Multi Units Probabilistic Safety Assessment: Methodological elements suggested by EDF R&D

Tu Duong Le Duy, Dominique Vasseur , and Emmanuel Serdet

Industrial Risk Management Department
EDF R&D

Abstract: Most nuclear generation sites worldwide have more than one reactor in operation. This should be taken into account when assessing the risk related to these installations, in particular, when assessing the consequences in terms of impacts on the health of the population and on the environment. Generally speaking, to date mainly models relating to a single unit have been developed by operators. The purpose of this paper is to present possible solutions or methodological options, suggested by EDF R&D division, in order to switch from a risk assessment for the unit to a risk assessment for the site. The case of a site with two units is addressed here. A review of practices and standards showed that the specific aim of a PSA at site level was to deal with the dependencies existing between the units on that site. The risk calculation for the site is therefore proposed for six configurations resulting from the combination of two types of scenarios and three types of systems which are defined. The treatment of CCF events and the adaption of the assessment of the Human Errors Probabilities to the case of multiple units are also addressed in this paper. The proposed approach is illustrated using a simplified case inspired by the EDF 900MWe units level 1 PSA model.

Keywords: PSA, multi-unit, common cause failures

1. INTRODUCTION

Most nuclear generation sites worldwide have more than one reactor in operation. This should be taken into account when assessing the risk related to these installations, in particular, when assessing the consequences in terms of impacts on the health of the population and on the environment. However, to date only PSA models relating to a single unit have been developed by operators, particularly because the events under consideration were mainly internal events. A review of practices and existing standards [1] showed that the specific aim of a PSA at site level was to deal with the dependencies existing between the units on that site. These dependencies may stem from various sources:

- Both units are on the same site and are therefore subject to the same environmental stresses, particularly in terms of external hazards.
- Systems may exist that are shared by both units. These shared systems may be of three types:
  - identical systems in each unit;
  - systems that are shared on a site level;
  - standardised systems where interconnections exist and a system on one unit can be backed up by the same system on the other unit.
- There may be shared or inter-connecting rooms between the two units.
- There may be shared resources in terms of operating and maintenance teams.

The figure 1 gives a representation of such a site. A unit level 1 PSA model is often developed by assuming that there is only one unit on the site considered. This case can therefore be summarized as follows: The initiating events emerge and/or are applied to a single unit and the consequences are therefore assessed for this unit only. The frequency of the initiating events (internal events and internal and external hazards) is expressed as /unit.year, as is the associated risk. Any systems shared on the "site" level and all human resources, are credited entirely for this unit. Any backup of one unit by a twin unit may be evaluated based on the assumption that it is systematically available.

The question that can be asked is the following: should the risk associated to the unit model simply be multiplied by 2 to obtain the risk for a site with two units? Strictly speaking, the answer is no. Indeed, a unit model, as previously described, can overestimate the risk by not correctly taking into account the standardization of certain systems. Conversely, it underestimates the risk by:

- fully crediting the site shared systems for the unit studied,
- not taking into account any sharing of human resources on the site in the event of accident scenarios,
- forgetting initiating events generated in a unit and that propagate to the other unit,
- not taking into account any impact of the presence of two units on the frequency of certain initiating events.

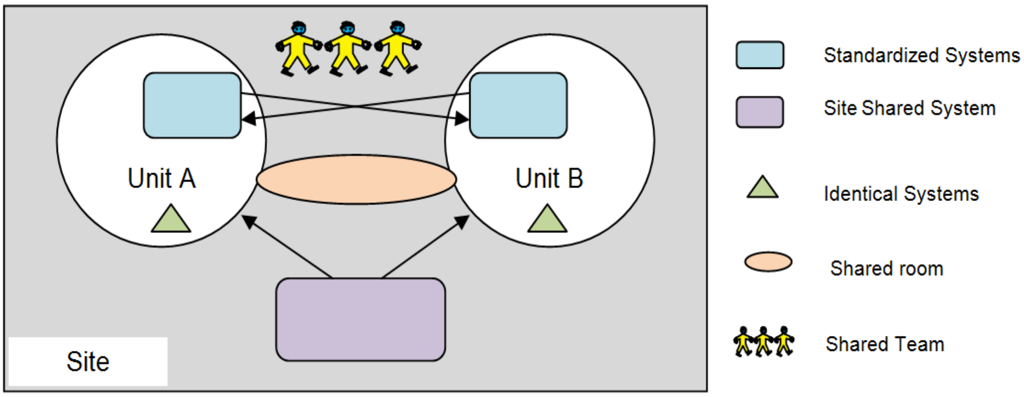


Figure 1: Representation of a site with two units with its dependencies

It is difficult to actually foresee the impact of these opposite effects on the overall risk. The case of the Seabrook PSA [2] [3] shows a risk of core meltdown at the site level that is slightly lower than twice the risk at the unit level. But can this be generalized? Probably not. Thus, the limits of a unit PSA model, as previously defined, need to be extended in order to correctly assess the risk for the site. These limits in fact relate to three aspects of the PSA model: initiating events, modelling of common systems (and related data) and consideration of the human factor. The purpose of this paper is to propose solutions or methodological options, depending on the situation, in order to switch from a risk assessment for the unit to a risk assessment for the site. Only the case of a site with two units is considered here.

The section 2 of this paper presents the general formula of evaluating the risk for a site and a proposal of classification of initiating events and common systems existing between the units on the site. In section 3, we propose the methodological options to switch a unit PSA model to a site model with the consideration of the existing dependencies between the units. The implementation of these proposed solutions is illustrated in section 4 by using a computerized PSA model in RiskSpectrum software, on a simplified example. Some conclusions and perspectives are given in section 5.

2. RISK ASSESSMENT FOR THE SITE

When a site with two units A and B is considered, the risk may be represented in the figure 2. This representation shows that some scenarios only concern unit A (respectively B) with no impact on unit B (respectively A) and that conversely, some scenarios have an impact on both units at the same time or within a short period of time. The calculation for the core meltdown risk for the site is therefore expressed by:

$$P(meltdown_{site}) = P(meltdown_A \cup meltdown_B) = P(meltdown_A) + P(meltdown_B) - P(meltdown_A \cap meltdown_B) \quad (1)$$

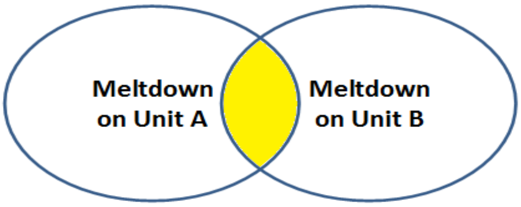


Figure 2: Representation of the core meltdown risk for a site with two units

To model this risk at site level, it should therefore be possible to correctly identify and treat in a unit PSA model:

- The initiating events that may only affect one unit at a time. These events will be called type I initiating events throughout the rest of this paper.
- The initiating events that have the potential to affect one or both units at the same time. These events will be called type II initiating events.

