unit PSA, and inter-unit CCF. CCF are significant contributors to the single unit risks, and are expected to be one of the major contributors to multi-unit risks. Thus, it is necessary to accurately take them into account in a multi-unit PSA model. The treatment of inter-unit CCF is complex, and several aspects have been studied:

- As for a single unit PSA, if the components of several units are identical and operate in the same conditions, inter-unit CCF have to be considered in addition of the existing intra-unit CCF for a multi-unit PSA. As a first approach, it has been decided to extend intra-unit CCF to inter-unit CCF only for CCF group having a large contribution to the single unit risk.
- When extending an intra-unit CCF group to an inter-unit CCF group, it is necessary to adapt CCF parameters. In case these specific parameters are not available, generic parameters are used. In any case, sensitivity analyses will be systematically performed in order to evaluate the importance of these parameters.
- Most of the PSA software allows accurately treating CCF group of size 8 at the maximum. In case the inter-unit CCF would be higher than the limiting CCF size of the software, intra-unit CCF are not modified, and the inter-unit CCF are addressed through the implementation into the PSA model of specific new basic events corresponding to the failure of all components.
- In a single unit PSA, failure of equipment used in normal operation are considered as initiating event (partial or total loss of heating ventilation and air conditioning…). In a multi-unit PSA, an inter-unit CCF of these equipment would lead to a site initiating event. In a first approach, only failure of equipment used in normal operation (as initiating event) having a large contribution to the single unit risk will be extended to inter-unit CCF as site initiating event.

2.3. Human reliability

In a single unit PSA, the human error probabilities are assessed without taking into account the status of the neighbor units. In a multi-unit PSA, following aspects need to be accounted:

- Additional stress of the operator in case of accident in the neighbor unit;
- The potential limited number of resources for local actions;
- The impossibility to perform some local actions due to radiological releases from others units;
- …

Depending on the HRA method, the way to penalize Human Error Probability (HEP) in case of multi-unit event may be different. As an example, if the ASEP method is used, it is possible to reassess all the HEP increasing some parameters (the level of stress, the recovery factor…). Another simpler solution is to systematically apply a penalizing factor to HEP in case of multi-unit event. In a first approach, the systematic penalization is the retained solution. Sensitivity studies should be performed to evaluate the importance of the HEP.

2.4. Management of different plants operating states

In a single unit PSA, external events are assumed to occur at a random time, equally repartee among the year. For a Multi-Unit PSA, it is necessary to establish the initial plant operating state of each unit of the site at the time of the initiating event. Considering all possible combinations of plant operating states in a multi-unit PSA is very ambitious, even in case of a site with only two units. Assumptions and simplifications need to be made in order to reduce the number of combinations of plants operating states to a manageable number. A reasonable assumption is the reduction of the number of combinations based on the single unit PSA results. As an example, if the contribution to the core damage frequency of one initiating event in a specific state is negligible compared to others states, then the configuration with at least one unit in this plant operating state could be screened out.

3. MULTI-UNIT PSA MODELING

For R&D perspective, the Multi-Unit PSA level 1 under development by Framatome considers a two-unit site, with two identical reactors. It is based on an existing single unit PSA model.

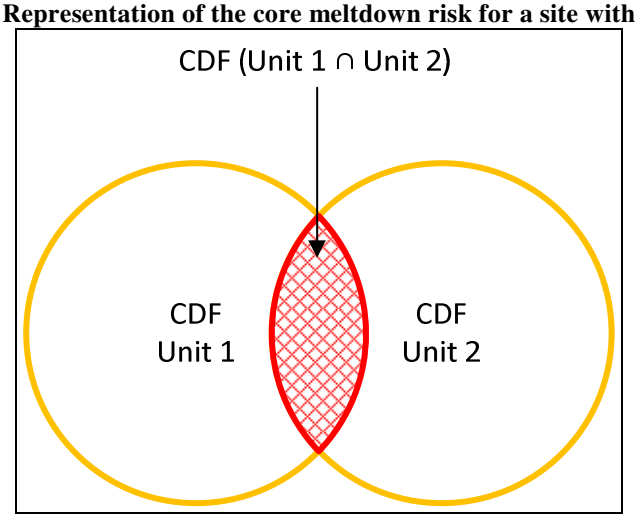
The mains steps to develop a Multi-Unit PSA are the following:

- Definition of new metrics;
  To take into account multi-unit consideration and to assess the site risk, the single-unit metrics are not appropriate. It is thus necessary to redefine them.
- Identification of shared components, structures and resources;
  In order to accurately model dependencies between both units, shared components, structures and resources have to be clearly identified. As an example, if a shared component is used by Unit 1, it has to be considered unavailable for Unit 2.
- Screening of Initiating Events;
  It is necessary to identify initiating events having the potential for a site impact. At this stage, the retained initiating events for multi-unit assessment are external events.
- Construction of a Multi-Unit PSA model
  It is necessary to adapt the current single unit PSA model to accurately model multi-unit aspects this is performed by:
  - Duplicating the single unit PSA model;
  - Creating multi-unit event trees.

