MARCUS R. NICHOL
Senior Director, New Reactors

1201 F Street, NW, Suite 1100
Washington, DC 20004
P: 202.739.8131
mrn@nei.org
nei.org

NUCLEAR ENERGY INSTITUTE

February 11, 2021

Mr. Mohamed Shams
Director, Division of Advanced Reactors and Non-Power Production and Utilization Facilities
Office of Nuclear Reactor Regulation
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001

Subject: Supplemental NEI Comments on draft Design Review Guide (DRG): Instrumentation and Controls for Non-Light-Water Reactor (non-LWR) Reviews [Docket ID NRC-2020-0072]

Project Number: 689

Dear Mr. Shams:

On August 3, 2020 the Nuclear Energy Institute (NEI)[1] and its members provided comments on the subject draft Design Review Guide (DRG): Instrumentation and Controls for Non-Light-Water Reactor (non-LWR) Reviews. In reviewing the October draft of the DRG we noticed that a number of enhancements have been made based on stakeholder feedback. In listening to the discussion at the Advisory Committee on Reactor Safeguards (ACRS) Subcommittee on Digital Instrumentation and Control (DI&C) meeting on October 21, 2020 and the ACRS Full Committee meeting on December 2, 2020, we realized that there is an opportunity to further clarify the guidance related to common cause failures as the staff begins to finalize the DRG. Our supplemental comments are focused solely on section X.2.2.1.3 "Diversity in Support of Defense-in-Depth to Address Common Cause Failures (CCFs)" and Appendix B "Cross-Cutting Issues and Interfaces."

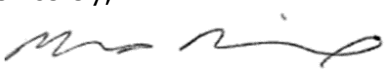
In the August 3, 2020 letter we noted that the approach in the draft DRG is based on applying deterministic criteria and would benefit from consideration of the Commission direction in SRM SECY-19-0036 regarding the application of risk-informed principles when strict, prescriptive application of deterministic criteria is unnecessary to provide reasonable assurance of adequate protection. Along those lines, NEI believes that section X.2.2.1.3 would be improved by clarifying and enhancing guidance to allow for a risk-informed and performance-based approach for identifying CCF vulnerabilities, ranking those vulnerabilities based on a risk assessment, and applying appropriate control measures to the DI&C system commensurate with their risk

[1] The Nuclear Energy Institute (NEI) is responsible for establishing unified policy on behalf of its members relating to matters affecting the nuclear energy industry, including the regulatory aspects of generic operational and technical issues. NEI's members include entities licensed to operate commercial nuclear power plants in the United States, nuclear plant designers, major architect and engineering firms, fuel cycle facilities, nuclear materials licensees, and other organizations involved in the nuclear energy industry.

significance. In order to support the regulatory review of the aforementioned risk-informed approach to CCF vulnerabilities, we also recommend that "PRA" be added to the Interface Discipline column in the second row entitled "Diversity and Defense-in-Depth" of Table X.2-1 "Cross-Cutting Interface Reference." Our detailed comments in the attachment, in the form of a markup to the NRC's text, are intended to clarify the option for a risk-informed and performance-based approach when considering diversity in support of defense-in-depth to address CCFs. Incorporation of these edits will support the NRC goals for this guidance to be safety-focused, risk-informed, and performance-based.

If you have questions concerning our comments, please contact me or Kati Austgen (202.739.8068 or kra@nei.org).

Sincerely,



Marcus Nichol

Attachment

c: Mr. John P. Segala, NRR/DANU/UARP, NRC
Mr. Jordan P. Hoellman, NRR/DANU/UARP, NRC
Document Control Desk

Section X.2.2.1.3 "Diversity in Support of Defense-in-Depth to Address CCFs"

To the degree that an I&C system plays a role (e.g., influences, challenges, or performs a safety function(s)), the reviewer should evaluate how the design addresses potential CCFs due to (1) systematic faults caused by design and implementation defects within redundant divisions of safety-related systems; (2) propagational faults from systems that are not safety-related to safety-related systems that can adversely impact the safety-related systems; and (3) internal and external hazards that can adversely impact a safety-related system or systems belonging to multiple levels of defense. For systematic faults within redundant safety divisions, diversity is one means of addressing these types of faults. There may also be systematic faults caused by design and implementation defects in highly integrated I&C systems that are not bounded by the assumptions in the accident analysis to define the LBEs. Good design practices along with design measures (e.g., sufficient physical separation) should be implemented to minimize the likelihood or limit the effects of such faults or undesired system behaviors. For propagation of faults from systems that are not safety-related to safety-related systems or from one safety division to a redundant safety division, having adequate independence minimizes this hazard. For internal and external hazards (e.g., seismic events) that can adversely impact a safety-related system or systems belonging to multiple levels of defense, qualification measures can be used to minimize the impacts of these hazards. Potential CCFs due to systematic faults caused by design and implementation defects are addressed in this subsection. Review guidance for the other two sources of CCF are in Sections X.2.2.1.1 and X.2.2.2 of this DRG.

