CONSIDERATIONS ON HARMONIZATION OF SAFETY ASSESSMENT OF NEW REACTORS’ DESIGN

N. NICAISE
C. MAYORAL
AREVA NP
Paris, France
Email: norbert.nicaise@areva.com
Email: claude.mayoral@areva.com

Abstract

High-level safety objectives and requirements between countries are comparable (notably in European countries) and in general do not show important gaps. However, the application of specific national regulatory documents and the impact of specific safety assessment processes can have an important impact on the design of a reactor.

Indeed, even with similar intention and definitions, a regulation in a country can lead to a different design than in another country due to scientific cultural background and/or NPP experience feedback of each country.

As a matter of fact, several differences could be highlighted between on-going EPR projects, coming from the safety assessment approach of the national Safety Authority more than differences coming from strict regulatory requirements.

We could for example present the postulated failure of safety digital I&C that leads to require a back-up system independent and diversified. In some countries the term ‘diversified’ allows to rely on another type of digital I&C, in other countries it is understood as being a non-digital I&C system.

After developing typical examples, this paper will discuss how harmonization of practices is desirable to increase standardization of reactors’ design that will facilitate licensing processes and bring benefits to safety.

1. INTRODUCTION

High-level nuclear safety objectives and requirements have reached a certain level of harmonization and are comparable between countries (notably in European countries). Nevertheless, going deeper in the analysis of the methods and practices followed by different national regulatory bodies to evaluate the respect of similar high-level safety requirements, puts in evidence that the safety evaluation culture of each country has an impact on the final safety evaluation. The objective of the article is to point out some differences in the safety evaluation approach followed by different regulatory bodies, but not to express a judgment about these approaches. The objective is to highlight, through examples based on the current EPR projects licensing feedback, that it still exists areas where safety evaluation approach and interpretation of safety concepts are not harmonized.

2. TYPICAL EXAMPLE OF DESIGN DIFFERENCES COMING FROM COUNTRY SPECIFIC SAFETY AUTHORITY ASSESSMENTS

2.1. I&C architecture

The I&C architecture differs from one EPR project to the other and this paragraph focuses only on the difference in the implementation of the back-up of the I&C Protection System.

On all the EPR projects there are two I&C digital platforms. An I&C platform is a set of equipment compatible between them. The safety I&C platform is an AREVA equipment (“Teleperm XS”) specifically designed according to nuclear safety requirements having the highest safety classification. The Protection System is one of the systems implemented in the safety I&C platform and houses the highest safety functions. The operational I&C platform is a Siemens equipment (“SPPA-T2000”) designed as per good industrial practices with a good experience feedback from the industrial sector. I&C is involved in the safety design and demonstration for all the design conditions of the safety referential, from the Design Basis Conditions (categories 2 to 4) to the Design Extension Conditions A (prevention of core-melt) and B (mitigation of core-melt). For the Design Extension Conditions A resulting from Design Basis Conditions of category 2 cumulated with the loss of the Protection System (covering ATWT cases), the safety demonstration proposed by EDF and
AREVA credit the availability of the Safety Automation System implemented in the operational I&C platform. This system has been specifically designed and validated to meet the requirements of an intermediate safety classification level (in particular IEC 62138 [1] and the French Fundamental Safety Rule II.4.1.a [2]). To justify this safety position EDF & AREVA performed very refined studies to show that the design and the verification and validation process of the overall I&C architecture conform to the applicable nuclear safety requirements. The French Safety Authorities evaluation concluded that such I&C equipment and architecture are able, through the way the different equipment are grouped into systems or at the contrary are independent (either through physical separation, electrical separation, technology diversity or by logic), to ensure that no design condition would lead to a situation not covered by the safety demonstration. For the OL3 (Finland) and HPC (UK) EPR projects, the regulatory bodies considered that it is not possible to credit the Safety Automation System in case of the loss of the Protection System. Indeed, whatever the reliability of the Safety Automation System and its design difference with the Protection System, the complete loss of all the digital I&C systems had to be postulated. The argument of physical separation between the Safety Automation System and the Protection Systems as well as the difference in terms of design is not considered sufficient by the UK and Finnish regulatory bodies to conclude that the I&C reliability is at a sufficient level to meet Design Extension Conditions A criteria. Then, to meet the safety criteria of these operating conditions, an additional I&C system had to be implemented called “hardwired Backup system” in Finland or “Non Computerized Safety System” in UK whose design is based on a non-digital technology.

This example shows that the notion of diversity and overall reliability of a complex architecture like the I&C is not evaluated with the same criteria even in countries having the same overall safety requirements. This example shows that, even though the treatment of common cause failure caused by software within digital safety systems has already been examined within a specific MDEP working group [3], this topic could be proposed for further harmonization between countries to get a better mutual understanding of the rational of the situations to be covered.

2.2. **Identification of the list of the Design Basis Conditions and Design Extension Conditions**

The identification of the list of the Design Basis Conditions and Design Extension Conditions differ from one country to another, and this paragraph will only focus on a specific aspect.

