DESIGN REVIEW GUIDE (DRG): INSTRUMENTATION AND CONTROLS FOR NON-LIGHT-WATER REACTOR (NON-LWR) REVIEWS

U.S. NUCLEAR REGULATORY COMMISSION

REVISION DATE: 02/26/2021

Table of Contents

X.0 OVERVIEW OF REVIEW PROCESS

X.0.1 INTRODUCTION

As discussed in the report "Near-Term Task Force Review of Insights from the Fukushima Dai-ichi Accident," [1] the current nuclear regulatory infrastructure was developed for the purpose of reactor licensing in the 1960s and 1970s and supplemented as necessary to address significant events or new issues. To modernize the NRC regulations, the Commission has provided direction to the NRC staff to promote, among other approaches, the use of Probabilistic Risk Assessment (PRA) technology in a manner that complements the NRC's deterministic approach and supports the NRC's traditional defense-in-depth (DID) philosophy. For example, in Staff Requirements Memorandum (SRM) to SECY-11-0024, "Use of Risk Insights to Enhance the Safety Focus of Small Modular Reactor [SMR] Reviews," [2] the Commission approved the staff's recommendation to enhance the efficiency and effectiveness of the SMR application reviews through a design-specific, risk-informed, and safety-focused approach. In response to the Commission's approval, the NRC instrumentation and controls (I&C) staff developed a Design-Specific Review Standard (DSRS) Chapter 7, "Instrumentation and Controls," initially for the BWXT mPower™ SMR design and subsequently for the NuScale SMR design [3]. The restructured safety-focused approach in DSRS Chapter 7, Section 7.1, emphasized fundamental I&C design principles (i.e., independence, redundancy, diversity in support of DID, and deterministic behavior (repeatability and predictability)), and was a step forward for other future SMR and advanced non-light water reactor (non-LWR) licensing applications.

This Design Review Guide (DRG) chapter provides guidance for the NRC staff to use in reviewing the I&C portions of applications for advanced non-LWRs within the bounds of existing regulations.[1] This guidance leverages the DSRS Chapter 7 framework while factoring in the lessons learned from new reactor reviews. This guidance supports the NRC's Vision and Strategy document entitled "Safely Achieving Effective and Efficient Non-Light Water Reactor Mission Readiness," [4] and the "Non-LWR Vision and Strategy Near-Term Implementation Action Plans" [5]. Specifically, the guidance discussed herein supports Implementation Action Plan Strategy 3, which involves developing: (1) guidance for flexible regulatory review processes for non-LWRs within the bounds of existing regulations; and (2) a new non-LWR regulatory framework that is risk-informed and performance-based, and that features staff's review efforts commensurate with the demonstrated safety performance of non-LWR technologies. This DRG chapter also factors in the principles in Regulatory Guide (RG) 1.233, "Guidance for Technology-Inclusive, Risk-Informed, and Performance-Based Approach to Inform the Licensing Basis and Content of Applications for Licenses, Certifications, and Approvals for Non-Light-Water Reactors" [6]. RG 1.233 endorses the methodology in Nuclear Energy Institute (NEI) 18-04, "Risk-Informed Performance-Based Technology-Inclusive Guidance for Non-Light Water Reactor Licensing Basis Development," [7] with clarifications and points of emphasis.

SECY-19-0117, "Technology-Inclusive, Risk-Informed, and Performance-Based Methodology to Inform the Licensing Basis and Content of Applications for Licenses, Certifications, and Approvals for Non-Light-Water Reactors," [8] references RG 1.233 and provides a methodology for identifying licensing basis events (LBEs); classifying structures, systems, and components (SSCs); and assessing DID adequacy. Many vendors have indicated that they plan to use the

[1] The DRG was developed to address the immediate needs associated with the non-LWR community. Since the DRG is technology inclusive, it may be used for the review of LWR plant designs and other reactor technologies.

approach outlined in RG 1.233 to develop the licensing basis for their applications. In SECY-19-0009, "Advanced Reactor Program Status," [9] the staff informed the Commission that it uses the core review team approach to conduct effective non-LWR preapplication reviews. The core review team comprises specifically assigned staff members across a range of technical disciplines. This DRG may be used for a more focused review of specific areas identified by the core review team.

Thus, the NRC staff guidance discussed herein is a proactive way to modernize the I&C safety review of advanced non-LWR applications by providing guidance for technology-inclusive, risk-informed, and performance-based reviews.

X.0.1.1 Scope of Review

This DRG chapter provides guidance for the NRC staff responsible for the review of the I&C portion of license applications to help determine whether: (1) the applicant has demonstrated that there is reasonable assurance that the plant is designed to adequately protect public health and safety; and (2) the design complies with the applicable regulatory requirements. Note that some advanced reactor reviews will use a core review team approach and the I&C topics will be addressed as part of the staff's collaborations on the overall plant design and associated programmatic controls. This guide supports the I&C-related reviews as part of such a core review team approach or a more traditional matrix-type review of applications.

This DRG chapter provides review guidance on all aspects of safety-significant I&C systems, which include safety-related I&C systems and I&C systems that are not safety-related but warrant special treatment. None of the I&C systems that are not safety-related and have no special treatment are classified as safety significant, but requirements[2] may apply to such systems to ensure that failures following a design-basis or licensing basis internal or external event do not adversely impact safety-related I&C systems or I&C systems that are not safety-related but warrant special treatment in their performance of safety-significant functions. Note that the guidance described in NEI 18-04 includes a methodology for selecting and analyzing LBEs; classifying SSCs; and assessing DID that differs from traditional licensing approaches and terminology for light water reactors (LWRs). Some steps described in this guide for reviewing I&C-related topics may be performed within the broader evaluations and analyses described in NEI 18-04.

The NRC staff should use the DRG to assess whether the applicant demonstrates how the specified I&C systems support the overall nuclear power plant (NPP) performance objectives for a particular plant design. The reviewer considers the systematic assessment used in the application to assess the adequacy of the I&C architecture and systems design. The reviewer

[2] The design of digital I&C systems is governed by the legal requirements set forth in NRC regulations, including those in several of the General Design Criteria in Title 10 of the *Code of Federal Regulations* (10 CFR) Part 50, Appendix A, and 10 CFR 50.55a(h), which incorporates by reference Institute of Electrical and Electronics Engineers (IEEE) Std 603-1991. NRC guidance endorses other IEEE standards, and these IEEE standards, as well as IEEE Std 603-1991, are written in terms of so-called system, functional, performance, design, and other "requirements." These terms are well-understood in the I&C technical community, but, except as used in IEEE Std 603-1991, are not legal requirements. To avoid confusion, the DRG will use the "requirements" terminology of the IEEE standards that are not incorporated into NRC regulations in connection with references to such standards. These "requirements," as referenced in this DRG, should be understood as recommendations that NRC staff considers adequate to satisfy portions of NRC regulatory requirements, but which are not the only acceptable methods of compliance.

should consider whether the assessment provides assurance that the I&C design is reliable and robust by demonstrating that: (1) the design criteria and testing and qualification requirements have been met and (2) credible hazards and failure modes of the design are identified and controlled. Therefore, the reviewer should focus on verifying the applicable attributes of the I&C system design that support the plant level performance objectives as depicted in Figure X-1. This figure depicts a hierarchical overview of the I&C system review framework, including the I&C review boundary and the interfaces to the I&C review. The figure, however, is not intended to provide a step-by-step view of the I&C review framework; rather, it presents an overview of the technical areas to be considered during the review. The broader plant assessments may result in system level performance objectives being defined for I&C systems, which could support a more focused review of the capabilities and reliability of I&C systems.