The reviewer should evaluate the CCF analysis results provided by the applicant to verify that a potential CCF due to latent systematic faults within the digital I&C system are within acceptable limits. In performing this evaluation for safety-significant functions, the FSAR should include a diversity in support of DID assessment for each event analyzed in the accident analysis section to determine whether:

(1) a potential CCF due to systematic ~~faults~~ failures in the digital I&C system could disable a safety function.~~; and~~ If using the Risk-informed and Performance-based Approach discussed below in making this determination, both the likelihood and consequence of a systematic failure and the associated CCF should be considered to provide a risk-informed assessment.

(2) a diverse means, to include functional diversity and/or internal diversity within the digital I&C system, not subject to the same CCF is available to perform either the same function or a different function such that radiological release limits are not exceeded.

NOTE:~~Note that~~ T~~t~~he overall analyses of LBEs and related DID assessment for safety functions may include the potential contributions from I&C systems.

Review Procedures

Where appropriate, the reviewer should confirm that a diversity in support of DID assessment has been completed ~~(or an equivalent assessment included in a PRA performed to support LBE selection, SSC classification, and evaluation of DID adequacy)~~ for the proposed I&C system and that the assessment demonstrates that vulnerabilities to CCFs have been adequately addressed (see Deterministic Approach). An equivalent assessment based on systems engineering techniques and/or PRA risk insights used to support LBE selection, SSC classification, and evaluation of DID adequacy can also be used to demonstrate that the vulnerabilities to CCFs have been adequately addressed (see Risk-informed and Performance-based Approach). For safety-significant functions, the application should contain information sufficient to demonstrate that the diversity in support of DID assessment analyzes each postulated CCF for each event that is evaluated in the accident analysis section of the application, using best-estimate or design basis analysis methods. The application should include the following information:

Risk-informed and Performance-based Approach:

1. Identification of systematic failures in the digital I&C system(s) that can cause a CCF in the plant SSC(s) in which it interfaces. The identification process used should be robust and recognized by industry and regulatory organizations (e.g., System Theoretic Process Analysis).

2. A graded assessment of the risk significance of the systematic failure in the digital I&C system(s) compared to well established reliability criteria for probability of failures on demand and probability of failures to run. Given that CCFs caused by systematic failures are a beyond design basis event, best estimate methods and realistic assumptions can be used in the assessment.

3. Based on the risk significance assessment of the systematic failures in the digital I&C system(s), a demonstration that appropriate control measures (e.g., internal diversity, functional diversity, independence, segmentation, defense in depth) have been applied to the digital I&C system(s).

Deterministic Approach:

1. Identification of digital I&C systems that are vulnerable to a CCF.

2. Analysis of plant response to demonstrate that (1) any radiation release due to a CCF of the digital I&C system for each of the events evaluated in the accident analysis does not exceed the

radiological dose guidelines; and (2) the integrity of the functional containment boundary as described in the applicant's PDC is demonstrated.

3. A demonstration that for each postulated CCF that could disable a safety function within the digital I&C system concurrent with each event evaluated in the plant safety analysis, a diverse means is identified to provide a diverse or a different function. This diverse means could be an automatic function or a manual operator action, provided the applicant has demonstrated that reliable equipment is accessible and available to perform the function, and the operator and equipment will perform the function within the response time credited to perform these actions.

4. If diversity within the system is credited as providing the diverse means of accomplishing the safety function, an analysis should be provided to demonstrate adequate diversity within the system (e.g., diversity of tools used to configure and program each diverse portion of the system, human diversity in the implementation of each diverse portion of the system).

5~~4~~. Equipment that is not safety-related can be used to provide the diverse means provided it is of sufficient quality or reliability to perform the necessary function under the associated event conditions in a reliable manner.

6~~5~~. The equipment performing the diverse or different function is diverse and independent from the system subject to the CCF. ~~6. If diversity within the system is credited as providing the diverse means of accomplishing the safety function, an analysis should be provided to demonstrate adequate diversity within the system (e.g., diversity of tools used to configure and program each diverse portion of the system, human diversity in the implementation of each diverse portion of the system).~~

7. If other means are credited to address vulnerabilities to CCF, these means should be identified and their effectiveness to ~~eliminate~~ adequately address the CCF vulnerabilities ~~from further consideration~~ should be demonstrated.

8. Provision of a set of displays and controls accessible to the operators for manual system level actuation of critical safety functions and monitoring of parameters that support the safety function. These displays and controls should be independent and diverse from the digital I&C system identified in Items 5 and 6 above.

9. Provision for the reactor operator to manually control components in a priority scheme. The priority scheme should allow the reactor operator to place such components in the safe state necessary to support the safety function. The application should discuss how the system accomplishes the reactor operator action.

10. If defensive measure(s) are used to ~~eliminate~~ adequately address the CCF vulnerabilities~~from further consideration~~, the application should include a supporting technical basis and acceptance criteria for the use of the defensive measure(s).