

## Adapt the level of detail of the reliability studies for mastering constraints of a nuclear project

Hervé BRUNELIERE<sup>1</sup>, Monica RATH<sup>1</sup>, Cécile LE MONTAGNER<sup>1</sup>, Pierre LACAILLE<sup>1</sup>

<sup>1</sup> AREVA NP - Tour AREVA, 1 place Jean Millier 92084 Paris La Défense cedex, France, herve.bruneliere@areva.com

**Objectives:** The communication presents the example of a typical nuclear reactor project for which it is necessary, in a fixed timeframe, to supply probabilistic evaluations, for the whole nuclear reactor (i.e. plant PSA) and also, individually, for each of the safety-related systems ("specific" reliability studies).

Communication addresses what is done during the various stages of the project, the encountered difficulties and the consequential strategic choices selected to improve the final results. The safety-related systems addressed in the communication are I&C systems. The methodological elements of experience feedback which were extracted from this process are also given.

The communication sheds light on the difficulty to take into account new constraints within the framework of a project.

**Methods:** The modelling in PSA is in accordance with the one described in [1] for the detailed design phase. More details are supplied in the communication.

The "specific" reliability studies are initially conducted with the same simplified and conservative model as PSA, which mutualizes the efforts. This, sometimes called "super-component" approach, models in the same event all the failures of an I&C unit which can impact at least a studied function. It presents the benefit, within the framework of PSA, to handle all dependencies.

The first calculations show:

- for PSA, a sufficiently low contribution of I&C with regard to the global probabilistic safety objectives (i.e. Core Damage Frequency),

- for the specific reliability studies, a significant deviation of the results with regard to expected quantitative unreliability.

To refine the results of the specific reliability studies, an analysis of the major contributors for every function is made. The conservatism associated to these contributors are identified. Main ones are:

- Detection means of the failures of sensors in the study

- Numbers of inputs / outputs taken by unit based on the worst studied function

Consequently and in a second time, for a better precision of the calculations, the general model was transformed into individual models for every studied function.

For each of these functions, main following improvements are realized:

- The detection means of the sensors failures are identified sensor per sensor. It allows the identification of sensors for which there is a redundant sensor supplying exactly the same value at the same time and on which the discrepancy processing can thus be valued in the calculation.

- The number of inputs by function is considered.

**Results:** The individual models realized are more precise on the important contributors but remain less precise than comprehensive studies which would precisely detail all the contributors. However, the quantitative result of the individual models is then rather close to the one of detailed studies and is sufficient for the application.

**Conclusions:** This example is representative of our capacity to adapt the risk studies to the needs in the frame of a project. This includes starting from simplified calculations to avoid systematically performing detailed studies that can be long and costly.

## I. INTRODUCTION

This article presents the example of a typical nuclear reactor project for which it is necessary, in a defined timeframe, to supply various probabilistic evaluations, for the whole nuclear reactor and for each of the safety-related systems in an individual way. The systems addressed here are I&C systems.

Objective of this article is to give a perspective on the difficulty for taking into account new constraints during project execution. The need to consider these constraints appearing in the initiation phase or during execution is explained.

A number of teachings can be concluded from these studies. They are described at the end of the article.

## II. GENERAL METHODOLOGICAL CONTEXT

I&C systems have a major importance in the design of nuclear power plants through their safe and reliable operation.

In Probabilistic Safety Analyses (PSA) of a nuclear reactor, the way I&C is integrated and modelled is a key point for the designer. It allows making sure of the respect for the global safety probabilistic objectives with a good confidence and a sufficient margin to warrantee that these objectives are met during all the life cycle of the plant. This problematic was detailed in particular in [1].

This importance also justifies that specific studies are made, as a complement to PSA. They respond to the interest to estimate the individual reliability of each I&C system at different steps of the project (including early phases). For certain systems, a maximum quantitative objective of failure probability on demand is contractually required.

These studies have traditionally a level of detail and precision more important than the modelling made in the PSA for which high level of detail is not systematically applied. These specific studies also aim at identifying the major contributors of the unreliability and at making sure that the design of every system is balanced, i.e. there are no contributors which are widely dominating with regard to the others.