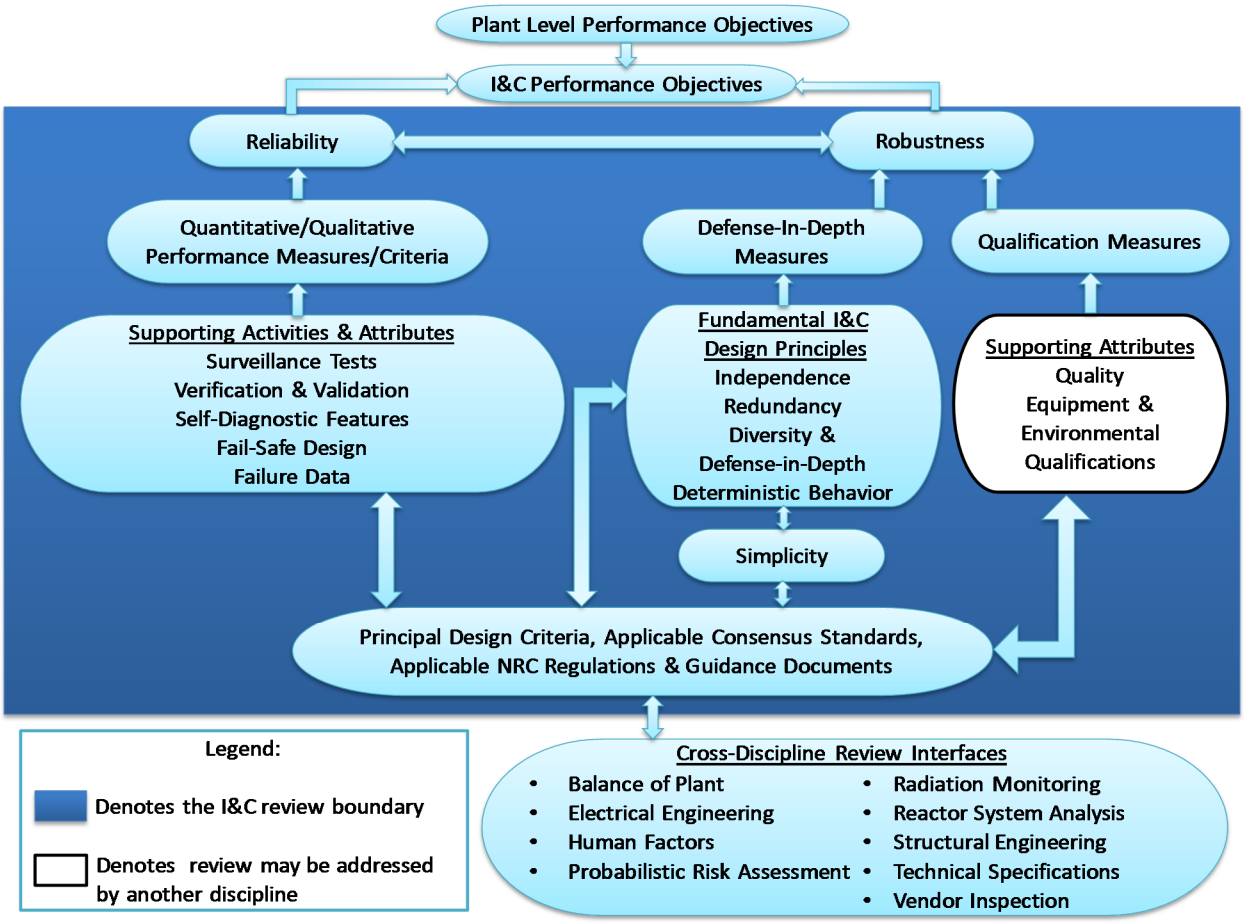

Figure X-1. I&C System Review Framework

Figure X-1 illustrates how the plant level performance objectives may result in system level performance objectives being defined for I&C systems. These I&C performance objectives should be achieved through demonstrating that the I&C architecture and systems are sufficiently reliable and robust commensurate with their safety significance:

1. "Reliability" of the I&C design is the probability that a system or component will meet its functional requirements under defined plant conditions. Reliability is achieved using quantitative and qualitative performance measures and criteria. These measures and criteria include but are not limited to surveillance tests, verification and validation, failure data, self-diagnostic features, and fail-safe design. The I&C quantitative reliability goals should be aligned with the plant's PRA and other risk assessment results.

2. "Robustness" of the I&C design is the degree to which a system or component can function correctly in the presence of invalid inputs or stressful environmental conditions. Robustness is achieved by having various measures of DID and qualification.

The I&C design should ensure that the I&C equipment or components can be qualified, procured, installed, commissioned, operated, and maintained to be capable of withstanding, with sufficient reliability and robustness, all conditions specified in the plant design basis or licensing basis.

To achieve adequate DID, the I&C architecture and systems design should meet the fundamental I&C design principles and simplicity needed to support the assessment of DID adequacy for the overall plant. Fundamental I&C design principles consist of independence, redundancy, diversity in support of DID, and deterministic behavior (predictability and repeatability). Incorporating these principles in the design facilitates addressing specific hazards within the design (e.g., fault propagation). While diversity is part of the fundamental I&C design principles, it is only considered as one means to address common cause failure (CCF). Therefore, the review guidance focuses more broadly on the diversity in support of DID assessment and other measures to address CCF.

Simplicity of the design will facilitate the NRC staff's efficient assessment of the safety of the I&C design. For example, complex I&C systems can challenge the demonstration of conformance with safety-related system design criteria such as independence. In this context, simplicity concepts support straightforward engineering analysis and testing of I&C systems to ensure that the DID measures have been appropriately implemented.

To ensure the I&C systems are qualified to function under their intended design-basis or licensing basis conditions, the reviewer should verify that the I&C system is developed with sufficient quality and applicable environmental and equipment qualification activities have been performed. The I&C reviewer provides an important role in supporting these reviews or serving as part of an integrated core review team.

The reviewer should confirm that the applicant has established the appropriate set of principal design criteria (PDC), applicable industry consensus standards, and applicable NRC regulatory guidance documents that will be used to ensure the performance measures, DID levels, and qualification measures are met. The reviewer should confirm the applicant has met the applicable regulations or requested appropriate exemptions if necessary. The reviewer should also coordinate with the appropriate cross-discipline interfaces in order to verify that any cross-discipline issues are adequately identified and resolved.

X.0.1.2 Objectives of Review

The framework depicted in Figure X-1 above supports achieving the objectives of I&C system reviews, which are to confirm that: (1) the I&C system design includes the fundamental safety functions necessary to assure adequate safety during operation of a NPP under normal operation, transient, and accident conditions; (2) the I&C system safety functions, systems, and equipment have been properly classified, and appropriate performance as well as special treatment measures have been established; and, (3) an application demonstrates I&C system and equipment will be designed, fabricated, constructed, and tested in accordance with quality standards commensurate with the safety significance of the I&C functions to be performed. When an applicant chooses to commit to an industry standard, the reviewers also evaluate whether the I&C systems and components are designed in accordance with the chosen domestic and/or international standards and via proven engineering design practices and processes.

Prior to performing the review in accordance with the DRG guidance discussed herein, the staff should review and confirm that the applicant either completed the items listed below or has a plan for completing them in support of the review. Such an approach allows the I&C staff's regulatory review to focus on safety-significant topics for the areas discussed within Section X.0.1.1:

1. The staff should confirm that there is an implemented management system by the applicant for ensuring that all requirements established for the I&C systems are considered and implemented in all phases of the development process and that the completed I&C systems meet these requirements.

2. The staff should review and confirm that the I&C systems and components are designed by the applicant in accordance with the relevant domestic and/or international standards and via engineering design best practices and processes. Furthermore, the I&C systems and components are designed so that they can be manufactured, constructed, assembled, installed, and operated in accordance with established processes that ensure the achievement of the design specifications and the required level of safety. The reviewer should consider the safety significance of SSCs in determining the level of detail of the review.

3. The staff should review and confirm that a qualification program is used by the applicant to verify that the I&C systems will reliably perform their intended safety functions when called upon to do so throughout their operational lifecycles, while considering the environmental conditions established in the design basis or licensing basis and the overall plant conditions (including maintenance and testing).

4. The staff should review and confirm that a systematic assessment is performed by the applicant to identify and evaluate the potential consequences resulting from internal and external hazards established in the design basis or licensing basis, including the potential for human induced events that directly or indirectly affect plant safety.

   As part of the systematic assessment, deterministic analyses and PRAs are performed by the applicant to ensure that all safety requirements for the I&C systems are met, including defining appropriate programmatic controls.

5. The staff should confirm that a systematic consideration of human factors is performed by the applicant, including the human–machine interface, at an early stage in the I&C design process and continues throughout the entire I&C design process.

6. The staff should confirm that digital I&C communication systems and networks are assessed by the applicant regarding hazards associated with communication paths that could affect the reliability and robustness of the system. Some technologies may not be subject to such hazards due to inherent or passive safety design features. The review should confirm that hardware characteristics that enforce unidirectional communication feature(s) (e.g., the use of a unidirectional/non-software based link that is connected to a transmitter in the higher classified system and a receiver in the lower classified system) are considered by the applicant as the preferred means for mitigating any hazard(s) associated with communication paths.

X.0.2 OVERALL REVIEW APPROACH

The staff review of a given I&C design consists of a three-tier approach as depicted in Figure X-2 below.