Furthermore, the accident scenarios produced by these initiating events may require the use of the 3 types of common systems, as defined in section 1. Therefore, the dependencies produced through the use of these systems should be modelled correctly and included in $P(meltdown_A)$ and $P(meltdown_B)$. Given the above-defined 2 types of initiating events and 3 types of common systems, 6 standard scenarios can be defined. A similar concept of classification of events and systems related to multi-unit PSA aspects is also discussed and proposed in [4]. Finally, the management of shared resources in terms of operating and maintenance teams needs to be taken into account specifically in a multi-unit PSA.

In the following paragraphs, the distribution of events by type of initiating event (I or II) are discussed based on their origin (internal events, internal hazards, external hazards), the types of common systems are presented in more detail.

2.1 Initiating events

The above-defined two types of initiating events may have various origins: internal events, internal and external hazards.

- **Internal events**

These initiating events emerge in a given unit for an intrinsic cause (equipment failure, human error) and are not propagated to the twin unit. Thus, this category includes all of the initiating events for the following families. These internal events only cause type I initiating events.

- Loss of Coolant Accident
- Loss of Low Voltage Power Supplies
- Loss of High Voltage Power Supplies excluding total loss of offsite power globally affecting a site
- Steam Generator Tube Rupture
- Feedwater Pipe Rupture
- Steam Pipe Rupture
- Secondary Transients
- Primary Transients

- **Internal and External hazards**

Internal hazards mainly include fires and internal flooding. Fire or internal flooding scenarios may remain confined to the unit studied. Therefore, these are type I initiating events. This may also apply to fire or internal flooding scenarios that propagate from one unit to the other. Therefore, there are two possibilities:

- fire or flooding occurs in unit A with no consequences on this unit then propagates to unit B with an initiating event occurring on this second unit. In this case, this is a type I initiating event on unit B.
- fire or flooding occurs in unit A with an initiating event occurring on this unit, then propagates to unit B with an initiating event occurring on this second unit. Therefore, these will be type II initiating events.

External hazards may potentially affect both units at the same time. Therefore, these will be type II initiating events. The hazards to be considered for a given site are identified via a screening stage during which the potentiality of the occurrence of the event and its consequences on the site are assessed [5].

2.2 Common systems

As indicated in section 1, three types of common systems are considered: identical systems, standardized systems and shared systems.

- **Identical systems in both units**

These systems are present in each unit. They do not have any possible interconnections. They may be required by each unit, for the mitigation of an initiating event affecting both units, and as they are identical, this makes them potentially sensitive to "inter-unit" common-cause failures, in addition to "intra-unit" common-cause failures that are usually modelled for systems with redundancy. The main diesel generators of the units constitute an example of such a type of system. Each unit has two redundant diesel generators, for which an “intra-unit” CCF (common-cause failure) group of 2 is generally modelled. The diesel generators are identical for both units, so in the event of total loss of offsite power affecting these two units, the potentiality of a CCF affecting the 4 diesel generators and thus leading potentially to "simultaneous" meltdown of both units should be studied.

- **Standardized systems**

These systems are identical and present in each unit; interconnections exist and a system on one unit can be backed up by the same system on the other unit. For these standardized systems, two cases are possible. In the first case, the system on one unit is in fact designed to support both units, for example, the service water supply system. In the second case, the system of each unit has redundancies that can be used to backup the neighbouring unit. This type of case can be illustrated via the RCV (CVCS charging pump) system of a 900 MW unit, which under certain circumstances, can be used to backup the twin unit. In this case, the problem of potential inter-unit CCF should be studied, as should the impact of the respective operating mode of both units on the success criteria to be taken into account in the modelling.

- **Site shared systems**

These systems are unique for the site. They can potentially be used by one or both units at the same time, providing that they are designed to do so. The Emergency Diesel Generator for the 900 MW units of EDF's unit constitutes an example of such a type of system. In this particular case, this shared system can only be used by one unit at a time.

3 CALCULATION OF THE RISK FOR THE SITE ACCORDING TO THE SCENARIO ANALYZED

As indicated in section 1, in order to evaluate the risk for the site from the existing the unit model PSA, the existing unit PSA model needs to be modified and upgraded to take into account the dependencies between the units. This upgraded PSA model needs to be developed for each unit. In this section, we propose some methodological solutions for each scenario. A specific methodology for the assessment of HEPs is also proposed.

3.1 Upgraded unit PSA model for the site given a type I initiating event

A type I initiating event cannot (or with an extremely low probability) cause meltdown on the two units at the same time. Thus, the conditional probability of having "simultaneous" meltdowns of both units $P(meltdown_A \cap meltdown_B)$, given this event, can be considered negligible.

- **Identical system (Type i)**

It is assumed that the type I initiating event that occurs on unit A, requires the operation of a system S_A that is identical on unit B (S_B). It is assumed that each system S_A and S_B has n identical redundant components (Figure 3). As the initiating event only affects one unit and the systems S_A and S_B are not interconnected, only S_A "intra-unit" failures will be taken into account in the modelling. Therefore, only potential CCF between identical components located on the same unit (called intra-unit CCF) needs to be considered in a

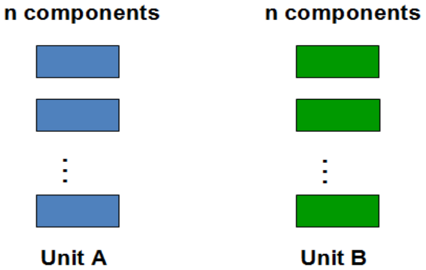


Figure 3: Representation of identical systems

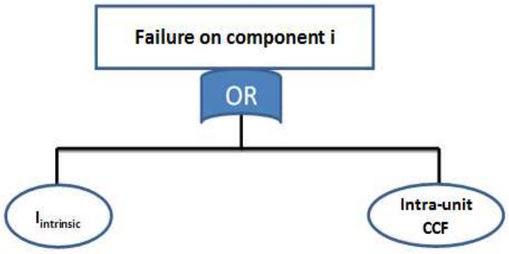


Figure 4: Failure of component i of a Type i system

unit PSA model (figure 4). The failure of a component i, for the system of a given unit, consists of the intrinsic failure of this component and the intra-unit common-cause failure shared with the other components of the same unit. In comparison of a traditional unit PSA model, there is no modification in modelling of this system to be made in this case.