## III. SPECIFIC CONTEXT

The typical approach presented here applies for a case where both types of activities, PSA and specific studies, must be realized in parallel within the same entity. A synergy between these two studies is wished to optimize the schedule and the resource management.

Sufficiently high level of detail of the analysis and of the results is a major objective in both approaches.

## IV. METHOD

Selected modelling is in accordance with the one described in [1] for the detailed design phase. To address the objective of high level of detail, a said "super-component" approach is introduced there.

This modelling is described below.

### IV.A. "Super-component" approach principle

Sub-fault trees are built, they model the logical units, i.e. a set of components for which the functional consequences of the failures and the dependencies to support systems are identical. An OR gate between the relevant failure modes of these components is elaborated.

Two sub-trees are modelled for every logical unit: one models the failure of the unit because of detected failures, and the second one models the failure of the unit because of undetected failures.

These sub-trees are not directly connected to the main fault trees. However they are used to produce reliability data injected in the basic events of these main fault trees. These basic events are called "super-components".

In practice, these sub-fault trees are developed first which allows calculating failure probabilities.

The so called "super-components" basic events are created in the main PSA model. They have for failure probability the one of the sub-tree which corresponds to them, this probability being manually assigned to "super-components".

Every logical unit is made by several components or modules. A given I&C function can require the use of several or all the modules included in a unit. Furthermore, some modules manage several channels with a distribution of the failure rate between the common part (board), where a failure would result in the failure of the whole module, and the channel part. An I&C function can require one or several channels of a given module. The following figure presents the typical structure of an I&C module: this is only an example.

Some modules have no channels. Others only have failures impacting a single channel, the module having then been designed so that channels are fully independent.

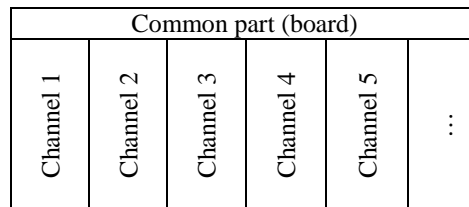


Fig. 1. Typical structure of an I&C module

The failure probability of a given module P (module i) is calculated with the following formula:

$$P(\text{module } i) = P(\text{module } i \text{ detected}) + P(\text{module } i \text{ undetected}) \quad (1)$$

$$P(\text{module } i) = \lambda(\text{module } i \text{ common board detected}) * MTTR(\text{module } i) + k * \lambda(\text{channel module } i \text{ detected}) * MTTR(\text{module } i) + \lambda(\text{module } i \text{ common board undetected}) * T_i(\text{module } i)/2 + k * \lambda(\text{module } i \text{ channel undetected}) * T_i(\text{module } i)/2 \quad (1')$$

Where:

- i = type of module
- P (module i detected) = probability of detected failure of module i
- P (module i undetected) = probability of undetected failure of module i
- MTTR = average duration of detection + repair + reconfiguration and restart
- T<sub>i</sub> = test interval
- k = maximum number of channels of the module used by a function (assuming that failure rates are given by channel).

A FMEA performed by the designer of the system, with the support of the supplier of the components, gives the failure rates that are necessary for the calculations, for all the failure modes of every module i:

- The failure rate associated with a detected failure of the common part of the module
- The failure rate associated with a detected failure of a channel of the module
- The failure rate associated with an undetected failure of the common part of the module
- The failure rate associated with an undetected failure of a channel of the module

In every unit and for each type of module, numbers of modules and of used channels are considered. The "worst" function is considered, i.e. the one which uses the highest number of modules and of inputs/outputs. This analysis is made on the basis of tables presented in the FMEA. These tables indicate, for every function:

- The various types and the numbers of modules used for the processing of the function,
- The number of channels used by every module for the processing of the function.

#### IV.B. Interest of "super-component" approach

The "super-component" approach presents the big advantage to be at the same time a modelling at the unit level and a modelling at the module level.

The same model indeed contains all the failure modes of all the modules, which allows tracing all the failures at this very fine level.