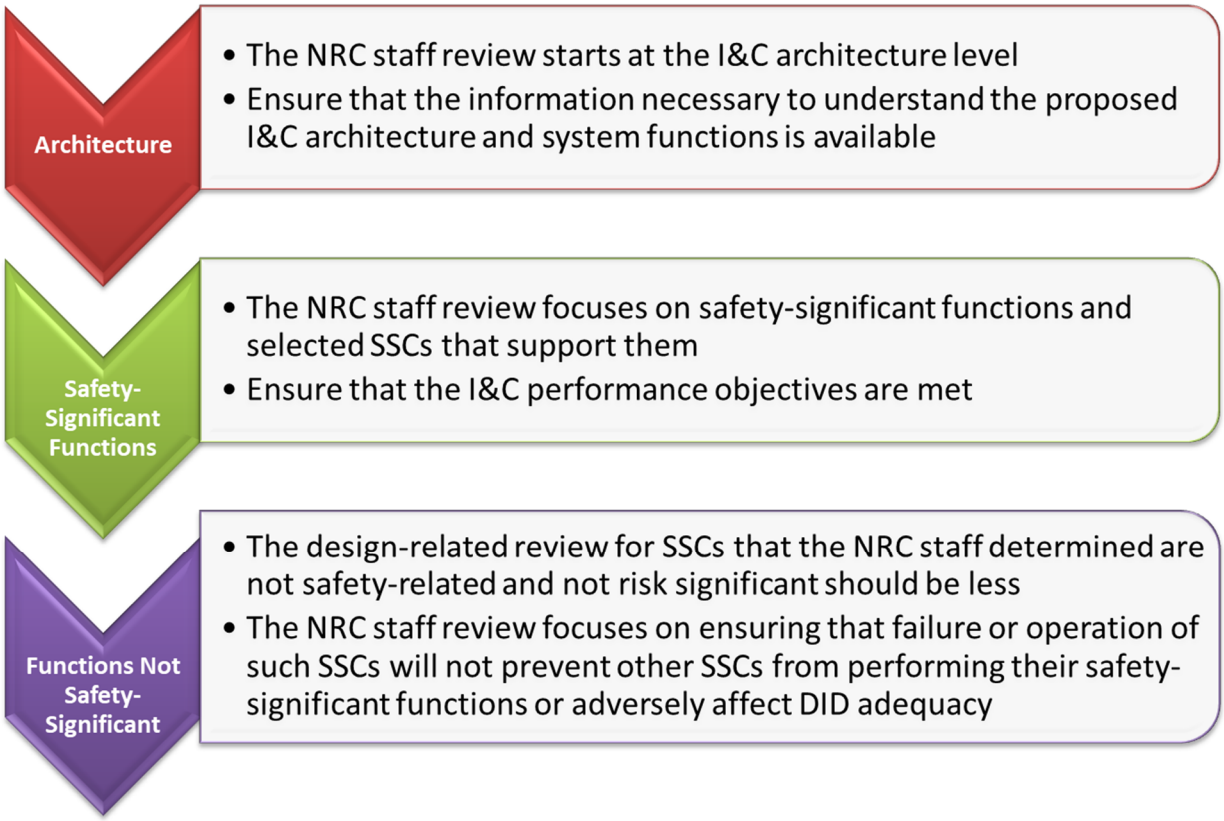

Figure X-2. Overall I&C Review Approach

This review approach begins with the staff evaluation of the proposed overall I&C architecture. In this approach, the staff should gain an understanding of the overall I&C architecture including, but not limited to, how the architecture supports the I&C system functions. Information such as one-line diagrams of the overall I&C architecture as well as functional block diagrams that show how the I&C system functions are accomplished should be available for the staff to review. Such information could be made available by the applicant during the preapplication phase.

Subsequent staff review steps should focus on those safety-significant functions and the SSCs selected to meet those functions. Safety-significant functions include those classified as risk-significant or credited for DID. The overall purpose of the staff evaluation is to confirm that the safety-significant functions, and the corresponding SSCs, adequately support the overall plant level or I&C system level performance objectives discussed in Section X.0.1.1. For SSCs the staff determines are not safety-related and do not receive special treatment, the design-related review may be less detailed or lower in depth than the review of safety-related SSCs. Specifically, the staff review focuses on ensuring that these SSCs will not adversely impact safety-related I&C SSCs and I&C SSCs that are not safety-related but warrant special treatment

in their performance of safety-significant functions. The applicable review guidance sections associated with each of the three tiers are listed in Figure X-2 above.

The level of review for a particular SSC is derived from the SSC's safety significance. The staff should review the information related to the I&C system functions that support the classification of SSCs, the SSCs selected to perform safety-significant functions, and the SSCs deemed not safety significant. The I&C staff should support a review of SSCs with other technical organizations to confirm that SSCs selected to perform safety-significant functions are appropriately addressed in the design and appropriately included within the scope of the review.

X.1 SYSTEMATIC ASSESSMENT

REVIEW RESPONSIBILITIES (as part of core review team approach or matrix assignments)

Primary - Organization responsible for the review of instrumentation and controls

Secondary - Refer to Appendix B, Table X.2-1, Cross-Cutting Review Interfaces

X.1.1 SYSTEMATIC ASSESSMENT REVIEW CRITERIA

A systematic assessment of the I&C architecture and systems design provides assurance that the I&C design is reliable and robust by demonstrating that (1) the design criteria and testing and qualification requirements have been met and (2) credible hazards and failure modes of the design are identified and controlled. The event sequences[3] considered in such a systematic assessment would help evaluate the adequacy of the level of reliability and robustness in support of the overall plant level performance objectives. The overall evaluation is derived from risk insights using deterministic analyses, PRAs, or other risk assessments. The systematic assessment methodology selected by the applicant should support the safety of the design.

A safety demonstration is one example of a systematic assessment. A safety demonstration consists of a selected set of claims on the reliability of the operation of a system that supports safety-significant functions and a structured argument supported by a body of information that provides a compelling, comprehensible, and valid case that a system is safe for a given application in a given environment. A safety demonstration is not necessarily a single document, but the totality of documents relied upon to support the safety of the design. An important part of the safety demonstration is the identification of the information that supports the claims and arguments made to support the I&C performance objectives, for example. The primary purpose of a safety demonstration is to present the claims and arguments (and supporting information) that show a system will perform its credited functions in a given context. The secondary purpose is to contribute to risk reduction by showing that all applicable hazards have been identified and adequately controlled. Hazard analysis techniques such as Systems Theoretic Process Analysis (STPA) may be used to demonstrate that hazards have been appropriately identified and controlled. Information on evaluating hazard analysis of digital safety-related systems is provided in Research Information Letter (RIL)-1101, "Technical Basis to Review Hazard Analysis of Digital Safety Systems" [10].

[3] NEI 18-04 describes a systematic process for identifying and categorizing event sequences as anticipated operational occurrences, design basis events, or beyond-design-basis events for non-LWRs. Such information is subsequently used for classifying SSCs and determining levels of regulatory treatment.

Review Procedures

The reviewer should verify that the systematic assessment of the I&C system demonstrates that the system's performance ensures the plant level performance objectives have been met. The reviewer should review the systematic assessment provided by the applicant to determine whether the assessment is complete and acceptable for demonstrating that the overall I&C performance objectives and safety requirements have been met. This review should include how the systematic assessment demonstrates that the I&C system design is robust and reliable by verifying that the I&C design adequately incorporates: 1) quantitative and qualitative measures for meeting the reliability goals; 2) DID measures, including those that support meeting the fundamental I&C design principles; and 3) qualification measures. An important element of the review is to identify uncertainties associated with the I&C system or uncertainties in plant behavior being addressed through the I&C system to ensure appropriate compensatory measures in the design or programmatic controls. The review guidance for each of these measures is provided in Section X.2 and Appendix A of this guide. Appendix A addresses review guidance associated with additional functional and design considerations for safety-related I&C systems that complement the reliability and robustness measures addressed in Section X.2.

The reviewer should verify that the selected systematic assessment methodology ensures traceability among architectural considerations and system requirements. The reviewer should verify that the systematic assessment methodology selected provides sufficient information to ensure 1) the safety requirements and design basis or licensing basis have been met; and 2) that the applicant has identified the hazards of concern and constraints to eliminate, prevent, or control them. The reviewer should verify that the application provides sufficient arguments and supporting information to support the claims (e.g., design requirements to address measures used to provide a robust and reliable design) presented in the assessment.

The reviewer should ensure that the information presented in the systematic assessment is complete, accurate, unambiguous, traceable, and verifiable. Any contextual information and assumptions that are needed to understand the systematic assessment should be reviewed. This includes information related to the I&C system design basis or licensing basis and any references to the plant design basis or licensing basis. The staff should verify that the information presented on the I&C system is consistent with the information on systems interfacing with the I&C system as shown in the cross-discipline interface review box in Figure X-1. Review guidance for cross-discipline review interfaces is provided in Appendix B of this guide.

X.1.2 ARCHITECTURE ASSESSMENT REVIEW CRITERIA

The I&C architecture for achieving the I&C performance objectives should ensure adequate NPP safety by considering concepts such as redundancy, independence, and diversity in support of DID. For example, the implementation of the DID concept for I&C is achieved mostly at the I&C architectural level by allocating I&C functions into systems belonging to different levels of defense within the I&C architecture.

The I&C architecture for the prevention or mitigation of LBEs establishes the I&C systems that comprise this architecture; the organization of these systems; the allocation of I&C functions to individual I&C systems; the definition of the boundaries among the various I&C systems; the interconnections across the I&C systems and the constraints on their respective interactions;

and the design constraints allocated to the overall I&C architecture. The architecture of individual I&C systems includes the allocation of system design requirements to functional units (e.g., divisions, processing units, human-system interfaces) and specifies the interactions between the functional units (e.g., communication links).

The overall I&C architecture and the architecture of individual systems should factor in design approaches and administrative controls to properly manage internal plant access to systems. In addition, the architecture should factor in the means for addressing the risk associated with remote electronic access to in-plant systems and networks from sources external to the plant. Such design approaches and administrative controls would ensure that digital I&C communication systems and networks are adequately protected against the potential hazards from physical and electronic access without adversely affecting the reliability and robustness of the systems.

The overall I&C architecture and architecture of individual systems should be simplified to the extent practical. The staff considers simplicity to be a cross-cutting concept that supports the fundamental I&C design principles discussed in Section X.0.1.1 for developing I&C systems with high reliability. Compared to simple systems and architectures, it is more difficult to demonstrate that complex I&C systems and architectures conform to fundamental I&C design principles such as independence; however, it is difficult to define and control simplicity and complexity. But from a safety perspective, the simpler design options are those that accomplish the safety function and address potential hazards while exhibiting the following properties: (1) the I&C system architecture design is as simple as practical; (2) any added complexity provides a safety benefit; and (3) any added complexity does not diminish the design's conformance to the fundamental I&C design principles. As such, designs that incorporate this concept will facilitate the staff's efficient I&C architecture evaluation.

The reviewer should consider the I&C system overall architecture in concert with the sections relating to the fundamental I&C design principles discussed in Section X.2.2.1. In addition, the reviewer should consider other sections of the review guide that discuss the I&C system design basis or licensing basis, the I&C system descriptions, and the I&C system functions for consistency and additional information.

