Safety Assessments of Nuclear Power Plants I&C Systems Architecture

Hervé Brunelière[a](*), Pierre Lacaille[a], Jean-Yves Brandelet[a], and Mariana Jockenhoevel-Barttfeld[b]

[a] Framatome, Paris La Défense, France
[b] Framatome, Erlangen, Germany

Abstract: Because of their role in fulfilling the majority of active safety actions, Instrumentation & Control (I&C) systems are of major importance in the design of nuclear power plants and in particular their safe and reliable operation. This implies that many safety analyses linked to I&C designs need to be performed in order to fulfill the probabilistic and deterministic safety requirements and safety targets that apply to the whole nuclear power plant. In the first step of the assessment, these requirements and targets are applied to the overall I&C architecture. In a second step, some of these are transferred to the architecture of each safety classified I&C system and to the hardware structure of all safety categorized functions. Framatome works on various projects where these kinds of analyses are needed. This includes new build projects, for example, EPR projects, and modernization of I&C systems of existing nuclear power plants so that digital I&C and Long Term Operation (LTO) can be introduced, and obsolete technologies can be replaced. The experience gained by Framatome generated feedback on these studies or the implementation of their conclusions in the design. This feedback provided knowledge which can be used to develop a more efficient process.

Keywords: I&C, safety studies, CCF, independence, defense in depth.

1. INTRODUCTION

Because of their role in fulfilling the majority of active safety actions, Instrumentation & Control (I&C) systems are of major importance in the design of nuclear power plants and in particular their safe and reliable operation.

As part of the digital transformation, the progressive switch from analog I&C to digital I&C for the nuclear power plants is a major event. It is an improvement opportunity because it:

- Allows the I&C systems to be maintained more easily,
- Makes the implementation of modifications during the whole plant lifetime easier, and
- Allows the use of more ergonomic human-machine interfaces with great human reliability advantages.

However, additional questions linked to the digitalization of the safety function processing, to the software development and implementation, and to the processing of functions (that were previously well separated) in the same logic units, are raised and need to be included in the safety approach.

This implies that many safety analyses linked to I&C designs need to be performed in order to fulfill the probabilistic and deterministic safety requirements and safety targets that apply to the whole nuclear power plant.

In the first step of this assessment, these requirements and targets are applied to the overall I&C architecture. In the second step, some of these are transferred to the architecture of each safety classified I&C system and to the hardware structure of all safety categorized functions.

* herve.bruneliere@framatome.com

2. **CONTEXT**

Framatome works on various projects where these kinds of analyses are needed. This includes new build projects, for example EPR projects, and modernization of I&C systems of existing nuclear power plants so that digital I&C and Long Term Operation (LTO) can be introduced, and obsolete technologies can be replaced.

3. **METHODS**

Framatome has a great experience in performing analyses that cover:

- Justification of defense in depth;
- Justification of safety classification;
- Failure Modes and Effects Analyses (FMEAs) / Justification of single failure criterion;
- Independence analyses;
- Common Cause Failures (CCF) analyses;
- Robustness of I&C architectures with regards to internal hazards;
- Reliability and availability analyses;
- Inclusion of I&C in Probabilistic Safety Assessment (PSA).

From performing these studies or the implementation of their conclusions in the design, useful feedback was obtained. This feedback provided knowledge which can be used to develop a more efficient process. This results in:

- Better quality;
- Optimized schedule. Because of the safety stakes that are addressed, these studies shall cover a very large scope and demonstrate exhaustiveness. After completing the studies, the major challenge is the ability to mutualize them without missing some safety insights;
- Better interface with I&C designers. It is very important to be able to give relevant recommendations to the designers during all design stages, in order to ensure that safety requirements and targets will be met with high confidence, and an adequate level of margin will exist throughout the life cycle of the plant.

3.1. Justification of defense in depth

The I&C functions are needed to operate the plant during normal plant conditions, to fulfill plant safety objectives, provide automatic control and protection functions, and provide operators with information and control capabilities to:

- Detect failures and control anticipated operational occurrences,
- Control design basis accidents within the design basis, and
- Control and mitigate design extension conditions with or without significant core degradation.