- **Standardized systems**

It is assumed that the type I initiating event occurring on unit A, requires the operation of a standardized system. This system comprises a system S_A in unit A and a system S_B in unit B, that can be interconnected (Figure 5). In this case, even if the initiating event only affects unit A, as all or part of system S_B can be used as backup, the potential for two types of CCF must be studied, i.e. intra-unit CCF usually taken into account and inter-unit CCF (figure 6). The latter is defined as the common-cause failure shared between the components of systems S_A and S_B located on two units.

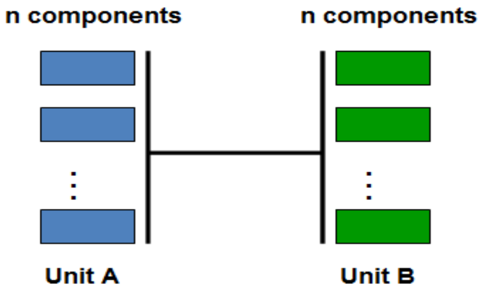


Figure 5: Standardized system

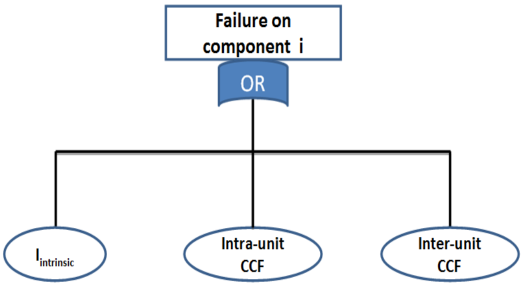


Figure 6: Failure of a component all causes

If it appears that inter-units CCF can occur, then the failure of standardised system (S_A or S_B) will therefore be modelled considering a CCF group of m=2n. Depending on the design basis of each system and the respective operating mode of both units, we may have various success criteria for the standardized system. Actually, in some situations, it may occur that the backup of unit A's system (S_A) by unit B's system (S_B) becomes impossible due to the fact that the latter is totally required in the operating mode of unit B.

To generalize, we can say that depending on the possible unit operating modes, a certain number of components are required for each unit. In this case, the calculation of the risk for each unit or for the site depend on the success criterion of each system S_A and S_B. Let us call x ($x \le n = m/2$) the number of components required for the normal operation of unit B which is not affected by the IE. This gives C_m^x (x out of m) possible mutually exclusive cases. Normally, by design, unit B needs n components located on this unit for the operation. In this case, this gives C_n^x possible cases (mutually exclusive). In each possible case, when x components are reserved for unit B, $m - x = 2n - x$ components remain available in order to mitigate the accident condition (IE) on unit A. Let us call y ($y \le n = m/2$) the number of components required for unit A out of $(m - x)$ available components. The standardized system S_A on a unit affected by the IE fails when at least $(m - x - y + 1)$ components out of $(m - x)$ are out of order. To illustrate the proposed modeling that needs to be integrated in a unit PSA model, the following example is used:

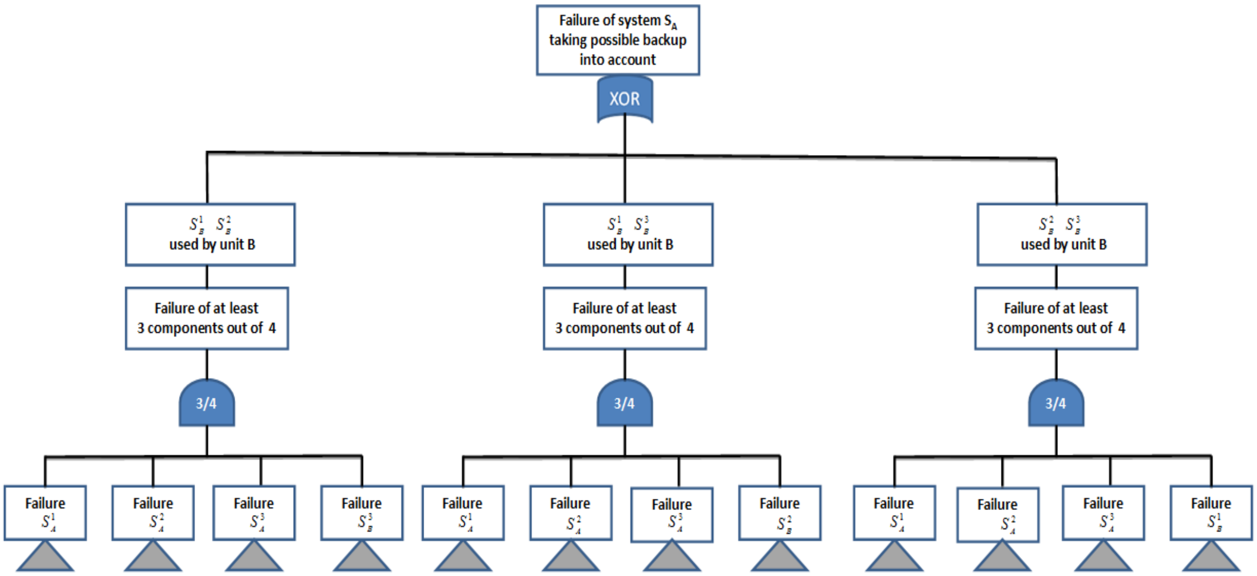

Failure of system S_A taking possible backup into account
XOR
S_B^1 S_B^2 used by unit B
S_B^1 S_B^3 used by unit B
S_B^2 S_B^3 used by unit B
Failure of at least 3 components out of 4
Failure of at least 3 components out of 4
Failure of at least 3 components out of 4
3/4
3/4
3/4
Failure S_A^1
Failure S_A^2
Failure S_A^3
Failure S_B^3
Failure S_A^1
Failure S_A^2
Failure S_A^3
Failure S_B^2
Failure S_A^1
Failure S_A^2
Failure S_A^3
Failure S_B^1

Figure 7: Failure of system S_A taking into account possible backup by neighbouring unit

It is assumed that each unit has 3 components (n=3). Therefore, this gives in total m=2n=6 components for two systems. Unit B, which is not affected by the IE, needs x=2 components for normal operation. This gives $C_n^x = C_3^2 = 3$ *possible and mutually exclusive cases. In each possible case, when x=2 components are reserved for unit B,* $m - x = 4$ *components remain available for unit A, which is affected by the IE. It is assumed that unit A needs y= 2 components to mitigate the accident condition (IE). The standardized system (S_A) on the unit affected by the IE fails when at least 3 components* $(m - x - y + 1 = 3)$ *out of 4 fails. Figure 7 shows the fault tree for the standardized system S_A taking into account possible backup for this example.*

- **Shared systems**

In the case where a type I initiating event occurs only on unit A, site shared system is considered as totally available for this unit.