The reviewer should use engineering judgment to verify that the application includes sufficient information at the architectural level to support a more streamlined review of the fundamental I&C design principles. The I&C architecture should complement and support the I&C systems' conformance with the fundamental I&C design principles.

Review Procedures

The staff should review, as a minimum, the following information, which the application should include:

1. Description of the overall I&C architecture and the architecture of individual I&C systems supporting the I&C performance objectives.

    A. The application should provide sufficient information to demonstrate that the overall architecture proposed is sufficiently robust and reliable. For example, the architecture description should demonstrate that the architecture reflects the fundamental I&C design principles.

B. The architecture description of each individual I&C system should:

   a. Include the I&C functions allocated to the system that support implementation of the overall I&C architecture design;

   b. Identify the redundancy (e.g., divisions) within each safety-related system to support meeting the single-failure criterion (if applicable) and;

   c. Identify all physical and logical interfaces and the purpose of each interface. This includes any direct and indirect interfaces (e.g., direct pathways, indirect pathways through logical connections).

2. I&C functions that are part of the design basis or licensing basis and the design strategies to be applied to achieve the reliability and robustness necessary for each safety function allocated to each individual I&C systems within the overall I&C architecture. The design strategies for achieving I&C system reliability may include redundancy, independence between redundant portions of safety-related systems and between the safety-related systems and the systems that are not safety-related, fail-safe design, and diversity.

3. Diagrams of the overall I&C architecture. These diagrams should illustrate the I&C system architecture principles and concepts (as addressed in Item 1 above). The staff review should ensure that sufficient detail is provided as follows.

   A. Physical architectural diagrams to include:

      a. all of the safety-related I&C systems and all the I&C systems that are not safety-related;

      b. connections between the above systems;

      c. interfaces and means of communications between the individual I&C systems;

      d. identification of signal and isolation devices.

   B. Functional block diagrams to include:

      a. major components from sensor(s) to actuation device(s), including various channels and divisions used for signal and data processing, voting unit(s) and actuation devices;

      b. signal and data flow paths.

4. Information necessary to support the DID concept to be implemented for the plant, which provides layers of defensive capabilities to prevent or mitigate potential hazards, including the following:

   A. the I&C systems, including their classification, technologies, boundaries, and interfaces with other systems;

B. end-to-end signal flows and their descriptions (e.g., signal flow paths from sensor input through signal conditioning, data processing, voting, and actuation);

C. key functional blocks that make up the I&C architecture, through which the data (plant process information or command signals) are transmitted and their descriptions;

D. simplified logic diagrams;

E. signal processing block diagrams and their descriptions;

F. when the design includes a prioritization scheme that is used to signal selections, the priority functions, diagrams, and their descriptions;

G. interfaces and comparisons of electrical and I&C diagrams and;

5. Specific constraints identified in the I&C design resulting from the general plant safety approach that could affect compliance with regulatory requirements (e.g., if plant system(s) specifically addressed in regulations or guidance are used in a manner different from that described in the regulations or guidance, or not used at all in the reactor design due to the general plant safety approach, the application should describe those differences and their impact on the overall I&C design should be identified).

6. Indications and operator controls that are needed for safety-significant functions during normal operation, transient, and accident conditions.

7. The rationale, justification, or reasoning behind architecture choices, including potential consequences of such choices.

X.2 REVIEW CRITERIA

REVIEW RESPONSIBILITIES (as part of core review team approach or matrix assignments)

Primary - Organization responsible for the review of instrumentation and controls

Secondary - Refer to Appendix B, Table X.2-1, Cross-Cutting Interface Reference

X.2.1 RELIABILITY

The reliability necessary for the overall I&C system depends upon the safety significance of the system's functions. Therefore, I&C systems or components should be designed for a reliability level that is commensurate with the safety significance of the function(s) to be performed. RG 1.233 provides guidance for the SSC function classification process for non-LWRs. Examples of design attributes for achieving a given level of functional reliability include those related to failure data, fail-safe behavior, independence, redundancy, diversity, failure detection, periodic testing, use of self-diagnostic features, surveillance tests, maintainability, and service life. Verification and validation should be included at appropriate stages of the I&C design to confirm that the necessary safety functions have been identified and can be reliably performed when called upon to do so.

The application should provide adequate information for the staff to evaluate whether the proposed I&C design meets its reliability goals via the use of qualitative or quantitative performance measures or criteria. These performance measures and criteria can be used to optimize goals such as minimizing outage time for repair and reducing the frequency of surveillance. The application should also identify programmatic controls needed to address uncertainties and ensure desired reliability.

Software faults may result from design errors and therefore, do not have the random failure behavior assumed in the analysis of hardware reliability. Consequently, the analysis may address different methods to assess the unreliability introduced by software and hardware, respectively. For example, the reliability of digital-based I&C systems may be demonstrated on the basis of a combined quantitative and qualitative evaluation (see Sections X.2.1.1 and X.2.1.2), with account taken of the complexity of the design, the quality of the system, verification and validation, and testing during the development process over a wide range of input conditions, and the feedback of operating experience.

X.2.1.1 Qualitative Performance Measures/Criteria

The overall I&C systems should be designed to perform safety-significant functions credited in the final safety analysis report (FSAR) with adequate reliability to address identified hazards. The reviewer should confirm that the I&C systems are designed to fail in a safe state, or into a state that has been demonstrated to be acceptable on some other defined basis, and potential failure modes are identified using a formal analysis. Potential failure modes may include single random failures, CCFs, etc. Formal analyses of the identified hazards should include a qualitative evaluation with such goals as discovering the fault propagation paths in the I&C systems to determine the root causes of a potential failure mode or cause, and to identify the best ways to minimize the associated risk.

Review Procedure

The reviewer should verify that the necessary level of reliability for each I&C system has been achieved for its intended safety-significant functions and supports the overall plant level performance objectives. The reviewer should verify that the application identifies the method(s) used to determine the reliability of each I&C system for each safety function, along with the qualitative performance measures or criteria imposed on the system design. For example, the reliability of an I&C system may be demonstrated on the basis of a qualitative evaluation that takes into account the complexity of the design, the design process, the rigor of the verification and validation activities applied to the system over a wide range of input conditions, and the feedback from applicable operating experience.

The reviewer should verify that the applicant has identified potential hazards in the I&C system that could challenge plant safety and provided adequate hazard controls to either prevent, eliminate, or mitigate each identified hazard. The identified hazards, corresponding controls, and the technique used to identify each hazard should be documented. The reviewer should examine the technique used for hazard identification and control to verify that it is appropriate to accomplish the above applicant's tasks and that any limitations to the technique have been identified by the applicant. This information can be included as part of the overall systematic assessment.

X.2.1.2 Quantitative Performance Measures/Criteria

The overall I&C system quantitative reliability goals should support the overall plant level performance objectives as determined via the PRA results or other risk assessments. The reviewer should determine whether the analysis in the application demonstrates that the overall I&C system quantitative reliability goals supporting the overall plant level performance objectives are achieved using appropriate methods. The analysis should account for the overall I&C design architecture and the effect of failures of individual components and systems as appropriate.

Review Procedure

The reviewer should evaluate the overall I&C system analysis provided by the applicant and verify that the methods used to demonstrate its reliability are acceptable. As part of this review, the staff should verify that: (1) the I&C system modeling in the analysis includes the system description, key assumptions, and failure effects and description of the event sequences following the failure; and (2) the overall I&C design architecture and function allocation support the assumptions in the I&C system modeling. If the system includes digital components, the staff should verify that the I&C system modeling includes potential failures of the hardware and software of the digital components, as well as the design features provided to prevent the failures or to mitigate or minimize their effects.

The reviewer should evaluate whether the hardware failure conditions to be considered in the analysis include failures of parts of the I&C system and failures of parts of the data communication systems (e.g., missing data, errors in the data). The reviewer should evaluate whether the contribution of component failure to an I&C system's unavailability has been determined to an appropriate degree of confidence (e.g., by a specified confidence level when a probabilistic-based approach is used). The reviewer should also evaluate whether the information (e.g. operating history, failure data for random failures and CCFs, statistical testing) used to support the assessment is complete.

X.2.2 ROBUSTNESS

"Robustness" of the I&C design is the degree to which an I&C system or component can function correctly in the presence of invalid inputs or stressful environmental conditions. A robust I&C design reflects the use of design methods and adherence to engineering best practices to ensure that the safety functions are achieved for all operational states and accident conditions. As such, the I&C design requirements for safety-significant SSCs should address robustness for the full range of operating environments associated with normal operation, transient, and accident conditions, as well as foreseeable internal and external hazards.

X.2.2.1 Defense-in-Depth Measures

Robustness is achieved via qualification measures, such as testing, analysis, or testing in combination with analysis, and by having various measures of DID, which are implemented by adhering to the fundamental I&C design principles. The degree of DID and qualification measures should be justified as being adequate to achieve the necessary robustness and reliability of the safety functions to be performed by the systems. Such demonstration may be based on a balance of deterministic criteria and qualitative or quantitative reliability analysis (see Section X.2.1). The reviewer should verify that the design does not include unnecessary

functions and interfaces that could challenge conformance to the fundamental I&C design principles.

X.2.2.1.1 Independence

Sufficient independence should be incorporated into the I&C design and preserved throughout the life of the NPP to prevent: (1) propagation of failures from systems that are not safety-related to safety-related systems; and (2) propagation of failures between redundant portions within a safety-related system. Furthermore, sufficient independence should be incorporated to ensure the effectiveness of the redundancy and diversity in the I&C design for maximizing the reliability of systems that support safety-significant functions, despite the potential for CCFs.