These functions shall be assigned to I&C systems in order to make the implementation of the successive Defense in Depth levels possible and effective. These five levels of defense are defined by the IAEA Safety Guide [1].

Level 1 I&C functions aim to prevent deviations from normal operation by keeping the plant parameters within the expected range.

Level 2 I&C functions aim to detect and control deviations from normal operation, in order to prevent anticipated operational occurrences from escalating to accident conditions.

Level 3 I&C functions aim to actuate engineered safety features or design features which were implemented to prevent core/fuel degradation accidents and limit radiological releases. This includes:

- All mitigating functions required to control the Design Basis Conditions and to operate the plant until it is in a controlled state, and then until it is in the safe shutdown state (these functions are named level 3a functions);
- All the functions necessary to prevent a core degradation accident (also called a design extended condition with core degradation) and to operate the plant until it has reached a safe and stable state in case of a complex sequence called “design extended condition without core degradation”, whose frequency is so high that it has to be considered in the design (these functions are named level 3b functions). This includes all the I&C functions identified as a necessary back up of level 3a I&C functions in case these functions fail on demand following a Design Basis Condition.

Level 4 I&C functions aim to mitigate the radiological consequences of core fuel degradation accidents so that only limited protective measures of area and time are needed for the public safety, and that there is sufficient time to implement these measures.

Level 5 I&C functions address the protection of people and environment in case of accident with radiological releases. They are supported by an emergency control centre for on-site and off-site emergency responses, with radiological monitoring and data communication to the emergency centre.

The justification of defense in depth has to prove that this concept has been well implemented in the overall I&C architecture.

The justification of defense in depth initially explains how this concept is derived for the considered nuclear power plant. This covers the list of I&C systems dedicated to a specific defense in depth level and those that are shared between defense in depth levels.

The logic for the application of defense in depth at I&C level has to be consistent with the one at plant level. It should, for example, take into consideration the way we want to achieve the independence between two given successive levels.

Secondly, it verifies, one initiating event at a time, whether sufficiently independent successive I&C functions involved in mitigation exist. This can be achieved by implementing the I&C functions in different systems. However, they can also be in the same system if some specific measures, which allow the necessary independence in one system, are implemented.

The main input is the plant application of the defense in depth concept. Then, in order to perform the analysis per initiating event, the list of these events (including design basis conditions and design extended functions), as well as all the I&C functions, are needed. For each I&C function, its role in the safety demonstration, the system where it is implemented and, on a case by case basis, some other details about its design, have to be known.

It should be mentioned that the person or team involved in their delivery has to have good knowledge and understanding of the design of the overall I&C architecture and of the different I&C systems, in order that the concept is well applied. If this has been done correctly, the justification is facilitated.

3.2. Justification of safety classification

I&C functions are categorized based on their safety significance. The safety significance is determined by assessing the following factors:

a) The consequence of failing to deliver the safety function;
b) The probability that the function will be demanded;

c) The time at and up to which the function is required, either directly or indirectly, to prevent, protect against or mitigate the consequences of the initiating event.

Taking these three factors into account, the safety significance of every I&C function is established and categorized into three categories C1, C2 and C3, the highest category C1 is dedicated to functions having the highest safety significance.

Once the categorization of the functions is completed, a safety class is assigned to every individual system/equipment, according to its individual safety significance.

A categorization of the functions, then a classification of individual components is performed to ensure that every function is designed and operated with a quality commensurate with its safety significance.

As a general principle, the safety class assigned to an individual Structure, System or Component (SSC) corresponds to the highest safety category level of the function it implements, and therefore, the individual component classification is based on three classes (safety classes 1, 2, 3) for safety related SSC, and one class (NC) for non-safety SSC.

The justification of safety classification has to prove that this general principle is achieved (and if relevant, justify exceptions).

The main inputs are:

- The categorization of all I&C functions. In general, this type of information exists in a specific document or database;
- The classification of all I&C units.

Then for each I&C function, the list of units involved in the processing has to be determined, based on detailed design I&C documents. Following this, the safety classification of each I&C unit is checked for accuracy according to the safety functions that are implemented within the system.