3.2 Upgraded unit PSA model given a type II initiating event

A type II initiating event may cause a core meltdown on at least one of the two units. Thus, the conditional probability of having two unit meltdowns at the same time, given this event, could be not zero. The modeling of common systems for a type II initiating event is described hereafter.

- **Identical systems**

It is assumed that the type II initiating event affects unit A and unit B at the same time or within a short period of time and requires the operation of systems S_A and S_B (see figure 3). Given the similarity of systems S_A and S_B, the potential for intra-unit CCF and inter-unit CCF must be studied (see figure 6). As in the case of standardized systems, the inter-unit CCF implies the common-cause failure shared between the components of systems S_A and S_B located on two units.

In order to model the intra-unit CCF and inter-unit CCF in a unit PSA model, there are two possibles solutions. The first solution consists of considering a CCF group of m=2n components by taking into account all possible combinations of failures of 2n components. The second solution which is proposed in [1] considers the intra-unit CCF and only the inter-unit CCF affecting all 2n components. Therefore, in comparison to the first solution, some possible combinations of inter-units CCF are excluded in this second solution. Based on the availability of operating feedback data or the expert's jugement, an appropriate solution can be adopted. In general, the first solution will give more conservative results in terms of risk.

- **Standardized systems**

It is assumed that the type II initiating event occurring on units A and B, requires the operation of a standardized system. As in the case of a type I initiating event, as all or part of the twin unit's standardized system can be used as backup, this requires studying the potential for two types of CCF in the system's modelling: intra-unit CCF and inter-unit CCF. The failure of this system would therefore be modelled considering a CCF group of m=2n. As in the previous case, depending on the design basis of each system and the respective operating mode of both units, we may have various success criteria for the standardized system. In this case, the risk for the site is calculated in the same way as for a type I initiating event except that the conditional probability of having "simultaneous" meltdowns of both units, could be different from zero.

- **Shared systems**

If the type II initiating event affects both units A and B and requires the operation of a site shared system, then an analysis must be carried out on the shared system's ability to be used by one or both units at the same time. Thus, for each shared system, a study must be conducted to check its ability to fulfill its safety missions if initiating events (internal or hazards) occur. Based on the results of this analysis, two cases can be distinguished for modelling such a system. In the case where the shared system is able to supply both units at the same time (e.g. case of the SER (conventional island dematerialized water distribution system) tank), then this system will be credited for each unit.

However; if it is demonstrated that the shared system is not large enough, then a conservative assessment of the risk will involve not crediting it for either units. A more realistic assessment will involve crediting the shared system for one of the units taking account of the respective operating modes of both units. Indeed it may exist some specific reactor operating modes where the shared system cannot be used. For example, let us suppose that the shared system is required at power (RP) but not in shutdown mode (AR). If unit A (respectively unit B) is at power and unit B (respectively unit A) in shutdown, then the shared system will be credited entirely for unit A (respectively unit B). If both unit are at power, an availability factor will be introduced in the model to represent the cases where unit A (resp. B) needs the shared system that is already used by unit B (resp. A). The fault tree presented in figure 8 shows a way to take account of the operating modes of both units.

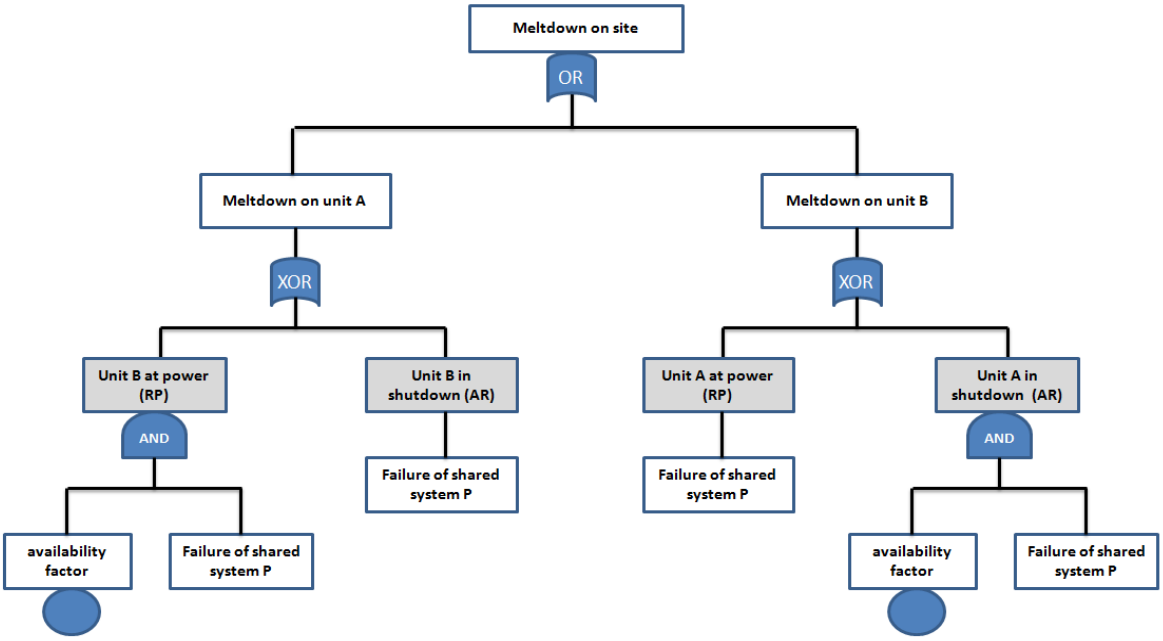


Figure 8: Fault tree for shared system given the reactor operating modes

3.3 Consideration of the human factor in the level 1 PSA

Consideration of the sharing of human resources across a particular site can have two types of consequences:

- An impact on certain assumptions associated with the PSA model, particularly repair times, mission durations or success criteria.