Review Procedures

The objective of the staff review is to evaluate the methods described in the application used to demonstrate independence of: (1) the redundant portions of a safety-related I&C system such as redundant safety divisions; (2) safety-related systems from one another; and (3) the safety-related systems from systems that are not safety-related. Where appropriate, the staff review should also assess the role of independence in I&C systems that are not safety-related but warrant special treatment. The reviewer should evaluate the physical and logical interfaces for the I&C system design, including the specific data sent, the purpose of the data, and the means of sending the data (e.g., hardwired or data communications). This review should include not only permanent interfaces but also temporary connections (e.g., for maintenance workstations).

The reviewer should evaluate whether there is sufficient physical separation, electrical isolation, communications independence, and functional independence as follows:

1. The reviewer should verify the physical separation of redundant portions of safety I&C systems and the physical separation between safety I&C systems and systems that are not safety-related. The reviewer should verify that the design will have sufficient physical separation or barriers between equipment belonging to (1) redundant portions of a safety-related system such as redundant safety divisions; (2) different safety-related systems; and (3) safety-related systems and systems that are not safety-related, such that the safety functions credited during and following any LBE can be accomplished. The reviewer should verify whether the design contains any associated circuits and ensure any identified associated circuits cannot degrade the safety-related equipment. (“Associated circuits” are circuits that are not safety-related and are not physically separated (e.g., via barriers) or are not electrically isolated (e.g., via isolation devices) from safety-related circuits).

2. The reviewer should evaluate whether there is sufficient electrical isolation between equipment belonging to (1) redundant portions of a safety-related system such as redundant safety divisions; (2) different safety-related systems; and (3) safety-related systems and systems that are not safety-related, such that an electrical fault originating from one safety division or equipment that is not safety-related will not adversely impact a safety function. The reviewer should verify that any electrical isolation devices or measures installed to prevent electrical fault propagation are qualified as part of the safety-related system.

3. The reviewer should evaluate whether there is sufficient communications independence between equipment belonging to (1) redundant portions of a safety-related system such

as redundant safety divisions; (2) different safety-related systems; and (3) safety-related systems and systems that are not safety-related, such that communications failures originating from outside a safety division cannot adversely impact the safety function. This evaluation should include identification of potential failures in the communications mechanism and information that is being communicated, and verification that adequate controls have been implemented to address these potential failures. The reviewer should verify that no safety division is adversely influenced by information received from outside the safety division. This includes verifying that spurious actuations of I&C equipment due to credible failures, or consequential actions of systems that are not safety-related, will not adversely impact the safety function. The reviewer should verify that sufficient measures (e.g., use of buffer mechanisms) are implemented to minimize the possibility of fault propagation and to increase the reliability of the information being communicated.

4. The reviewer should verify there is adequate functional independence, if needed, between equipment belonging to (1) redundant portions of a safety-related system such as redundant safety divisions; (2) different safety-related systems; and (3) safety-related systems and systems that are not safety-related, such that a safety division does not rely on information from outside the safety division to perform its safety function. To reduce the potential hazards associated with resource sharing, functions that are not necessary for safety should be executed outside the safety-related system.

X.2.2.1.2 Redundancy

RG 1.233 endorses the methodology described in NEI 18-04, which replaces the single-failure criterion with a probabilistic (reliability) criterion. Application of the single-failure criterion under the NEI 18-04 methodology may not be necessary because some advanced non-LWRs designs employ a diverse combination of inherent, passive, and active design features to perform the credited safety functions across layers of defense. Such designs will be subjected to an evaluation of DID adequacy.

Applicants for a non-LWR design that derive the design basis or licensing basis for the design using an alternative to the NEI 18-04 methodology would need to maintain, or justify not applying, the single-failure criterion in analyses of safety-related systems.

When evaluating application of the single-failure criterion, the reviewer should evaluate the level of redundancy used in the safety-related system to assure that: (1) no single failure results in loss of the safety function and (2) removal from service of any component or channel does not result in loss of the minimum redundancy credited in the FSAR unless the acceptable reliability of operation of the I&C design can be otherwise demonstrated.

Review Procedures

The NRC staff conducts a review of design information, including functional block diagrams, descriptions of operation, architectural descriptions, and other design details, and the reviewer should confirm that the application provides information sufficient to address the single-failure criterion.

In addition to addressing the single-failure criterion, the design should include sufficient redundancy to enable (1) system testing and (2) component bypass or removal from service

without loss of function. Additional redundancy may be warranted when I&C systems share common components.

The reviewer should consider the following when assessing redundancy:

1. The application should address the single-failure criterion, if applicable, and the I&C architecture description should describe how redundancy is implemented in the I&C system design. The application may address the single-failure criterion via identifying potential single failures in the system as part of the safety I&C system hazard analysis and using measures such as redundancy to address the identified single failures.

2. The reviewer should confirm that: (1) the application includes an evaluation of the effects of each component failure mode on the overall system; (2) any component failure mode that could contribute to a failure of the safety-related system is identified; (3) the design of a safety-related system precludes single failures from resulting in spurious actuations or in unacceptable safety consequences; and (4) necessary action is taken to eliminate, prevent, or control failure modes.

3. The reviewer should confirm that the application provides information sufficient to demonstrate that all SSCs needed for safe shutdown, as defined for each facility, are sufficiently redundant to address the single failure criterion, if applicable. The use of shared data networks (e.g., ring networks) among multiple safety divisions as single paths for multiple signals or data raises concerns about extensive consequential failures as the result of a single failure. This review should confirm that channel assignments to individual communication networks or links can ensure that adequate redundancy within the supported systems is maintained.

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 in the digital I&C system could disable a safety function; and (2) a diverse means 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 that the 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. 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:

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

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 CCF vulnerabilities from further consideration should be demonstrated.

8. Provision of a set of displays and controls located in the main control room, or in a location that supports the operator needs based on a human factors engineering analysis, 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 measures are used to eliminate the CCF from further consideration, the application -should include a supporting technical basis and acceptance criteria for the use of the defensive measure.

X.2.2.1.4 Predictable and Repeatable Behavior

Safety-related I&C systems should be designed to operate in a predictable and repeatable manner. “Predictable” is defined as the ability to determine the output of a system at any time through known relationships among the controlled system states and credited responses to those states, such that a given set of input signals will always produce the same output signals. “Repeatable” is defined as the output of a system being consistently achieved given the same input and system properties (including internal and external conditions). The reviewer should evaluate the methods described in the application to demonstrate that the output for the I&C system that supports safety-significant functions is predictable and repeatable.

The reviewer should evaluate whether the I&C systems (including digital I&C and data communications systems) are designed to operate in a predictable and repeatable manner. The objective of this review is to: (1) verify that the assumed system timing derived from the analysis of transient and accident conditions has been allocated to the I&C system architecture, as appropriate, and has been satisfied in the I&C system design; (2) confirm that the I&C system design and communication protocols provide features to assure that the system (or logic) produces the correct response to inputs within the time credited to produce a response; and (3) confirm that hazards that could challenge predicted behavior have been adequately identified and accounted for in the design.

Review Procedures

Through a review of design information, including functional block diagrams, descriptions of operation, architectural descriptions, and other design details, the reviewer should confirm that the application demonstrates that systems credited to perform safety-significant functions will perform those functions within the time credited in the FSAR.

The timing of specific system responses credited in the safety analysis may affect the system architecture, because it may not be possible to obtain sufficient computational performance for a specific function or group of functions from a single processor, or the locations where functions are performed may be widely separated. Features used to achieve correct timing of credited actions may also increase complexity, for example, fragmenting the system into multiple processors, makes the software product (or logic) more difficult to understand, verify, and maintain. Note that a typical attribute of advanced reactors is a larger system heat capacity and slower thermal time constant, which may significantly reduce the importance of quick response times for I&C systems, related performance of mitigation systems, and human actions.

The reviewer should confirm that the application provides a detailed timing analysis describing how the I&C systems that support safety-significant functions, including supporting communication systems, address the concept of predictability and repeatability.

The reviewer should confirm that the application provides sufficient information (for example, in the form of architectural descriptions, functional block diagrams, descriptions of operation) to demonstrate that the proposed digital I&C system's real-time performance is predictable and repeatable. This evaluation should include verifying that:

1. The digital I&C system timing analysis identifies limiting response times, digital system timing requirements, architecture, and design constraints

2. The digital I&C system timing analysis addresses all system components from signal collection to completion of protective action (e.g., sensor, transmitter, logic processor, data communication equipment, etc.)

3. The timing of specific system responses credited in the safety analysis has been allocated to the digital logic portion of the system, as appropriate, and has been satisfied in the digital system architectural design

4. The digital I&C system timing analysis demonstrates that the safety-significant functions are achieved within the times credited in the safety analysis

5. Data communications in support of the safety-significant functions operate in a predictable and repeatable manner (e.g., data communication is cyclic, no event driven data communications, fixed-size and pre-defined data packets)

6. Design practices that do not implement a digital I&C system's real-time performance that is predictable and repeatable are documented. For those practices identified, verify that: (1) the methods used for assessing the risk associated with such design practices have been documented; (2) such practices cannot adversely affect any safety-significant functions; and (3) the design does not adversely impact any safety-significant function

7. Logic processing units are monitored by an independent hardware-based, diverse means that produces a trip in the affected redundant portion of the system if the logic processing unit ceases operation or "locks-up" (i.e., ceases to respond)

X.2.2.2 Qualification Measures

Qualification is the process of identifying hazards in the environment in which the I&C systems and equipment may be operating and conducting tests or analyses or both to determine whether

the credited safety-significant functions can be reliably performed under the specified service conditions. Therefore, qualification measures should confirm that the I&C systems and equipment will be capable of reliably performing the design-basis functions for which they are credited over the range of environmental conditions postulated for the area in which they are located.