3.3. FMEAs/justification of single failure criterion

FMEAs are related to an I&C system in the sense that they cover the failure modes and failure consequences of the I&C system. In order to analyze the effects of the failure modes properly, they are performed by considering I&C safety functions. The failures of equipment which does not affect safety functions are not analyzed.

The FMEA has the following objectives:

- Identify the failure modes of the system (these inputs are given by the manufacturer);
- Demonstrate that all relevant I&C functions have met this required criterion (this generally concerns category 1 functions and part of category 2 functions);
- Demonstrate the extent of coverage of self-monitoring/test features and of periodic tests;
- Serve as an input for other studies, e.g. the reliability study.

FMEAs are performed in a function-oriented way in order to analyze the effects of the single failures of the I&C modules on the I&C functions. Firstly, the functions of the I&C system are identified. In order make the analysis easier, functions, which have the same structure and properties, with regard to the analysis, can be grouped into families. A common analysis is then made for the whole family of structures.

Secondly, the failure modes of the I&C modules used to implement the I&C function are identified.

Thirdly, the consequences of each failure mode at functional level are analyzed, and the corresponding detection means are identified.

The FMEA can be performed at two different stages of the design of the system. A preliminary FMEA can be performed based on system specifications and concepts, and documents detailing preliminary allocation of I&C functions to I&C units. The final FMEA is performed based on the detailed design documentation.

It should be mentioned that for this activity, the best option is to involve both safety and I&C specialists in order to ensure that the methodology is applied correctly, to have a critical viewpoint, but also a good understanding, of how the system works and can fail.

3.4. Independence analyses

According to IAEA safety glossary [2], independent equipment is *"equipment that possesses both of the following characteristics:*
(a) The ability to perform its required function is unaffected by the operation or failure of other equipment;
(b) The ability to perform its function is unaffected by the occurrence of the effects resulting from the postulated initiating event for which it is required to function."

Additionally, IEC 61513 [3] mentions that "*means to achieve independence in the* [I&C] *design are electrical isolation, physical separation and communications independence"*.

Independence analysis consists in evaluating that these means have been implemented adequately, so that needs of independence between I&C systems, units or functions are correctly addressed in the design.

It should be mentioned that also for this activity, both safety and I&C specialists need to be involved.
With regard to safety, a list of required independences, based on defense in depth or safety classification, has to be established.
In parallel, with regard to I&C, all potential adverse effects that an I&C system can have on another one, have to be identified.
Based on this, the impact of all potential effects on required independences is assessed. If consequences are not judged acceptable, design measures have to be implemented.

3.5. CCF analysis

A mentioned in IEC 62340 ([4]), although common cause failures have been considered to be beyond the deterministic design basis rules of the I&C architecture and safety systems for a long time, a diversity and defense in depth analysis, proving that vulnerabilities of CCF have been adequately addressed, is expected in the design certification application of the I&C design for a new reactors. As an input, latent failures and common failure modes, which might potentially result in a common failure of two or more redundancies, must be identified. This means that an analysis to identify relevant common cause failures and justify if some other ones have been eliminated, is necessary.

A complete elimination of all vulnerabilities of individual I&C systems inflicted upon CCF is not necessary. But in the overall architecture, consistent with the defense in depth definition, a new defense in depth level is required to mitigate the consequences of Design Extension Conditions. This prevents from escalating to an accident with core degradation. Most of the consequences could only exist if multiple failures occurred and made the level 3a functions inoperable.

This is managed by implementing complementary I&C functions needed to cope with a CCF in the level 3a I&C, with the goal to prevent the core degradation or to mitigate the radiological

consequences to an acceptable level. Thanks to I&C level 3b, a sequence combining an initiating event and the simultaneous failure of both DiD levels 3a and 3b functions is considered in the residual risk.

The need to provide a back-up of a level 3a function is identified by either, or both, probabilistic and deterministic approaches, and it depends on both the estimated consequences in case of CCF, and the estimated frequencies of the initiating events.

In the event of a CCF, the probabilistic approach is often more appropriate. But practically, in order to secure the design, a decoupling deterministic approach can be used, as long as it is verified with the PSA studies. This deterministic approach is the CCF Analysis.

For every level 3a I&C system, credible CCF are first identified. For each of these credible CCF, it is decided with which set of Design Basis Conditions analyzed in the accident analysis they have been to be combined.