- An impact on the assessment of the probability of the failure of the missions carried out by these shared teams.

These two points will be addressed only for type II initiating events. They are explained in the sections below.

- **Impact of the consideration of shared teams on assumptions of the PSA model**

The existence of shared maintenance teams may have an impact on the way in which the type II initiating events are modelled. This is because if the same maintenance team needs to work on items of equipment in both units, the operations will take longer to complete. This may have an impact on the repair times if they are explicitly modelled. There could also be an impact on other assumptions. Even if the repair times are not explicitly modelled, they may be subject to modelling assumptions or may even be concealed behind corrective factors.

- **Human reliability assessments**

A specific process for determining and analyzing the HEPs is proposed. The idea is to apply a fixed penalty to the critical HEPs in the PSA, linked to the "additional human and organizational workload" involved when two accidents are handled at the same time (even if there is no exact association between the operating modes of the reactors and the actions required at the units concerned). This fixed penalty must be applied unit by unit, and only if the analysis of HEP shows that one or more “function” of the team (action implementation, monitoring and coordination, independent checking) are diminished. This penalization overcomes the HRA method (particularly in order to estimate multi-units impacts in the PSA level 2).

The process proposes four steps as below.

Step 1 : selection of critical HEPs

Given a specific Initiating event, critical HEPS to consider are identified using qualitative sequence analyses (QSAs). The suggestion is to focus only on the major HEPs, and to carry out screening as follows:

- Risk increase factor RIF 1%
- Risk decrease factor RDF 1.0 E-05

Step 2 : analysis of each critical HEPs selected according to the context of hazard

The actions to be taken within each of the HF missions are identified according to the following categories:

- State-oriented approach management actions in the main control room;
- Local state-oriented approach management actions (reactor building), using the compendium of local electrical equipment sheets or the compendium of local alignment sheets for the state-oriented approach;
- Additional specific incident management actions related to the context of the hazard (e.g. fuel handing and storage system / fuel building);
- Equipment recovery actions required by the state-oriented approach instructions, to be carried out by on-call staff, using the compendium of on-call sheets.

Step 3 : determine the generic assumptions for the site

Organizational and staffing assumptions must be determined, as functions that are normally provided for two or more units and presence and/or arrival time on site:

- Operations Manager and Supervisor: number of units managed / supervised;
- Safety Engineer: on site or on call, arrival time…;
- Number of control room operators and field operators by unit;
- Time rigging for on-call staff (recovery actions)
- …

Step 4 : fixed penalty for each HEPs

We could apply a penalty for the HEPs, in exactly the same way for each of the units, for the following reasons:

- The overall hazard context at the site is taken into account, as it is assumed that the hazard initiating event will cause the same initiating event at each unit (i.e. overall degradation: need for inter-unit communication, coordination between control rooms, etc.);
- A single "unit" PSA model is used.

To do this, the HEPs are given penalties on three levels (figure 9), according to the roles defined by the state-oriented approach policy, taking into account the data of steps 2 and 3 :

- Permanent supervision (SPE), the management strategy "independent checking" function, by the Operations Manager or the Safety Engineer;
- Incident/accident management supervision, the management strategy "monitoring & coordination" function, by the Supervisor;
- The "action implementation" function, in the control room and in the area/room involved.

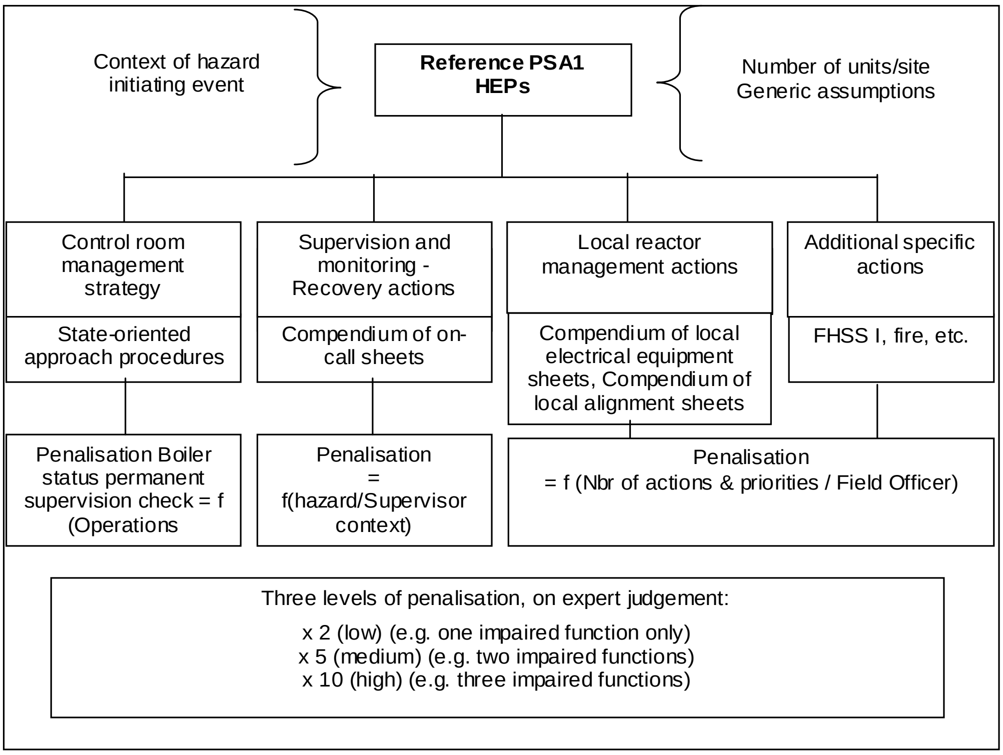

Context of hazard initiating event
Reference PSA1 HEPs
Number of units/site Generic assumptions
Control room management strategy
Supervision and monitoring - Recovery actions
Local reactor management actions
Additional specific actions
State-oriented approach procedures
Compendium of on-call sheets
Compendium of local electrical equipment sheets, Compendium of local alignment sheets
FHSS I, fire, etc.
Penalisation Boiler status permanent supervision check = f (Operations
Penalisation = f(hazard/Supervisor context)
Penalisation = f (Nbr of actions & priorities / Field Officer)
Three levels of penalisation, on expert judgement:
x 2 (low) (e.g. one impaired function only)
x 5 (medium) (e.g. two impaired functions)
x 10 (high) (e.g. three impaired functions)

Figure 9: HEP penalization process

4 PRACTICAL EXAMPLE

The aims of this section are to show how to set out the above-mentioned methodological recommendations in practical terms and illustrate how a "usual" PSA model for a unit can be converted into a model for a site and to draw particular lessons from it on the strategy to be implemented. To ensure that all stages of the construction and development of the model are successfully managed, implementation in PSA RiskSpectrum software is based on a simplified case, which is representative of a real situation.