In parallel, failures of units are the ones that are in the minimum cutsets issued from the PSA software. It makes easier the analysis of the scenarios where I&C is playing a dominating role.

Then when it is identified that a failure of unit has a strong impact on the result, it is possible to analyze the contents of corresponding sub-tree to identify the failure modes of the modules which have the strongest impact.

This analysis in two steps with progressive levels of detail brings a very high added value for continuous reliability improvement during the design of the systems.

#### IV.C. I&C systems

I&C systems implement several functions. Each of them is represented by a specific fault tree and sub-trees. Some sub-trees can be common to several functions.

Every function consists of two main parts:

- The instrumentation part,
- The processing part.

The instrumentation part corresponds to sensors and to their connected conditioning modules (electronic converters and transmission couplers).

Figure 2 presents a general overview of the instrumentation part, including sensors and their conditioning. The conditioning is made by combinations of modules.

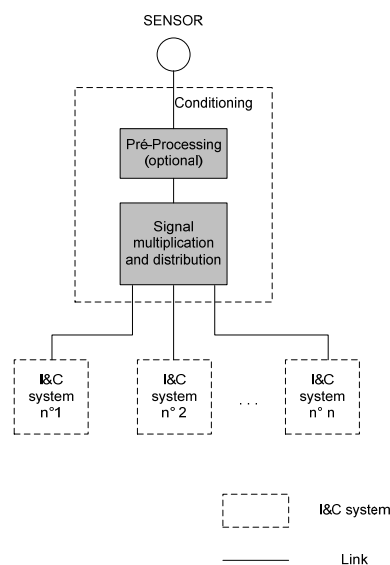


Fig. 2. General presentation of instrumentation part

Processing part corresponds to processing functions implemented in I&C systems from level 1 (automation systems). These functions receive and process (calculations, thresholds, voting logics) signals from instrumentation part.

For a given I&C function, the processing part modelled in the PSA includes:

- A specific part for every individual function which models the units which are particularly used by the concerned function and the combinations of failures of these units.
- A part which is common to all the functions processed in the same I&C platform and which represents particularly the common cause failures which can be introduced by the use of the same platform.

#### IV.D. Instrumentation part modelling

Sensors used for the elaboration of every signal are individually modelled with the following failure modes: failure to a low value, failure to a high value, erroneous value in the range, frozen in the current value when the failure occurred.

In complement for every sensor, all the failures not detected immediately of one of the conditioning modules are handled in one sub-tree which supplies failure probabilities to the super-components.

Same principle applies for all the failures detected immediately of conditioning modules of every sensor.

When redundant sensors are used for the elaboration of a signal, a logic gate is modelled in the PSA to model the failure criterion. The following table shows some examples:

TABLE I. Voting logics and Logical gates

Voting logic	Sensors numbers	PSA logical gate (failure criterion)
2/4	4 sensors	$\geq 3$
2/3	3 sensors	$\geq 2$
2/2	2 sensors	OR
1/2	2 sensors	AND
1/1	1 sensor	OR

In a conservative way, the degradation of the voting logic is not modelled. This is done for a simplification purpose and because the experience of AREVA NP shows that the conservatism is finally negligible.

Unavailability values are calculated. They base themselves on:

- Hourly failure rates of equipment
- Efficiency of the components internal self-tests or of external means of surveillance, as well as mean duration of detection of self-tests and other means.
- Time interval between periodic tests.
- Mean duration for detection + repair + reconfiguration and restart of the component.

Common Cause Failures (CCF) are considered for redundant sensors. For the conditioning modules, an evaluation of the complexity is made on an individual basis.

It should be noted that the software used for the modelling cannot always model all the intermediate combinations in case of CCF groups including more than four components. To compensate this, directly redundant sensors are often put in a CCF group, and events handling wider CCF scenarios on sensors are introduced as a complement.

For example, for modelling a CCF of 16 redundant sensors, shared in 4 sensors by train, as it can be the case for steam generator level sensors, the chosen solution is the following one:

- 4 CCF groups of 4 sensors (one group by train),
- 1 event of "CCF event" type modelling the failures of the 16 redundant sensors.