3.1. Site risk assessment

In a single unit PSA, the PSA level 1 consequences can be tagged as "S" (Safe) or "CD" (Core Damage). These consequences are not appropriate to assess the risk of a site composed of several units. Indeed when a site with two units is considered, the risk may be represented by a diagram as shown in Figure 1 below.

Figure 1: Representation of the core meltdown risk for a site with two units



This representation shows that some accident sequences concern only Unit 1 (respectively Unit 2) and that conversely, some accident sequences impact both units at the same time or within a short period of time.

In order to assess the PSA level 1 site risks (core damage in one unit or in both units at the same time) the following consequences are considered:

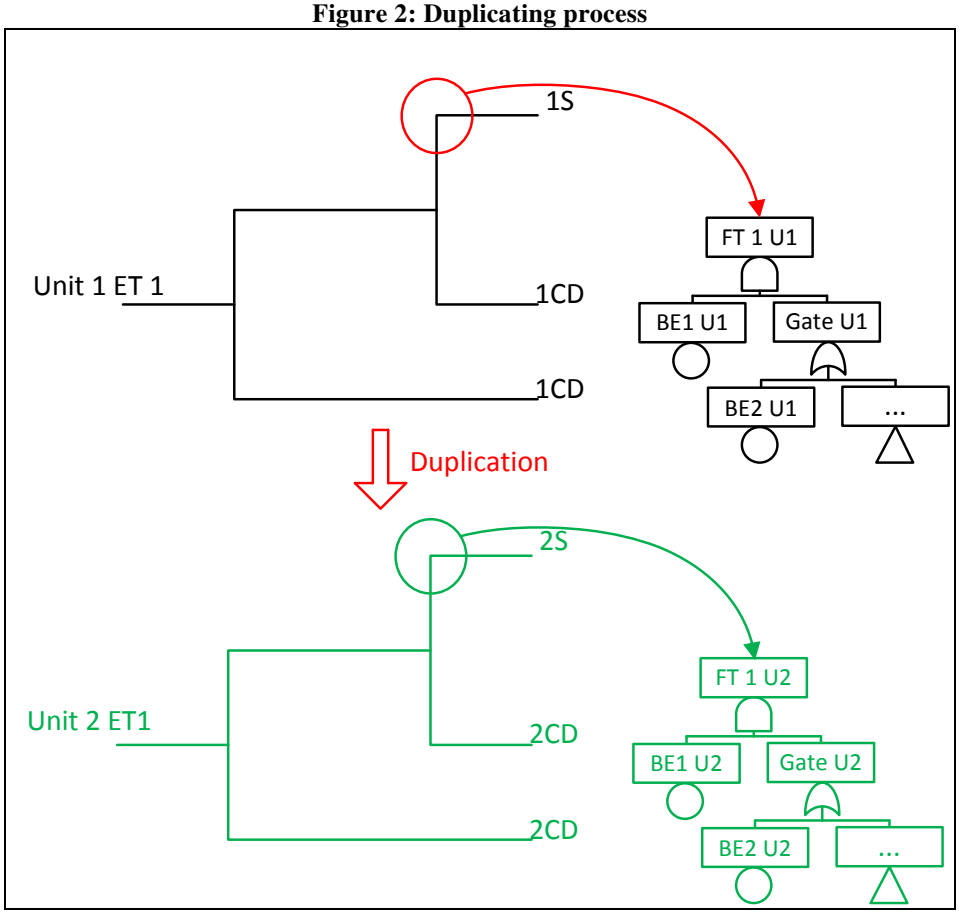
- 1S2S: no core damage in both units;
- 1S2CD: no core damage in unit 1 and core damage in unit 2;
- 1CD2S: core damage in unit 1 and no core damage in unit 2;
- 1CD2CD: core damage in both units.

