Date: May 2020
Validity: Approved
Version 1

MDEP Design-Specific Common Position CP-EPRWG-07

Common Positions on the EPR Instrumentation and Controls Design

Participation

Regulators involved in the MDEP working group discussions:	NNSA (China), STUK (Finland), ASN (France), SSM (Sweden), ONR (UK)
Regulators which support the present common position:	NNSA (China), STUK (Finland), ASN (France), SSM (Sweden), ONR (UK)
Regulators with no objection:	AERB (India)
Regulators which disagree:	

Purpose

To identify common positions among the regulators reviewing the EPR Instrumentation and Controls (I&C) Systems in order to:

1. Promote understanding of each country's regulatory decisions and basis for the decisions,

2. Enhance communication among the members and with external stakeholders, and

3. Identify areas where harmonization and convergence of regulations, standards, and guidance can be achieved or improved.

Discussion

Since January 2008, the EPR I&C Technical Expert Subgroup (TESG) members have met periodically to exchange information regarding their country's review of the EPR I&C design. The EPR I&C TESG consists of regulators from China, Finland, France, India, Sweden and the United Kingdom[1]. The information exchange includes presentation of each country's review status and technical issues, sharing of guidance documents, and sharing of regulatory decision documents. The TESG focused on the following aspects of the EPR I&C design:

1. I&C system independence
2. Level of defence-in-depth and diversity
3. Qualification/quality of digital platforms
4. Categorization/classification of systems and functions

As meetings were conducted, some areas were emphasized more depending on the significance of the issues for each country. During the TESG interactions, it became apparent that there were aspects of the EPR design where the countries had common agreement. On November 2, 2009, three of the subgroup countries, France, Finland and the United Kingdom, issued a joint regulatory position on the EPR I&C design as a result of the ASN advisory committee meeting in France. This statement of common positions expands upon that joint regulatory position to include other design aspects.

[1] Canada and the United States initially participated in the EPR I&C TESG and contributed to some of the common positions, but they discontinued participation when EPR review activities in their countries were suspended. At the time of publishing, EPR project in India is under siting stage, and no design review has started.

The regulators identified differences between the EPR I&C design presented to each country. To the extent possible, regulators communicated in order to identify causes of these differences.

At the beginning of each country's review, there was an impression of a standard EPR design. However, as the countries discussed their reviews, it became apparent that there were differences in EPR I&C designs for Finland, France, the U.K., and China. The differences were primarily in the areas of diverse back-up systems, prioritization of commands (priority modules), safety classifications, and the perceived ability of digital platforms to support safety functions. The differences in design are partly driven by meeting regulatory expectations (e.g. different classification schemes and different backup requirements) and also by customer preferences and the overall I&C designer's choice.

Positions

I. *Design simplicity is a fundamental principle for developing safety systems with high reliability. The regulators recommended that guidance for simplicity be addressed generically through MDEP.*

Design simplicity is a fundamental principle for development of safety/high-reliability systems. However, some regulators found the EPR I&C architecture and systems to exhibit a higher degree of complexity than previous design due, e.g. to the management of 4 mechanical divisions rather than 2. Part of the complexity arose from the level of interconnectivity between I&C systems of different divisions and safety classes. It appears there are few regulations, standards, or guidance to address the aspect of simplicity directly because there is no objective definition of simplicity/complexity, but instead require testability or proof-of-determinism avoiding by nature too much complexity. The subgroup recommended the MDEP Digital I&C Issue Working Group (DICWG)[2] consider complexity of digital I&C architecture and systems as a topic to address generically, as the issue will appear in other new reactor reviews. DICWG issued Generic Common Position CP-DICWG-06: Simplicity in Design in March 2013.

II. *Independence between systems and divisions is essential to the safety of I&C design, but portions of the original EPR design did not demonstrate adequate independence in data communications. Regulators addressed data communications independence by requiring safe data communication design practices and thoroughly reviewing the EPR data communication architecture, processes, logic, and information exchange.*

Independence between redundant safety divisions and between I&C system of different safety classes is necessary to ensure a failure in one portion of the I&C system will not prevent the safety function from being accomplished. The EPR I&C design is highly interconnected through data communication links. To ensure adequate independence with data communications, the overall I&C designer (which is not AREVA or Framatome in all cases) must demonstrate electrical and functional isolation, such that either hardware failures or subtle data transmission or timing errors over communication links will not affect one or more safety functions. Portions of the original EPR I&C design did not adequately address these criteria or aspects of the design were found to be non-compliant with the independence principle. The independence issue was a high priority technical issue for each country, and the regulators engaged the I&C designer to address the issue by modifying some parts of the I&C design.

