MDEP Common Position No EPR-01

Related to : EPR Working Group activities

COMMON POSITIONS ON THE EPR INSTRUMENTATION AND CONTROLS DESIGN

Multinational Design Evaluation Program

EPR Working Group

EPR Instrumentation and Controls Technical Expert Subgroup

COMMON POSITIONS ON THE EPR INSTRUMENTATION AND CONTROLS DESIGN

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,
3. Identify areas where harmonization and convergence of regulations, standards, and guidance can be achieved or improved, and
4. Supports standardization of new reactor designs.

Discussion

Since January 2008, the EPR I&C Technical Expert Subgroup (TESG) members met five times to exchange information regarding their country's review of the EPR I&C design. The EPR I&C TESG consists of regulators from China, Canada, Finland, France, the United Kingdom, and the United States. 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 four core areas of the EPR I&C design:

1. I&C System Independence (particularly for data communications)
2. Level of Defense and Diversity (back-up systems)
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 result of the Groupe Permanent meeting in France. This statement of common positions expands upon that joint regulatory position.

Positions

I. The regulators identified differences between the EPR I&C design presented to each country. To the extent possible, regulators will communicate and coordinate regulatory decisions to support standardization of the EPR I&C design.

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 different EPR I&C designs for Finland, France, the U.K., China, and the U.S. 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 driven by meeting regulatory requirements, customer preferences, and the overall I&C designer's choice.

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

Design simplicity is a fundamental principle for development of safety/high-reliability systems. However, the regulators have found the EPR I&C architecture and systems to exhibit a high degree of complexity. Much of the complexity arises from the high level of interconnectivity between I&C systems of different divisions and safety classes. It appears there are little to no regulations, standards, or guidance to address the aspect of simplicity because there is no objective definition of simplicity/complexity. Regulators are addressing the specific effects of simplicity/complexity such as testability or proof-of-determinism. The subgroup recommends that the MDEP Digital I&C Issue Working Group 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.

III. 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 are addressing 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 NP 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 is a high priority technical issue for each country, and the regulators continue to engage the overall I&C designer to address the issue.

IV. To date, 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 have reviewed the TELEPERM XS platform to various levels of detail. To date, no country has identified any significant issues from their assessments of the platform.

V. To date, the regulators have not identified significant issues regarding the assessment of the application software used to run on the TELEPERM XS platform; however the assessments are ongoing for all countries.

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.

VI. The design, quality, and qualification of digital devices will influence the safety of plant systems in which they are embedded. The regulators recommend that acceptance criteria for digital devices be addressed generically through MDEP.

As digital technology gains expanded use in nuclear power reactors, digital devices will appear 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. It appears there are little to no regulations, and limited information in standards, or guidance to address the aspect of embedded digital devices. The subgroup recommends that the MDEP Digital I&C Issue Working Group consider embedded digital devices as a topic to address generically as it will appear in other new reactor reviews.

VII. The regulators find back-up systems as an effective means to enhance defense-in-depth of the EPR I&C design.

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 defense-in-depth of I&C safety functions.