4.1 Presentation of the case

In the case studied, a site with two units is always considered. The units may be in two operating modes: power operation for 80% of the time and outage for 20% of the time. These units are affected by two initiating events only:

- An EI_I type I initiating event, with a frequency equal to 1E-05/yr, requiring the completion of the following missions:
  - an LP mission, specific to each unit, with a failure probability γ_{LP} equal to 1E-03;
  - if the LP mission fails, an SI mission supported by train A of the SI system, which is identical in each unit;
  - if the SI mission fails, an SP mission supported by an SP system shared at site level and requiring an HF mission;
  - if the SP system mission fails, an SB mission supported by an SB system standardised for both units. The two systems are assumed to be connected through the same human mission as previously;
- an EI_II type II initiating event, with a frequency equal to 1 E-4/yr, requiring the completion of the same missions with the exception of LP. The SI system mission, in this case, involves making one of the two components I_k operate in redundancy mode for one unit.

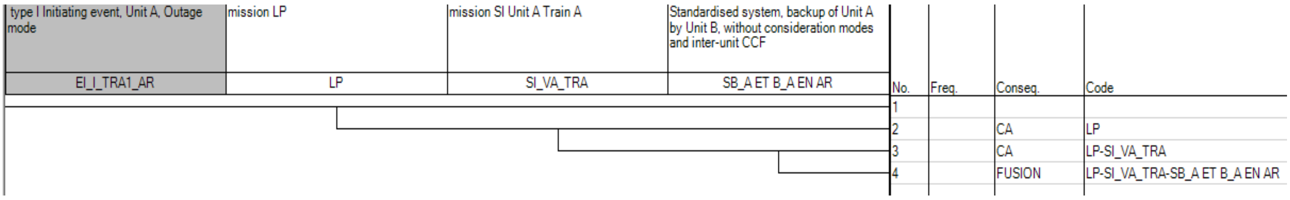
The features and data associated with each of the systems in question are as follows:

- The shared system SP comprises a single component P, which has a failure probability γ_P equal to 1 E-03. When the unit is at power, this system is required to deal with type I and II initiating events. However, it cannot be used during unit outage.
- Each unit's SI system comprises two components I_k in redundancy mode. The failure probability of each component γ_i is equal to 1 E-03. Intra-unit common cause failures may affect this system's components; the corresponding alpha factor α_2 is equal to 1 E-02. Inter-unit common cause failures are possible and it is assumed that they are only capable of generating an order 4 component failure. The associated probability Q4 it taken to be equal to 2 E-07, i.e. around 1% of the probability of both SI system components experiencing a common cause failure at a given unit.
- The standardised system SB comprises three components B_k in redundancy mode at each of the units. The failure probability of each component γ_B is equal to 1 E-03. Intra-unit common cause failures may affect this system's components; the corresponding alpha factors α_2 and α_3 are equal to 1 E-02 and 1 E-03 respectively. Inter-unit common cause failures are possible and an order 6 common cause failure group for the system components at the two units is modelled with the following parameters: $\alpha2 = 1$ E-02, $\alpha3 = 1$ E-03 and $\alpha4 = 1.8$ E-4. It is also assumed that for each of the units, the requirement with regard to this system depends on the operating modes of the unit. During power operation, i.e. 80% of the time, the unit requires one out of three components to operate; during outage, i.e. 20% of the time, the unit requires two out of three components to operate.

For the purpose of illustration of the proposed methodological options, a reference unit PSA model and a site model PSA are developed.

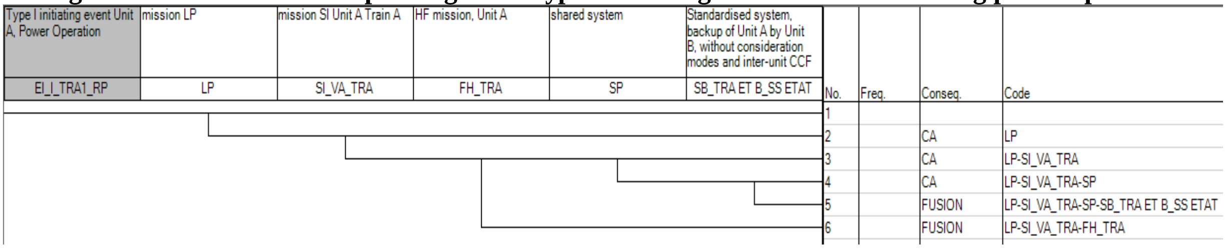
- **Case 1: Reference unit PSA model**

A reference unit PSA model is developed to correspond to the current practice. Consequently, only unit A is considered. The mutual backup of Unit A by Unit B by the standardised system S_B is assessed, without taking inter-unit common cause failure or the respective operating modes of the two units into account (Unit B is assumed to be in the most favourable mode, i.e. power operation). The identical systems are modelled without considering inter-unit common cause failures given the initiating type II. The shared system is considered to remain available for Unit A, as are the human resources needed to operate it. The event trees corresponding to the type I initiating event and the type II initiating event for unit A (the same for unit B) during power operation and outage are shown in figures 10, 11, 12 and 13. The HEP mission FH_TRA is represented by the basic event FH_TRA with a probability 1 E-01.


type I Initiating event, Unit A, Outage mode
mission LP
mission SI Unit A Train A
Standardised system, backup of Unit A by Unit B, without consideration modes and inter-unit CCF
EI_I_TRA1_AR
LP
SI_VA_TRA
SB_A ET B_A EN AR

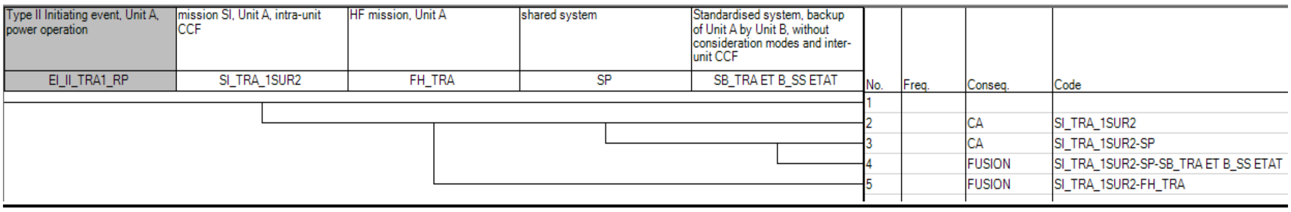
No.	Freq.	Conseq.	Code
1			
2		CA	LP
3		CA	LP-SI_VA_TRA
4		FUSION	LP-SI_VA_TRA-SB_A ET B_A EN AR