#### IV.E. Processing part modelling

"Super-components" are at the processing unit level. For every unit, an event of "undetected failure" type and an event of "detected failure" type are created and connected to the models.

The failure probabilities of every unit are determined by calculating the probability of sub-trees. Sub-trees contain the failure modes of the following components:

- Subracks,
- Processing modules,
- Input modules,
- Output modules,
- Communication modules.

Reliability data used in entry are:

- Reliability data (failure rates), estimated in detail by the supplier of the I&C system (module per module, failure mode per failure mode).
- Frequencies of periodic tests
- Times of detection + repair + reconfiguration and restart.

CCF are taken into account between the units which execute redundant processing.

Besides, a CCF is taken between all the units based on the same I&C platform. This CCF considers that from its occurrence, no function implemented in a system using this platform could be anymore executed due to common cause hardware failures.

Specific case of software failures is addressed in IV.F.

#### IV.F. Accounting of software failures

Basic events of type "complete failure of the system due to the software" are modelled. They take into account in particular failures due to temporal effects or to communication defects. They consider the fall-back position of the system when this type of defect appears. The way these rare defects probability can be estimated is handled in [2].

#### **IV.G. Accounting of support systems**

Every component (sensor, unit) is connected to its support systems (power supply, ventilation). This is made by OR gates between the super-components and the transfers towards support systems fault trees.

These support systems fault trees model failure modes of elements ensuring the power supply and ventilation of the I&C components.

This modelling is possible due to the way logical units were previously defined.

#### **V. RESULTS REFINEMENT**

The first calculations generally show:

- For PSA, a sufficiently weak contribution of I&C systems towards the respect for the global safety probabilistic objectives.

- For the specific reliability studies, a significant increase of the results with regards to the unexpected reliability, especially in the first iteration.

To refine the results of the specific reliability studies, an analysis of the major contributors for every function is made. The conservatisms linked to these contributors are identified. Among the main identified conservatisms appear:

- The number of inputs/outputs per unit based on the "worst" studied function.

- The uniform processing of the valuations of the detection means for the failures of sensors in the study.

These conservatisms can be handled in both studies. Nevertheless it is generally recommended to address them in priority for specific reliability studies because of the significant increase of the results with regards to the unexpected reliability

The continuation of the article enters more in detail in the management of these two conservatisms:

#### **V.A. Switch from a generic model to specific models**

For a part of the functions in a given system, the number of inputs/outputs used by module is important. The fact of using the same model for all the functions of the system implies, by application of the methodology, to size the number of inputs/outputs with regard to these functions.

The reliability of all the functions is thus degraded by the number of inputs/outputs on these few functions.

It is penalizing as these few functions are not necessarily the most important of the system in terms of safety classification. Additionally, in projects where this is applicable, they have less stringent reliability targets.

Contrarily to the PSA the specific reliability studies are not addressing dependencies between functions. Consequently, it is acceptable for these studies (which is not the case for the PSA) to have all the functions in the same model.

A model by function can thus be created.

In this model:

1) For every unit, the composition retained in sub-trees consists in the exact number of modules and channels used for the function of the model.

2) The formula for the failure probability of a module P (module i) becomes:

$$P(\text{module } i) = P(\text{module } i \text{ detected}) + P(\text{module } i \text{ undetected}) \quad (2)$$

$$P(\text{module } i) = \lambda(\text{module } i \text{ common board detected}) * MTTR(\text{module } i) + n * \lambda(\text{channel module } i \text{ detected}) * MTTR(\text{module } i) + \lambda(\text{module } i \text{ common board undetected}) * Ti(\text{module } i)/2 + n * \lambda(\text{module } i \text{ channel undetected}) * Ti(\text{module } i)/2 \quad (2')$$

Where:

- i = type of module

- P (module i detected) = probability of detected failure of module i

- P (module i undetected) = probability of undetected failure of module i

- MTTR = average duration of detection + repair + reconfiguration and restart
- Ti = test interval
- n = number of channels of the module used by the function of the model.