[2] The DICWG has been closed in April 2018 and its activities have been transferred to the WGDIC within the CNRA

III. The regulators' assessment of the TELEPERM XS digital platform has not identified any significant design issues. The platform is being used in the highest I&C safety classes.

The member countries reviewed the TELEPERM XS platform to various levels of detail. No country has identified significant issues from their assessments of the platform.

IV. The regulators have not identified significant issues regarding the assessment of the application software used to run on the TELEPERM XS platform[3].

The member countries have reviewed the application software used to run on the TELEPERM XS platform to various levels of detail. To date, no country has identified any significant issues from their assessment of the application software they have reviewed.

V. The design, quality, and qualification of digital devices of limited functionality will influence the safety of plant systems in which they are embedded (also called smart devices). The regulators recommended acceptance criteria for digital devices be addressed generically through MDEP.

As digital technology gains expanded use in nuclear power reactors, digital devices of limited functionality are appearing in plant systems where they have not previously been used. For example, embedded digital devices will be utilized in EPR plant systems such as circuit breakers, diesel generators, and cooling systems. In discussions with the overall I&C designer, each member country acknowledges the use of these embedded digital devices and is engaging the overall I&C designer regarding their design, quality, and qualification. In the beginning of EPR projects there were little to no regulations, and limited information in standards, or guidance to address the aspect of embedded digital devices/smart devices. The subgroup recommended DICWG consider embedded digital devices/smart devices as a topic to address generically as it will appear in other new reactor reviews. DICWG issued Generic Common Position CP-DICWG-07: Selection and Use of Industrial Digital Devices of Limited Functionality in July 2014
.

VI. The regulators find back-up systems as an effective means to enhance defence-in-depth of the EPR I&C design if they do not make the I&C architecture and its maintainability over complex.

The regulators find that each EPR uses some type of back-up system. If the backup systems are sufficiently qualified for the functions they perform, and meet applicable regulatory criteria, then they can be effectively used to support defence-in-depth of I&C safety functions. However, the experience feedback of safety systems demonstrates that common-cause faults are mainly due to incorrect maintenance or calibration actions and not to design faults; therefore, it should not be presupposed that adding a system (which increases the burden of maintenance and calibration) always increases safety.

VII. Interface issues between the EPR I&C systems and other plant systems produced complex technical review issues. Some regulators and design organizations recognized the value of utilizing cross-disciplinary teams and techniques to identify and address complex plant interface issues.

Like many new reactor designs, the EPR I&C design possesses a high number of direct and indirect interfaces with other plant systems. Part of regulators found some of the most difficult and complex technical issues were associated with the interactions between I&C and plant systems. Examples include spurious actuation of I&C systems and its subsequent plant effects, and the

[3] At the time of publishing, the application software has not yet been available for review for regulator in the United Kingdom.

interdependence between I&C systems and supporting systems, including electric power supply and heating, ventilation, and cooling systems. In some cases, failure of I&C systems or their interfacing plant systems could have indirect, negative impacts to systems they interface when there is no physical connection between interfacing systems (i.e., linkage through plant processes).

Some regulators found the use of multi-disciplinary teams and hazard assessment techniques capable of capturing such interface issues were useful to identify and address such issues with the EPR design. The regulators interacted with the DICWG to provide the EPR review experience and to promote the benefits of multi-disciplinary teams and hazard assessment techniques when addressing such interface issues. As a result, the DICWG issued Generic Common Position CP-DICWG-13: Common Position on Spurious Actuation in July 2017.

VIII. The regulators evaluated the EPR design to ensure both I&C systems and their interaction with plant systems ensure lower class systems would not compromise the functionality of higher class systems.

Within the original EPR design, there were a few cases where lower safety class I&C systems could impact higher class plant systems. Such instances included loading of higher class electrical buses by lower class I&C systems or heating and ventilation of higher class plant equipment controlled by lower class I&C systems. The regulators requested such interactions would not compromise the functionality of higher class systems by requiring design changes in I&C or plant systems and by thorough evaluation of safety class separation and engineering analysis.