Figure 10: Event tree corresponding to the type I initiating event for Unit A during power operation


Type I initiating event Unit A, Power Operation
mission LP
mission SI Unit A Train A
HF mission, Unit A
shared system
Standardised system, backup of Unit A by Unit B, without consideration modes and inter-unit CCF
EI_I_TRA1_RP
LP
SI_VA_TRA
FH_TRA
SP
SB_TRA ET B_SS ETAT

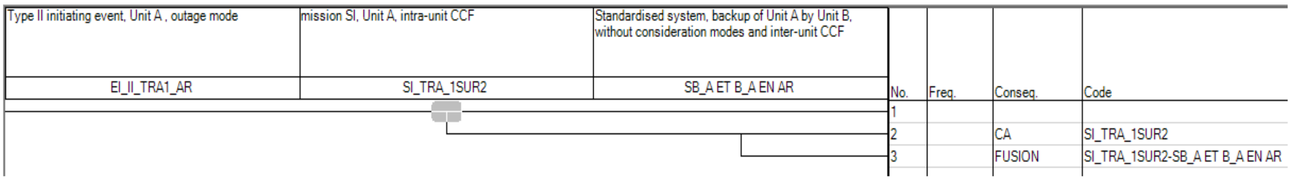
No.	Freq.	Conseq.	Code
1			
2		CA	LP
3		CA	LP-SI_VA_TRA
4		CA	LP-SI_VA_TRA-SP
5		FUSION	LP-SI_VA_TRA-SP-SB_TRA ET B_SS ETAT
6		FUSION	LP-SI_VA_TRA-FH_TRA

Figure 11: Event tree corresponding to the type I initiating event for Unit A during outage


Type II Initiating event, Unit A, power operation
mission SI, Unit A, intra-unit CCF
HF mission, Unit A
shared system
Standardised system, backup of Unit A by Unit B, without consideration modes and inter-unit CCF
EI_II_TRA1_RP
SI_TRA_1SUR2
FH_TRA
SP
SB_TRA ET B_SS ETAT

No.	Freq.	Conseq.	Code
1			
2		CA	SI_TRA_1SUR2
3		CA	SI_TRA_1SUR2-SP
4		FUSION	SI_TRA_1SUR2-SP-SB_TRA ET B_SS ETAT
5		FUSION	SI_TRA_1SUR2-FH_TRA

Figure 12: Event tree corresponding to the type II initiating event for Unit A during power operation


Type II initiating event, Unit A , outage mode
mission SI, Unit A, intra-unit CCF
Standardised system, backup of Unit A by Unit B, without consideration modes and inter-unit CCF
EI_II_TRA1_AR
SI_TRA_1SUR2
SB_A ET B_A EN AR

No.	Freq.	Conseq.	Code
1			
2		CA	SI_TRA_1SUR2
3		FUSION	SI_TRA_1SUR2-SB_A ET B_A EN AR

Figure 13: Event tree corresponding to the type II initiating event for Unit A during outage

The risk obtained by this model is equal to 1.67 E-10.

- **Case 2: Upgraded unit PSA model**

A PSA model at site level is obtained by developing two upgraded PSA model for both unit (A and B). Each model is based on the reference unit PSA model with the consideration of the dependencies existing between two units:

- In comparison with the previous case, this model incorporates the fact that for the type II initiating event, the shared system may already be connected to a unit when the other needs it. Similarly, the model includes the fact that the team using this shared system is a site team and that consequently, in this case, the mission's failure probability is penalised. The HEP mission FH_TRA_PENALISE is represented by the basic event FH_TRA_PENALISE with a probability of 2 E-01. A penalty factor of 2 has been applied to the reference value (1 E-01).

- A basic event represents the probability of the shared system being available and not being available for Unit A is introduced. This probability corresponds to the inclusion of the fact that when Unit A requires the use of the shared system SP, this may have already been taken by Unit B, experiencing the same initiating event.

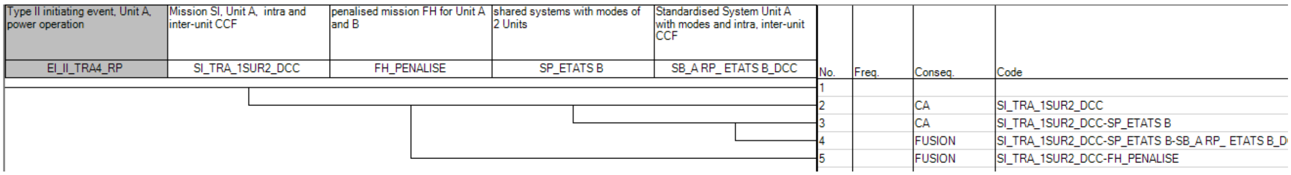
- In this model, the operating mode of the twin unit is also modelled for both types of initiating events. As the shared system cannot be assessed for a unit during outage, when Unit B experiences an outage, the system becomes fully available again for Unit A in power operation. As far as the standardised system is concerned, if Unit B is experiencing an outage, it will need two of the three components of its SB system. Consequently, only one of Unit B's three components will remain available to back up Unit A.

- The inter-unit common cause failures are also taken into account. Two systems are involved: the identical systems and the standardised systems. For the identical systems, given the type II initiating event, only the order 2 intra-unit CCF and the order 4 inter-unit CCF are considered to be possible, to the exclusion of any other combination of failures. For the standardised systems, due to the physical connection between the two systems, a common cause failure group of the size 2n is modeled (where n is the number of components in a system) for both types initiating events. Here, an order 6 common cause failure group has therefore been defined, which replaces the order 3 common cause failure groups initially defined.