3.2. Multi-Unit PSA model construction

The first step of the construction of the Multi-Unit PSA model consists in the duplication of the existing PSA model, inside a single model as shown in Figure 2. This allows having one PSA model containing two single units PSA. It consists in:

- Duplicating Event Trees (ET) of unit 1 renaming them for unit 2;
- Duplicating Fault Trees (FT) of unit 1 and renaming them for unit 2;
- Duplicating Basic Events (BE) (with associated parameters), Gates, House Event, common cause failures groups… of unit 1 and renaming them for unit 2.

Figure 2: Duplicating process

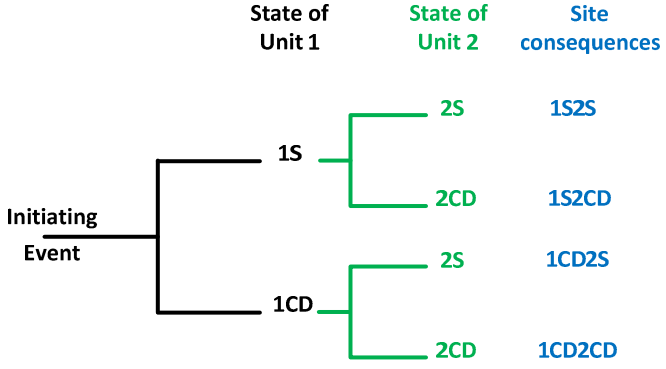


Firstly, all attributes of the single unit PSA model (event trees, fault trees, basic event, parameters, house event, BC set…) must be renamed to associate them to the unit 1. Then, event trees of unit 1 (Unit 1 ET 1) and their associated fault trees (FT1 U1), basics events (BE1 U1, BE2 U1), gates (Gate U1) consequences (1S, 1CD) and all associated attributes are duplicated and renamed for unit 2. This duplication process is applied for all attributes, except for those related to shared components, structures or resources. For this specific case, a basic event modeling the failure of one shared component will be linked to both fault trees of unit 1 and unit 2.

Eventually, the created model contains two single unit PSA models, which will be the basis of the multi-unit PSA model.

To obtain Multi-Units Event trees, it is necessary to link the event trees of unit 1 and unit 2 and to address the site consequences, as shown in Figure 3.

Figure 3: Multi-Units Event Trees



Following an initiating event having a site impact, it is necessary to assess the states of both units. Thus, the event tree of unit 1 is modeled in order to define the state of unit 1 (Safe – 1S or Core Damage – 1CD). At the end of each sequence, event trees of unit 2 (created in the previous step), are linked to assess the state of unit 2 (Safe – 2S or Core Damage – 2CD). Eventually, the state of each unit is known at the end of each sequence, which allows defining the site consequences (1S2S or 1S2CD or 1CD2S or 1CD2CD) and finally assessing the site risk.

4. LESSONS LEARNED

4.1. Duplication method

The duplication process is very time consuming, and faced a lot of issues.