X.2.2.2.1 Quality

Design and manufacturing methods and practices should be of sufficient quality to ensure that I&C systems can reliably perform their credited safety functions. As such, the application should provide information to confirm that I&C system equipment will be designed, developed, fabricated, and tested to quality standards commensurate with the safety significance of the functions to be performed. The scope of this section covers I&C systems that support safety-significant functions.

Review Procedures

The application should describe the methods and practices for the planning, design, development, integration, testing, operation, maintenance, and retirement of I&C systems, including those relating to hardware and software engineering. The application should describe how these activities will be coordinated with organizational and project management processes, which include configuration management, reviews/audits, validation and verification, quality assurance (QA), and procurement. Such coordination should assure adherence to appropriate standards and procedures.

The staff organization responsible for the review of QA evaluates the applicant's QA program description for the overall NPP. I&C systems development, including hardware and software, should be performed under the QA program for the overall NPP and should meet applicable regulatory requirements. The I&C reviewer should assess the framework that will be used to design and develop I&C systems with assistance from the organization responsible for the QA review. Specifically, the I&C reviewer should confirm that this framework supplements the applicant's overall QA program descriptions with specific system, hardware, and software development activities, including a description of the proposed development life cycles and management activities that will be implemented in the design and development of I&C safety-related systems.

The I&C reviewer should verify that the applicant has defined the activities that will be performed for each stage of the I&C safety-related system life cycle (or the life cycles of I&C systems that are not safety-related but warrant special treatment) and the outputs that will be generated from these activities. If portions of the I&C safety-related system will be commercially dedicated, the organization responsible for the QA review, with support from the I&C reviewer, should confirm the dedication process and activities meet applicable NRC requirements for commercial grade dedication.

X.2.2.2.2 Equipment Qualification

Equipment qualification should demonstrate that the equipment is capable of functioning under environmental and operational conditions. As such, the application should provide information to confirm that I&C system equipment that performs safety-significant functions is designed to perform the functions for which the equipment is credited in the safety analysis over the range of environmental conditions postulated for the area in which it is located.

The I&C review of equipment qualification is limited to confirmation that: (1) I&C equipment, including isolation devices, located in areas subject to seismic and environmental qualification requirements has been identified and design criteria established in the application; (2) criteria specific to qualification of digital I&C system equipment have been met; and (3) the I&C system design includes design requirements for safety-related instrument sensing lines and lightning protection systems.

Review Procedures

1. Equipment Qualification

   The I&C technical review should be coordinated with the review of the seismic and environmental qualification programs and the review of the list of equipment that is subject to qualification.

   The reviewer should confirm that I&C system equipment performing safety-significant functions is designed to perform the functions for which they are credited over the range of environmental conditions for the area in which it is located. The I&C reviewer should confirm that the I&C equipment, including isolation devices and digital equipment, subject to seismic and environmental qualification requirements has been identified, and design criteria to govern the equipment qualification established in the application.

2. Instrument Sensing Lines

   Design of the instrument sensing lines and selection of the tap locations should allow these components to perform the safety-significant functions for which they are credited in the FSAR over the range of environmental conditions for the area(s) in which they are located (e.g., slope, tube diameter, pipe/tube classification, and heat tracing). The I&C reviewer should confirm that the application identifies the design functions of the instrument sensing lines and establishes the associated design criteria.

3. Environmental Control Systems

   If environmental control systems are relied upon in support of a safety-significant function, the application should provide information to confirm that a single failure within the environmental control system will not result in conditions that could result in damage to the safety-related system equipment. The reviewer should confirm that the use of environmental control systems will protect safety-related instruments and instrument sensing lines from freezing. In this regard, the loss of an environmental control system in any area in which safety-related equipment is located is treated as a single failure, which should not prevent the safety-related system from accomplishing its safety functions.

   The design basis of environmental control systems may rely upon monitoring environmental conditions. In the event of environmental control system malfunction, the design may take credit for appropriate action to ensure that environmental conditions are maintained within predetermined limits within which system or component damage will not occur during the period until the environmental control systems are returned to normal operation. In such cases, the reviewer should verify that sufficient information is provided in the application to confirm that the environmental control systems are

independent from the sensing systems credited to indicate the failure or malfunctioning of environmental control systems.

4. Electromagnetic and Radio-Frequency Interference (EMI/RFI)

   The I&C reviewer should determine whether the EMI/RFI qualification conforms to the existing regulatory guidance on design, installation, and testing practices for addressing the effects of EMI/RFI, electrostatic discharge, and power surges on safety-related I&C systems. The reviewer should also confirm that lightening protection has been addressed as part of the review of electromagnetic compatibility.

X.3 MAPPING TO REGULATIONS AND GUIDANCE

REVIEW RESPONSIBILITIES (as part of core review team approach or matrix assignments)

Primary - Organization responsible for the review of instrumentation and controls

Secondary - None

In addition to reviewing the I&C systems design by following the approach discussed in Sections X.1 and X.2 above, the reviewer should also assess whether the design complies with the applicable regulatory requirements. This includes the PDC established by the applicant for the particular design and the applicability of these PDC to I&C systems. Such an approach would help the reviewer determine whether the applicant has demonstrated that the I&C design is acceptable as part of the basis for a staff finding that there is reasonable assurance that the design and associated programmatic controls adequately protect the public health and safety.

The reviewer should confirm that the application provides sufficient information to allow the reviewer to: (1) determine which regulatory requirements apply to a particular design; (2) understand how the applicable regulatory requirements are met (guidance, industry standards, methodologies, etc. used to meet requirements); and (3) explain exemptions, if any, taken from the applicable regulatory requirements. The reviewer should verify that the application demonstrates that regulatory requirements are met through (1) conformance to an applicable regulatory guide; or (2) use of other means (e.g. conformance to international consensus standards).

Appendix A contains review guidance on topics that are addressed by the safety-related system design criteria within Institute for Electrical and Electronics Engineering (IEEE) Standard (Std) 603-1991, “Standard Criteria for Safety System for Nuclear Power Generating Stations.” IEEE Std 603-1991 has been incorporated by reference in 10 CFR 50.55a(h)(3) as a requirement for construction permits and operating licenses under 10 CFR Part 50 and for design approvals, design certifications, and combined licenses under 10 CFR Part 52. An applicant can propose alternatives to the requirements in this standard under the conditions specified in 10 CFR 50.55a(z), “Alternatives to Codes and Standards Requirements.” The reviewer should confirm whether the application (1) meets the requirements within IEEE Std 603-1991 or (2) proposes an alternative that meets the requirements of 10 CFR 50.55a(z).

Note that advanced non-LWRs will likely rely less on active features (e.g., pumps and valves powered by electrical motors) but more on inherent or passive safety features to perform safety functions. In addition, the overall risk profile of the non-LWRs will also be significantly different. Therefore, the staff anticipates that some applicants will propose alternatives to elements of IEEE Std 603-1991 in accordance with 10 CFR 50.55a(z).

APPENDIX A SYSTEM CHARACTERISTICS

Introduction

This appendix addresses review guidance associated with additional functional and design considerations for safety-related I&C systems. The characteristics discussed below address specific functional and design requirements for safety-related I&C systems (and I&C systems that are not safety-related but warrant special treatment), including system criteria, sense and command features, and execute features that complement the reliability and robustness measures addressed in Section X.2.

Relevant Information to Support Consideration of System Characteristics during Design Review

A.1 Operating and Maintenance Bypasses

The reviewer should evaluate the operating and maintenance bypasses for safety-related I&C systems. The specific review criteria for operating and maintenance bypasses are as follows:

Operating Bypasses

The review should focus on evaluating how the safety-related I&C system design includes measures to address operating bypasses. The reviewer should verify the following:

1. If the applicable permissive conditions are not met, the safety-related system automatically prevents the activation of an operating bypass or initiates the appropriate safety function.

2. If plant conditions change such that an active operating bypass is no longer permissible, the safety-related system either removes the active operating bypass, restores plant conditions to the permissive conditions, or initiates the appropriate safety functions. Automatic removal of active bypasses means that the reactor operator may not have a role in such removal; however, the operator may take action to prevent the unnecessary initiation of a protective action.

3. Indication of bypass and inoperable status is automatically provided in the control room.

Maintenance Bypass

The reviewer should focus on evaluating how the safety-related I&C system design includes measures to address maintenance bypasses. The reviewer should verify the following:

1. While sense and command features equipment is in maintenance bypass, the capability of a safety-related I&C system to perform its safety functions is retained. Additionally, Technical Specification (TS) action statements are consistent with the provisions for maintenance bypass.

2. When a portion of the system is placed in maintenance bypass, the remaining portions of the system provide acceptable reliability or meet the single failure criterion.