Then the CCF analysis identifies whether a function exists in a system diversified from the 3a level defense in depth I&C system, designed to respond to the accident which was caused by a failure of some sort (as the CCF might be due to a latent default on an I&C platform, it is better to postulate that all functions processed by I&C systems based on the same technology or software, failed). Other systems important to safety and designed to provide diversity are considered to respond as expected. This function can be designed by using best estimate analyses with realistic assumptions.

3.6. Robustness of I&C architecture with regard to internal hazards

Analysis of robustness of the I&C architecture with regard to internal hazards is performed in order to analyze the effects of one internal hazard on the I&C functions.

The analysis of the I&C architecture robustness against internal hazards is very similar to the approach used for the FMEA, where failure modes of components are replaced by internal hazards. Internal hazards that are generally addressed in these studies are fire and flooding. A common analysis can be made for all functions that are part of the same family (as defined for FMEAs). The consequences of each hazard at a functional level are analyzed.

The analyses can be performed at two different stages of the design. A preliminary study can be performed on the basis of system specifications and concepts, documents detailing preliminary allocation of I&C functions to I&C units, and preliminary allocations of I&C units to buildings. The final analysis is performed on the basis of the detailed design documentation.

3.7. Reliability analyses

This study is related to each particular I&C system in the sense that it covers the quantitative assessment of the failures of the I&C system itself. However, in order to obtain significant reliability figures for the plant itself, it is performed by considering an assessment of the I&C functions. Only safety relevant functions are generally studied, meaning that the failures of the equipment which does not affect safety functions are not analyzed.

The reliability study has the following objectives:

- Calculate the reliability of the I&C system, i.e. the probability of failure on demand of the functions implemented in the I&C system(s);
- Validate the required frequency for periodic tests;
- Demonstrate that the reliability targets imposed on the safety system are fulfilled.

The reliability analyses are performed in a function-oriented way, similar to the FMEA of the I&C systems. One calculation is made per family of functions. However, some families can be studied by

comparing them to other ones (e.g. if it can be justified that one family is more reliable than another one).

Firstly, fault trees are established using the FMEA of the I&C system(s): these fault trees identify the combination of the single failures identified in the FMEA, leading to events which impact the reliability of the system.

The failure rates are introduced in these fault trees to quantitatively assess the failure modes. Common cause failures are also considered. The credible failure modes identified in the CCF analysis (see §3.5) are also included in the fault trees. Software failures are considered on a case by case basis. These evaluations also take into account the maintenance and test policy. Based on these fault trees, the probability or frequency of the unexpected event is calculated.

When the model is worked out and validated, it is possible to evaluate the system performance and, if necessary, to perform sensitivity studies on tricky parameters (for example, frequency of periodic tests).

If targets imposed on a system are not met:

- The main contributors to the unreliability are analyzed,
- Then the possible refinements of calculations or data are identified,
- If this is not sufficient, possible modifications of test periods are identified,
- If this is still not sufficient, possible design improvements are needed,
- Finally, fault trees and calculations are updated.

Reliability analyses of digital I&C systems are subject to a specific communication and paper [5] in this PSAM conference.

The reliability study can be performed at two different stages of the design of the system. A preliminary study can be performed, based on system specifications and concepts, documents detailing preliminary allocation of I&C functions to I&C units, and the preliminary FMEA. The final study is performed on the basis of the detailed design documentation and final FMEA.

3.7. Inclusion of digital I&C in the PSA

The way the I&C is modeled in the PSA is vital in ensuring that the PSA meets the safety requirements confidently, and that with an adequate level of margin. For this reason, the I&C model shall provide:

- Support to design in all phases (including easy and comprehensive analysis of the minimal cutsets);
- Support to licensing by giving confidence to the regulator during the modeling;
- The capacity to assess that the final design will meet the probabilistic objectives with confidently;
- An assessment that the diversity of systems and components in the overall I&C architecture is sufficient from a probabilistic point of view;
- The mapping of the dependencies (including support systems).

In addition, the I&C model should be easy to update and suitable, when needed, for Risk-Informed applications and Risk Monitoring.