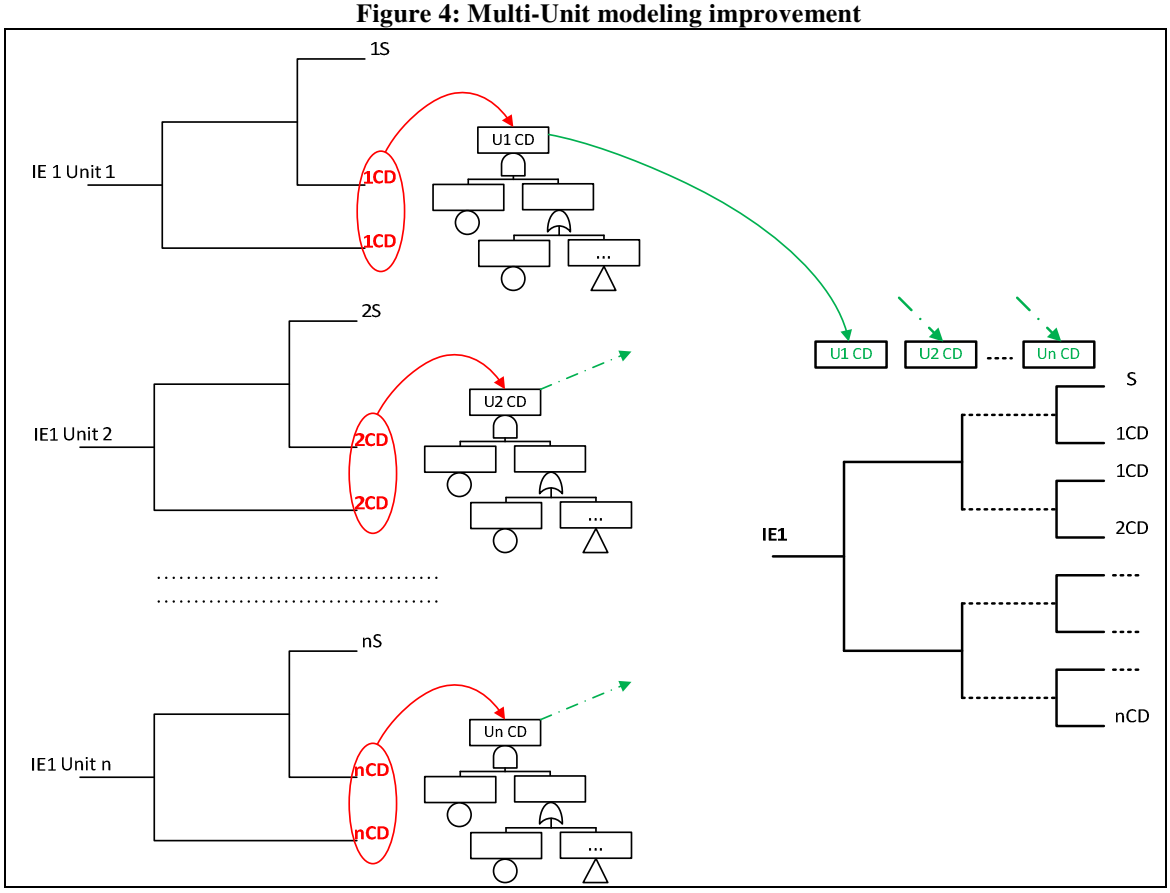
- Conventional PSA software does not allow automatically duplicating a PSA model. It is thus necessary to manually export all the data to an external file, to modify them by adding a "1" character for unit 1 components identification, or a "2" character for unit 2 components identification and eventually to reimport the data.
- The export/import process cannot be applied to Event Trees, which means that duplication of Event Trees has to be performed manually.
- The export/import process also generates some bugs (as an example some fault tree were not linked correctly between them). These bugs cannot be automatically detected, thus their identification and correction was manually performed.
- The identification length of basic event, fault trees, gate… is limited, and some identifications of the existing PSA model already reached this limit. In order to solve this problem, a complete rework of the naming rules was necessary.

The single unit PSA was not build having in mind the possibility to duplicate it. For future PSA model, it is recommended to anticipate this need, and to define an appropriate naming rule allowing adding a character to identify the considered unit.

3.2. Multi-Unit Event Trees

The construction of Multi-Unit Event Trees as shown in Figure 3 leads to a large number and complexes sequences to be evaluated, which leads to very long calculation times. In addition, even if this modeling could be appropriate for a two unit's site risk assessment, it would rapidly become unmanageable if the number of units of the site increases. An alternative approach for dealing with complexity of sequences for MUPSA exists. It aims at converting Event Trees into Fault Trees and to eventually build a new Event Tree allowing counting the number of units in core damage as described in Figure 4. The main advantages of this modeling are that it can be applied to a large number of unit and that the number of sequences to be assessed is limited, which should reduce the calculation complexity. However the converting process may be complex and needs to be investigated.

Figure 4: Multi-Unit modeling improvement



In the above example, a site initiating event affecting "n" units (IE1 Unit i) is considered. For each event tree of each unit, sequences leading to core damage are converted into a single fault tree (Ui CD). The conditional core damage frequency (conditioned to initiating event "IE1") of each unit can thus be assessed by the "Ui CD" fault tree analysis, instead of the classical consequence event tree analysis. Then, a multi-unit event tree is build, having these fault trees as input. The success branch represents the safe state of unit i, while the failure represents the core damage state. At the end of each sequence, the state of each unit is known, and the associated consequences represent the number of unit being in core damage.

5. CONCLUSION

This paper has presented the modeling principles of a Multi-Unit PSA under development by Framatome in R&D, and some lessons learned specific to multi-unit PSA. Although the duplicating process faced a lot of issues mainly due to PSA software limitation, the construction of the multi-unit PSA model based on an existing single unit PSA model is a success. Some improvement are already identified to reduce the calculation time and to anticipate the need of a multi-unit model including more than two units. Some differences between a single unit and a site PSA model have also been presented as well as the way to manage them in a first approach. These aspects must be investigated deeper in the future as well as the following points:

- Management of different plants operating states;
- Adaptation of the methodology to deal with PSA level 2 and level 3;
- Development of a methodology to take into account accident sequences involving reactor building accident and spent fuel pool accident;
- Development of a methodology allowing taking into account different accident progression on various unit (investigation on dynamic PSA).