3. Indication of bypass and inoperable status is automatically provided in the control room.

If the reviewer confirms that the application conforms to the guidance identified above, the staff can conclude that the application provides sufficient information to demonstrate that: (1) the design of operating and maintenance bypasses ensures the initiation of the appropriate safety function(s) under the conditions described above; (2) the proposed TS accurately reflect the effects of operating and maintenance bypasses on system functions credited in the safety analyses; and (3) adequate indication for bypass status is provided in the control room. If the application proposes a different method for achieving any one of these functions, the reviewer should review the method on a case-by-case basis.

A.2 Interlocks

The reviewer should evaluate the acceptability of I&C and mechanical interlocks that: (1) operate to reduce the probability of occurrence of specific events; (2) maintain variables within the ranges of values specified in the safety analyses; (3) assure proper system alignment during plant operation; and 4) maintain safety-related systems in a state that assures their availability in an accident.

I&C Interlocks

The reviewer should evaluate all proposed I&C interlocks to ensure that the applicable requirements in the following areas are met: redundancy, independence, single failure criterion, qualification, bypasses, status indication, and testing. Although the primary I&C review emphasis is on equipment comprising the interlocks, the reviewer should consider the interlock functions at the system level.

Mechanical Interlocks

The I&C reviewer should confirm the adequacy of all proposed I&C associated with mechanical interlocks. Examples of these types of interlocks may include: (1) interlocks to prevent overpressurization; (2) interlocks related to heat removal function(s); (3) interlocks to isolate safety-related systems from systems that are not safety-related; and (4) interlocks to preclude inadvertent inter-ties between redundant or diverse systems that perform safety-significant functions.

If the reviewer confirms that the application conforms to the guidance identified above, the staff can conclude that the application provides information sufficient to demonstrate that the design incorporates interlocks that: (1) operate in a manner to reduce the probability of occurrence of specific events; (2) maintain variables within the ranges of values specified in the FSAR; (3) assure proper system alignment during plant operation; and (4) maintain systems that perform safety-significant functions in a state that assures their availability in an accident. If the application proposes a different method for achieving any one of these functions, the reviewer should review the method on a case-by-case basis.

A.3. Derivation of System Inputs

The I&C reviewer should evaluate the methods described in the application used for the derivation of system inputs to ensure, to the extent feasible and practicable, that sense and command feature inputs are derived from signals that are direct measures of the variables specified in the design basis. For example, a system that provides protection from loss of flow would normally derive its signal from flow sensors; however, a design may use an indirect parameter such as pump speed as a surrogate for system flow rate. In this example, the

reviewer should confirm whether the application identified flow sensors signal as the input for the flow measurement or justified why the indirect parameter is acceptable.

The guidance provided below should be used to review the acceptability of information associated with derivation of system inputs:

1. The reviewer should focus on examining documentation such as the safety-related I&C system design basis, safety-related I&C system architecture, or logic diagrams that show sense and command feature inputs and measured variables for applicable systems.

2. The reviewer should confirm that system inputs are, to the extent feasible and practicable, derived from signals that are direct measures of the desired variables that reflect the physical processes of interest, as specified by the design bases.

3. The reviewer should confirm that, if indirect parameters are used, the indirect parameter is a valid representation of the corresponding direct parameter for all evaluated events.

4. The reviewer should confirm that, for both direct and indirect parameters, the characteristics of the instruments that produce the safety-related I&C system inputs, such as range, accuracy, resolution, response time, and sample rate, correctly reflect the applicable analyses provided.

If the reviewer confirms that the application conforms to the guidance identified above, the staff can conclude that the application provides information sufficient to demonstrate that sense and command feature inputs are derived from signals that are, to the extent feasible and practicable, direct and indirect measures of the variables specified in the design basis. If the application proposes a different method for achieving any one of these functions, the reviewer should review the method on a case-by-case basis.

A.4 Setpoints

The reviewer should evaluate the methodology that establishes the setpoint values that are assigned to the I&C systems and components that perform automatic protective actions. The setpoints of concern in this review include: (1) setpoints specified for process variables on which safety limits (SLs) have been placed or a process variable that functions as a surrogate for one on which an SL has been placed; and (2) setpoints related to process variables associated with safety-significant functions but do not protect any SLs.

The reviewer should have a thorough understanding of the relationships between nominal trip setpoints, limiting trip setpoints, as-left values and as-found values, as-left and as-found tolerances, analytical limits (ALs) and SLs to ensure that the terms are properly utilized in the establishment of the setpoints.

The reviewer should verify the following when evaluating the setpoint methodology:

1. The methodology accounts for all uncertainties in each setpoint analysis and properly identifies all analysis terms.

2. The established calibration intervals and methods are consistent with the safety analysis assumptions and are accurately reflected in the TS.

3. Each setpoint analysis demonstrates that an adequate margin exists between setpoints and ALs or normal process limits (to be used as a starting point in calculations for variables with no related SL or AL).

4. The analysis demonstrates that an adequate margin exists between operating limits and setpoints to avoid inadvertent actuation of the system.

If the reviewer confirms that the application's setpoint methodology conforms to the guidance identified above, the staff can conclude that the application provides information sufficient to establish setpoints that: (1) are adequate to assure that protective actions are initiated before the associated plant process parameters exceed their ALs or nominal process limits; (2) are adequate to assure that control and monitoring setpoints are consistent with their system specifications; and (3) confirm that the established calibration intervals and methods are consistent with the safety analysis assumptions and are accurately reflected in the TS. If the application proposes a different method for achieving any one of these functions, the reviewer should review the method on a case-by-case basis.

A.5 Auxiliary Features

The review of I&C systems relied upon for functionality of auxiliary features is composed of evaluating both auxiliary supporting features and other auxiliary features. Auxiliary supporting features are systems or components that perform a function that safety-related systems rely on to accomplish their associated functions. Other auxiliary features are defined as systems or components that perform a function that is not needed for the safety-related I&C system to accomplish its safety function and are part of the safety-related I&C systems by association because these features cannot be isolated from the safety-related system.

The reviewer should verify the following when assessing auxiliary features:

1. The application identifies and describes all auxiliary features proposed in the design. These features may be described in other chapters of the application.

2. Safety-related I&C system controls, instrumentation, and signals relied upon for proper operation of auxiliary supporting features, including isolation signals, under abnormal conditions such as accident conditions are adequate.

3. Any feature identified as an other auxiliary feature is designed to meet applicable functional and design criteria to ensure the feature does not prevent the safety-related system from performing a credited function.

If the reviewer confirms that the application conforms to the guidance identified above, the staff can conclude that the application provides information sufficient to demonstrate that: 1) auxiliary supporting features are designed consistent with the applicable requirements; and 2) other auxiliary features are designed such that they do not degrade safety-related I&C systems below an acceptable level. If the application proposes a different method for achieving any one of these functions, the reviewer should review the method on a case-by-case basis.

A.6 Control of Access, Identification, and Repair

Control of Access

Control of access to I&C system hardware and software allows a licensee to limit access to the means for bypassing safety functions to qualified plant personnel. Typically, control of access includes provisions such as alarms and locks on panel doors for safety-related systems that control access to rooms in which such I&C system equipment is located.

The reviewer should confirm that the design allows for the administrative control of access to safety-related I&C system equipment. These administrative controls should be supported by provisions within the systems, by provisions in the generating station design, or by a combination thereof. The reviewer should verify the following information is provided in the application:

1. Design features provide the means to control physical access to system equipment, including access to test points and the means for changing setpoints.

2. For digital-based safety-related I&C systems, controls are provided on electronic access to safety-related I&C system software and data. Physical and electronic access to digital computer-based control system software and data is adequately controlled to prevent changes by unauthorized personnel. Controls are provided to prevent unauthorized and inadvertent access through network connections and maintenance equipment. Controls are established such that access to maintenance equipment is limited to only authorized personnel for the period of time during which maintenance is being performed.

3. Measures are included to ensure that I&C systems do not present an electronic path by which unauthorized personnel can change plant software or display erroneous plant status information for the operators. Hardware characteristics that enforce unidirectional communication feature(s) (e.g., the use of a unidirectional/non-software based link that is connected to a transmitter in the higher classified system and a receiver in the lower classified system) are considered by the applicant as the preferred means for mitigating any hazard(s) associated with communication paths.

4. A demonstration that (a) features to support establishment of a secure operational environment have been incorporated into the design; (b) the secure development environment will identify undocumented codes and preclude their use; and (c) safety-related systems will be installed and maintained in accordance with the station administrative procedures and control of access programs.

If the reviewer confirms that the application conforms to the guidance identified above, the staff can conclude that the application provides information sufficient to demonstrate the proposed administrative provisions to control access to safety-related I&C systems and equipment are adequate to prevent unauthorized access and modification to these systems. If the application proposes a different method for achieving any one of these functions, the reviewer should review the method on a case-by-case basis.

Identification

Identification refers to the naming and labeling of I&C-related SSCs, and I&C system documentation, software, and firmware to ensure adequate control of system equipment that

performs safety-significant functions. The reviewer should evaluate the description of identification controls for safety-related I&C equipment to confirm:

1. There is or will be distinct means to easily identify redundant divisions of the safety-related I&C system components, cables, and cabinets, such as by a color code scheme, unique symbols, or other acceptable means.

2. For digital-based safety-related I&C systems:

    a. Adequate firmware and software identification is provided to assure that the correct software version, along with the correct control parameters and constants, are installed in the correct hardware component; and

    b. Configuration management is used for maintaining the identification of software to support version control.