When implementing two upgraded PSA models for 2 units in a PSA software, e.g Riskspectrum, some precautions need to be taken:

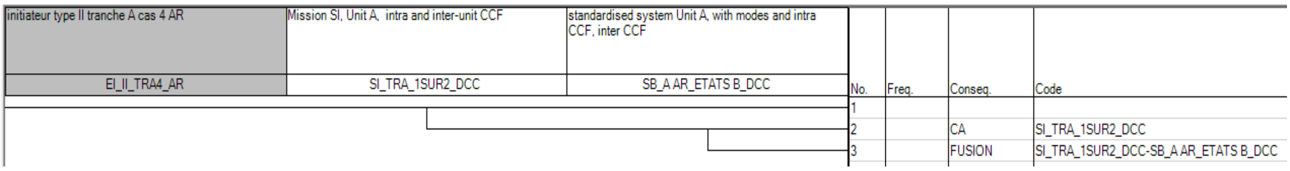
- The type I initiating events need to be named differently for two units, to ensure that the result of the site level calculation would be an "exclusive OR" for the accident sequences for these units.
- Conversely, the type II initiating events were given identical names for the two units.
- The EBs for the identical systems and the standardised systems were also differentiated for the two units. However, the systems and human resources shared by the two systems were modelled by the same EBs for the two units.

The event trees corresponding to the type II initiating event for unit A (the same for unit B) during power operation and outage are shown in figures 14, 15.


Type II initiating event, Unit A, power operation
EI_II_TRA4_RP
Mission SI, Unit A, intra and inter-unit CCF
SI_TRA_1SUR2_DCC
penalised mission FH for Unit A and B
FH_PENALISE
shared systems with modes of 2 Units
SP_ETATS B
Standardised System Unit A with modes and intra, inter-unit CCF
SB_A RP_ ETATS B_DCC

No.	Freq.	Conseq.	Code
1			
2		CA	SI_TRA_1SUR2_DCC
3		CA	SI_TRA_1SUR2_DCC-SP_ETATS B
4		FUSION	SI_TRA_1SUR2_DCC-SP_ETATS B-SB_A RP_ ETATS B_D
5		FUSION	SI_TRA_1SUR2_DCC-FH_PENALISE

Figure 14: Event tree corresponding to the type II initiating event for Unit A during power operation


initiateur type II tranche A cas 4 AR
EI_II_TRA4_AR
Mission SI, Unit A, intra and inter-unit CCF
SI_TRA_1SUR2_DCC
standardised system Unit A, with modes and intra CCF, inter CCF
SB_A AR_ETATS B_DCC

No.	Freq.	Conseq.	Code
1			
2		CA	SI_TRA_1SUR2_DCC
3		FUSION	SI_TRA_1SUR2_DCC-SB_A AR_ETATS B_DCC

Figure 15: Event tree corresponding to the type II initiating event for Unit A during outage

The risk obtained for the upgraded unit PSA model of each unit is equal to 3.33E-10.

4.2 Results

The table 1 below summarized the risk at unit level and the corresponding risk at site level obtained by multiplying simply the risk at unit level by 2.

Table 1 Risk at unit level and the corresponding risk at site level

	Unit level risk	Site level risk
Case 1: Reference PSA model	1.67 E-10	3.33 E-10
Case 2: Upgraded PSA model	3.33 E-10	6.66 E-10

As can be seen, at the unit level, the reference model underestimates the risk (1.67 E-10) compared to the risk of the upgraded unit PSA model (3.33 E-10). This difference results from the impact of the consideration of the dependencies existing between both units. In this example, we realized that the dependency factor between the units that has a principal impact on the risk is the inclusion of a shared site team, whereby the HF is penalised. The other dependencies (respective operating modes of the units and inter-unit common cause failures) have no visible impact, bearing in mind the fact that they concern the systems whose failure does not lead directly to core meltdown.

At site level, compared to the upgraded model, the reference model underestimates the site level risk by a factor of 2. In the case 2, a more realistic risk at site level can be obtained, according to formula (1), by using the calculation of P(A∪B)) directly in Riskspectrum software. In this case, the obtained risk is 6.63E-10 which is lower than that obtained by multiplying the risk for upgraded unit A model only by 2 (6.66 E-10). The difference is due to the minimization of the MCS shared by both units.

The risk associated with the simultaneous meltdown of both units (P(A∩B)) can be calculated as follows: 2P(A)–P(A∪B)= 3.2E-12. This corresponds to the common MCS which can be interpreted as the occurrence of the type II initiating event at both units, followed by the loss of the identical system due to inter-unit common cause failure, and the shared site team's failure to put the shared system into operation.

5 CONCLUSION AND PERSPECTIVE

The paper has presented some possible solutions or methodological options in order to switch from a level 1 unit PSA model to a model for the site to take into account the multi-unit dependencies. A study case was used to illustrate the proposed methodology. However, additional developments must be provided to cover the level 2 PSA, particularly its implementation in RiskSpectrum, as well as level 3. Even when multi-unit aspects are taken into account in a level 1 PSA, some methodological problems arise which will need to be the focus of further developmental work:

- Suggest a selection criterion for the systems that definitely need to be modelled, retaining the multi-unit aspects (operating mode of the twin unit, inter-unit common cause failures).
- Suggest a less conservative modelling of the shares site resources.
- Suggest a precise method for establishing the inter-unit common cause failure parameters, based on the feedback available or existing parameters.
- Suggest a precise method for post-processing the MCS from the level 1 PSA, to identify the scenarios that will form the type II initiating events (simultaneous meltdown of both units) for the development of the level 2 and level 3 PSA.
- Suggest a method for dealing with potential situations in which, following a type II initiating event, one unit is already experiencing a severe accident and the other is not.

All of these developmental aspects are currently studied in our on-going projects at EDF R&D.

References

[1] H-T51-2013-00462-FR -Etat de l'art de la prise en compte des aspects multi tranche dans les Etudes Probabilistes de Sûreté, EDF R&D Technical report.

[2] Karl N. Fleming, “*On The Issue of Integrated Risk– A PRA Practitioners Perspective*”,– Proceedings du PSA05 San Francisco.

[3] Seabrook Station Probabilistic Safety Assessment – Summary reports & Volumes 1 to 6 – Décembre 1983.

[4] Schroer S and M Mohammad, “*An Event Classification Schema for Evaluating Site Risk in a Multi Units NPP PRA*”, Reliability Engineering and system safety117 (2013)10-51.

[5] Gallois M., Luzoir C., Dutfoy A, Vasseur D and Bordes D. *Development of a method for the screening of natural hazards at EDF*, ANS PSA 2013 International Topical Meeting on Probabilistic Safety Assessment and Analysis Columbia, SC, September 22-26, 2013, American Nuclear Society, LaGrange Park, IL (2013).