#### **V.B. Optimization of modeling of sensors failures detection**

This optimization consists in identifying the means for detection of sensors failures, sensor by sensor, instead of doing it with a general logic that would be conservative for all sensors.

Concretely, it consists in identifying the sensors for which there is a redundant sensor supplying exactly the same value at the same moment. For these sensors, it is authorized to take credit of the discrepancy processing in the calculation. The failure mode "erroneous value in the range" is therefore detected by a discrepancy alarm.

These sensors basically represent more than 90 % of the sensors for a typical protection system.

In addition, for other sensors, if the parameter is a parameter which evolves frequently in normal (or non-accidental) operating conditions, the failure mode "frozen in the current value at the failure occurrence can also be detected earlier than next periodic test.

This finer analysis allows limiting the contribution of sensors, but also of the conditioning modules, to the final result.

#### **V.C. Reliability gain**

For some projects, the implementation of these two major improvements allowed a reliability gain in the order of magnitude of 10 to 50 for the most critical functions.

### **VI. TEACHINGS**

The individual models are more precise on the important contributors but remain less precise than studies which would detail all the contributors. However, the quantitative result of the individual models is then rather close to the one of the detailed studies.

A number of wider teachings can be derived from these studies. These teachings are considered by the authors as applicable in other industry sectors. The three main teachings are:

#### **VI.A. Project risk management due to schedule**

As already mentioned, the followed approach is less straight forward than the one usually used for the specific I&C reliability studies. It presents a gain on the schedule, as long as all the actors of the project agree on the process.

However, it is possible that, as mentioned in this article, the first iteration is not considered satisfactory. Then, a second iteration, to decrease the conservatisms of the first one, is relevant and, even more if necessary.

It is thus advisable to take into account this risk by leaving enough time in the schedule of the project between foreseen date for the first iteration and the deadline for the finalization of the document.

#### **VI.B. Need for feedback and expertise**

It is recommended to balance the conservative assumptions in the trust which we can have on their relevance and on the fact that they will have reasonable impact on final results.

Concretely, it is essential that the author owns, by himself or by another person that he will have the possibility to refer frequently, a high knowledge and expertise on the following points:

- the type of architecture,
- the technology of the used components
- the classic methods for this type of studies.

This big knowledge can be acquired only by an experience feedback consecutive to the performance of a sufficient number of studies of the same type realized on similar systems and on which the author can capitalize to define relevant assumptions and conservatisms for ongoing study.

This knowledge is also essential to have the capacity to identify quickly the improvements to be made from the first calculations.

Should the opposite occur, the risk would be important to finish with a high number of iterations. If these conditions are not filled, it is recommended to keep a more classical approach.

#### **VI.C. Relevance of the modelling towards sensitivity studies**

The calculations using super-components involve a certain number of assumptions. The use of these models for sensitivity studies thus has to be the subject of a particular attention.

Nevertheless, if modeling of support systems was made sufficiently precisely, sensitivity calculations on the parameters (probability, failure rate) remain relevant as long as the architecture is not modified.

#### **VII. CONCLUSIONS**

This article presents an example of studies optimized to answer stakes in tasks organization, in synergies, in schedule and in management of resources.

This type of studies presents a certain level of risk. Recommendations are thus uttered both in term of schedule and use of sufficiently experienced skills to ensure the success.

This communication is representative of challenges to come for this type of studies who, in order to answer constraints inherent to the project, must be adaptable in the course of project while keeping their relevance and the level of quality assurance relative to the nuclear domain.

#### **REFERENCES**

1. H. BRUNELIERE, C. LEROY, L. MICHAUD, N SABRI and P.OTTO, “Finding the best approach for I&C modeling in the PSA in the different design phases”, *PSAM11/ESREL 2012*, Helsinki (Finland), June 2012.
2. O. BÄCKSTROM, J-E. HOLMBERG, M. JOCKENHÖVEL-BARTTFELD, M. PORTHIN, A. TAURINES and T. TYRVÄINEN, “Software reliability analysis for PSA: Failure Mode and Data”, Nordic nuclear safety research (NKS) Report, NKS-341 (2015)