For all EPR projects, the Design Basis Conditions of categories 2 to 4 are identified to determine, on the basis of a conservative approach, provisions enabling to limit the effects of the selected initiating events. Then, depending on their occurrence probability, these events are distributed in three categories (2 to 4) and studied with conservative assumptions as for example the application of an additional single failure, and the consideration of the preventive maintenance leading to the systematic unavailability of equipment possibly in maintenance when the event occurs. Then, to ensure fulfillment of the probabilistic core melt frequency target, more complex accident sequences are taken into account and grouped in a category called Design Extension Conditions A, which cover notably Design Basis Conditions with additional failures. These Design Extension Conditions A are evaluated using less stringent rules and requirements than the ones used to evaluate the Design Basis Conditions. As for example, Design Extension Conditions A are evaluated without taking into account an additional single failure (as the considered event is already a multiple failure event). This approach is commonly adopted even if some differences exist in the level of conservatism applied in terms of coverage of the main transient parameters.

For FA3 (France), TSN (China) and OL3 (Finland) EPR projects, the Design Basis Conditions are based only on single initiating events, and the multiple failures are only addressed in the Design Extension Conditions A. For HPC (UK) project, the identification of the Design Basis Conditions is performed using mainly the occurrence probability of the initiating event, independently of its nature (single or multiple events). As a consequence, some multiple initiating events must be studied following the stringent conservative rules of the Design Basis Conditions, such as the additional single failure and the combination of simultaneous preventive maintenance. This specific methodology of identification of the Design Basis Conditions leads, for example in the design of the HPC HVAC system, to implement additional safety chillers and to upgrade the classification of two non-classified preventive maintenance HVAC trains.

This example shows that the identification of Design Basis Conditions (depending on the definition retained for the associated initiating events, only single events or possibly multiple events, which corresponds to
different approaches between deterministic and probabilistic aspects) could be proposed as a topic for harmonization between countries.

2.3. **Rules used to evaluate Design Basis Conditions**

This paragraph addresses some specifics about differences between countries in the rules used to evaluate the Design Basis Conditions of category 2 (also called Anticipated Operational Occurrences).

For the FA3 project, the French practice imposes to credit only the safety grade systems (with exceptions concerning some main plant controls). Then, taking into account the required conservative assumptions (additional single failure, preventive maintenance considered simultaneously with the event occurrence) leads to transients that significantly deviate from the ones that would normally result from the initiating events.

For OL3 project, the Finnish practice allows to credit the operation of the main plant controls and limitations in addition to the safety grade systems. That allows sticking to a more realistic transient evolution. In addition, the Finnish practice requires to complement the analyses by addressing the same initiating events while crediting only safety grade systems and to meet safety criteria corresponding to Design Basis Conditions of category 3, instead of category 2.

The difference between the two approaches leads to very different transient evolutions for the same initiating events and for the same reactor design. It can artificially lead to conclude that safety margins are considerably different from one EPR project to the other, although differences in the results and consequences of the transients are often only due to different levels of conservatism taken into account for the same criteria and physical phenomena. This example shows that the rules to be used to analyse Design Conditions could be proposed as a topic for harmonization between countries.

3. **CONCLUSION**

High-level nuclear safety objectives and requirements have reached a certain degree of harmonization and are comparable between countries (notably in European countries). As a matter of fact, the IAEA Safety Requirements Series, the WENRA reference levels, and the will to compare safety evaluations performed in different countries for the same reactor design through the MDEP organisation, help harmonizing the safety assessment. Moreover, the World Nuclear Association (WNA) established the Cooperation in Reactor Design Evaluation and Licensing (CORDEL) Working Group with the aim of stimulating a dialogue between the nuclear industry (including reactor vendors, operators and utilities) and nuclear regulators (national and international organizations) on the benefits and means of achieving a worldwide convergence of reactor safety standards for reactor designs [4]

Nevertheless, it appears that the application of specific national regulatory approaches and safety assessment processes can have an important impact on the design of a reactor. As illustrated in the paragraphs above, the licensing experience feedback of the current EPR projects show examples of design modifications that had to be implemented depending on the understanding/interpretation of a safety requirement and also on the importance given in terms of probabilistic and/or deterministic rules. The differences in interpretation of a same safety requirement can be explained by scientific cultural background or specific Nuclear Power Plants experience feedback.

These examples show that even if a number of organizations already promote the cooperation between Safety Authorities and nuclear industry players (IAEA, WENRA, MDEP, WNA) and played an important role to improve the standardization of the regulatory framework in force in each individual country, this cooperation needs to be carried on. Indeed, even keeping specific national regulatory frameworks, a common understanding of the safety evaluation and safety concepts and requirements would be beneficial both for lighting the regulatory bodies workload and the predictability of the licensing of a reactor design, and of the cost to completion for new nuclear projects.

**REFERENCES**
[1] IEC 62138 “Nuclear power plants Instrumentation and control important for safety Software aspects for computer-based systems performing category B or C functions”