A methodology based on a comparison between I&C models in EPR PSAs, expert and engineering judgments with regard to these models, detailed I&C reliability studies, as well as on knowledge of the systems behavior, has been developed and is summarized in [6].

4. **ROLES IN THE I&C SAFETY DEMONSTRATION**

The roles of these studies in the whole safety demonstration cover overall I&C justifications, as well as individual I&C systems justifications. Additionally, probabilistic and deterministic aspects are assessed. This is summarized in Table 1.

Table 1: Roles of the I&C analyses in the safety demonstration

	Overall I&C justification	**I&C system justification**	**Probabilistic demonstration**	**Deterministic demonstration**
Justification of defense in depth	X			X
Justification of safety classification		X		X
FMEAs/Justification of the single failure criterion		X		X
Independence analyses	X	X		X
CCF analysis	X		X	
Robustness of I&C architecture with regard to internal hazards	(X)	X		X
Reliability analyses		X	X	
Inclusion of I&C in PSA	X		X	

5. **LINKS BETWEEN METHODS**

Table 2 establishes the links between the different methods.

Table 2: Links between methods

	Justification of safety classification	FMEAs / Justification of single failure criterion	Independence analyses	CCF analysis	Robustness of I&C architecture with regard to internal hazards	Reliability analyses	Inclusion of I&C in PSA
Justification of defense in depth	No	No	Yes (1)	Yes (2)	Sometimes (3)	No	No
Justification of safety classification		No (4)	Yes (5)	No	No (6)	No (7)	No
FMEAs / Justification of single failure criterion			Partially (8)	No	Yes (9)	Yes (10)	Yes (11)
Independence analyses				No	Sometimes (12)	No	Yes (13)
CCF analysis					No	Yes (14)	Yes (15)
Robustness of I&C architecture with regard to internal hazards						No	Yes (16)
Reliability analyses							Yes (17)

(1) Justification of defense in depth is an input to identify cases to be studied in independence analyses. It also uses results of independence analyses.
(2) Common cause failure analysis justifies adequate diversity between levels 3a and 3b in the defense in depth concept.
(3) Depending on concept of defense in depth.
(4) Nevertheless, necessity to apply single failure criterion is correlated to safety classification.
(5) Justification of safety classification is an input to identify cases to be studied in independence analyses.
(6) Nevertheless, the necessity that a system is robust to internal hazards is correlated to safety classification.
(7) Nevertheless, in some cases, reliability targets are linked to the classification of the I&C system.
(8) FMEA can help to identify common points in postulated redundant parts of a system.
(9) Analyses are very similar. Both studies can use the concept of family of functions.
(10) FMEA is input for the reliability analysis. Both studies can use the concept of a family of functions.
(11) FMEA is input for PSA.
(12) These analyses are sometimes mixed.
(13) Independence analysis can be used as input for PSA.
(14) CCF analysis is input for reliability analysis.
(15) CCF analysis is input for PSA.
(16) Robustness of I&C architecture with regard to internal hazards can be used as an input for PSA (hazard PSA).
(17) Reliability analyses help to justify the modelling of I&C in PSA.

6. CONCLUSION

This paper has given insights to people involved in any kind of activities related to the safety assessment of I&C designs, including I&C systems qualification, in order to have a complete picture of all the safety issues with this kind of system, and to allow them to identify potential improvements in their own practices.

References

[1] IAEA Safety Standard, *"Safety of Nuclear Power Plants: Design - Specific Safety Requirements"*, SSR-2/1 (Rev. 1)
[2] *"IAEA Safety glossary - Terminology used in nuclear safety and radiation protection"* - 2007 edition
[3] International standard IEC 61513 edition 2.0, *"Nuclear power plants - Instrumentation and control important to safety - General requirements for systems"* (2011)
[4] International standard IEC 62340 edition 1.0, "*Nuclear power plants – Instrumentation and control systems important to safety - Requirements for coping with common cause failure (CCF)*" (2007)
[5] M. Jockenhövel-Barttfeld, S. Karg, C. Hessler and H. Brunelière, *"Reliability Analyses of Digital I&C Systems within the Verification and Validation Process"*, PSAM 14, 2018, Los Angeles
[6] H. Brunelière, 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/ESREL12, 2012, Helsinki