If the reviewer confirms that the application conforms to the guidance identified above, the staff can conclude that the application provides information sufficient to demonstrate that safety-related I&C systems are distinctively marked, versions of hardware are marked accordingly, and configuration management is used for maintaining identification of software. If the application proposes a different method for achieving any one of these functions, the reviewer should review the method on a case-by-case basis.

Repair

The reviewer should confirm that the safety-related I&C systems are designed to facilitate timely recognition, location, replacement, repair, and adjustment of malfunctioning equipment. The reviewer should confirm that the application provides sufficient information to demonstrate:

1. The software and hardware surveillance testing and self-diagnostic features within the safety-related I&C system design facilitate timely fault recognition, fault location identification, replacement, repair, and adjustment of malfunctioning equipment.

2. The I&C architecture allows for bypassing system design features to allow for repairs without adversely affecting the safety functions.

3. Digital safety-related I&C equipment includes self-diagnostic capabilities to aid in troubleshooting.

If the reviewer confirms that the application conforms to the guidance identified above, the staff can conclude that the application provides information sufficient to demonstrate that the design of safety-related I&C systems facilitates timely recognition and location of faults, and replacement, repair, and adjustment of malfunctioning equipment. If the application proposes a different method for achieving any one of these functions, the reviewer should review the method on a case-by-case basis.

A.7 Interaction between Sense and Command Features and Other Systems

The application should identify any credible single event, including all direct and consequential results of that event, that can cause an action from a system that is not safety-related to result in conditions for which the FSAR credits protective actions and concurrently prevent the sense and

command features from performing these protective actions. If any such events are identified, the reviewer should confirm one or both of the following criteria have been met:

1. Alternate sense and command features not subject to the failure resulting from the same single event are available to initiate the protective action.

2. Equipment not subject to failure caused by the same single event is provided to detect the event and limit the consequences to acceptable values designated in the design basis.

If the reviewer confirms that the application conforms to the guidance identified above, the staff can conclude that the application provides information sufficient to demonstrate that interactions between safety-related I&C systems and equipment that is not safety-related do not adversely impact plant safety. If the application proposes a different method for achieving any one of these functions, the reviewer should review the method on a case-by-case basis.

A.8 Multi-Unit Stations

Since SSCs can be shared among NPP units of multi-unit stations, the reviewer should confirm the following:

1. I&C design descriptions in the application provide assurance that safety-related I&C SSCs such as reactor trip systems and engineered safety features actuation systems are not shared among units in multi-unit stations. If safety-related I&C SSCs are shared among NPP units then, the reviewer should confirm that the ability to simultaneously perform required safety functions in all units is not impaired.

2. Any design that proposes sharing of SSCs other than safety-related I&C SSCs maintain the ability to simultaneously perform credited safety functions in all units.

3. Provisions are included in the I&C design to ensure that a single failure within safety-related I&C systems of one unit will not adversely affect or propagate via shared systems to another unit such that they cause safety-related systems to fail in the other unit.

4. Any proposed contingency or emergency plans for temporary sharing of systems (such as electrical power cross ties) will not impair the ability of the safety-related I&C system in any unit to perform its safety functions.

If the reviewer confirms that the application conforms to the guidance identified above, the staff can conclude that the application provides information sufficient to demonstrate that (1) safety-related I&C SSCs are not shared among units of multi-unit stations; and (2) sharing of SSCs that are not safety-related across units will not impair the ability of safety-related I&C SSCs in any unit to perform its safety functions. If the application proposes a different method for achieving any one of these functions, the reviewer should review the method on a case-by-case basis.

Note that non-LWRs may include multiple modules, and in this respect differ from multiple large LWR units discussed above. The staff should carefully review the multiple-module designs partly based on some of the guidance above on multiple units.

A.9 Automatic and Manual Control

The review of this area includes evaluation of automatic and manual initiation of protective actions to ensure that safety-related I&C systems automatically initiate and execute protective action for the range of conditions and performance specified in the safety analysis. In addition, the review of manual controls should confirm that the controls will be functional, accessible within the time constraints of operator responses, and available during plant conditions under which manual actions may be necessary. Logic processing units are monitored by an independent hardware-based, diverse means that produces a trip in the affected redundant portion of the system if the logic processing unit ceases operation or "locks-up" (i.e., ceases to respond).

Automatic Control

The reviewer should verify that safety-related I&C systems provide capability to automatically initiate and control all protective actions. The application should provide information to confirm that these systems have been designed to demonstrate that the performance specifications are met, and that the precision of these systems are adequate to the extent that setpoints, margins, uncertainty, and response times are factored into the analysis. These safety-related I&C systems should also be designed with capability in the execute features to receive and act upon automatic control signals from the sense and command features.

The reviewer should confirm that the proposed response times assure that automatic actuations have an acceptable level of determinism with predictable performance margins when a demand signal is present. For digital safety-related I&C systems, the reviewer should confirm that the functional requirements have been appropriately allocated between hardware and software. This includes accounting for response times for all I&C timing delays involved in an instrument channel from sensor to final actuation device.

Manual Control

The review of manual controls should confirm that the controls will be functional (e.g., power will be available and command equipment is appropriately qualified).

The reviewer should verify that the design provides the capability to allow actuation from both the automatic safety-related I&C system and manual controls. The reviewer should also verify that the design provides displays of the plant parameters necessary for the operator to perform the manual action.

The reviewer should confirm that the manual controls are independent and diverse from the digital I&C safety systems (e.g., simple, dedicated, discrete hardwired logic components). The manual controls provided in the I&C design should be connected downstream of the plant's digital I&C safety system outputs. These connections should not compromise the integrity of interconnecting cables and interfaces between local electrical or electronic cabinets and the plant's electromechanical equipment.

If the reviewer confirms that the application conforms to the guidance identified above, the staff can conclude that the application provides information sufficient to: (1) demonstrate that safety-related I&C systems provide the capability to automatically initiate and control all protective actions for the range of conditions and performance specified in the safety analyses; and (2) demonstrate that manual controls will be functional, accessible within the time constraints of

operator responses, and available during plant conditions under which manual actions may be necessary. If the application proposes a different method for achieving any one of these functions, the reviewer should review the method on a case-by-case basis.

A.10 Displays and Monitoring

The review of this area includes the display and monitoring systems, which provide information for (1) the safe operation of the plant during normal operation, transient, and accident conditions; (2) supporting manual initiation and control of systems that perform safety-significant functions; and (3) the normal status and the bypassed and inoperable status of such systems. The display and monitoring systems include the annunciator system, which consists of sets of alarms (which may be displayed on tiles, video display units, or other devices) and sound equipment; logic and processing support; and functions to enable operators to silence, acknowledge, reset, and test alarms.

The reviewer should confirm that the display and monitoring systems provide sufficient information to allow operators to:

1. Ensure plant safety during normal operation;

2. Determine what automatic or manual actions are necessary to mitigate the consequences of transient and accident conditions;

3. Perform manual system or division-level actuation of safety functions; and

4. Determine the status of safety-related I&C systems.

For the parameter display system that provides information to emergency response facilities and the emergency response data system, the reviewer should limit the review to the system interface with the plant control systems.

If the reviewer confirms that the application conforms to the guidance identified above, the staff can conclude that the application provides information sufficient to demonstrate that I&C display and monitoring systems: (1) provide the necessary information for the safe operation of the plant during normal operation, transient, and accident conditions, as described in the safety analyses; (2) will provide the necessary information for manual actuation of safety functions; and (3) will display normal status and the bypassed and inoperable status of such safety-related I&C systems. If the application proposes a different method for achieving any one of these functions, the reviewer should review the method on a case-by-case basis.

A.11 Capability for Testing and Calibration

The review of this area includes evaluating the capability for testing and calibration of safety-related I&C equipment to ensure SSCs retain the capability to accomplish their associated functions. The reviewer should confirm the following:

1. Test and calibration functions do not adversely affect the ability of the safety-related I&C system to perform its safety function.

2. The system has the capability to allow for testing that duplicates, as closely as practicable, the overall performance of the safety-related I&C system credited in the safety analysis.

3. The system has the capability to allow for testing that confirms operability of both the automatic and manual circuitry. The capability for testing should be provided to permit testing during reactor operation.

For sense and command features, the reviewer should confirm that the application provides a means for checking the operational availability of each sense and command feature input sensor relied upon for a safety function during reactor operation.

If the reviewer confirms that the application conforms to the guidance identified above, the staff can conclude that the application provides information sufficient to: (1) demonstrate that safety-related I&C components and systems are capable of being tested and calibrated while retaining their manual and automatic capability to accomplish their safety functions during reactor operation; and (2) demonstrate that, for digital-based safety-related I&C systems, testing and calibration functions (including any self-diagnostic functions) do not adversely affect these systems' ability to perform their safety functions. If the application proposes a different method for achieving any one of these functions, the reviewer should review the method on a case-by-case basis.

APPENDIX B CROSS-CUTTING ISSUES AND INTERFACES

The reviewer should, through either a core review team approach or a matrix review approach, consider interfaces between I&C systems and other plant systems and disciplines during the review. This may include considerations for human factors engineering, reactor systems design, balance of plant design, QA, and TS. Table X.2-1 identifies the review interface topics, the interface branch and the sections in this review guide that address those topics. The reviewer should coordinate with these interface branches when addressing these topics during the review.

Table X.2-1: Cross-Cutting Interface Reference

Review Interface Topic	Interface Discipline	DRG I&C Section Reference	Review Interface Guidance
Quantitative Reliability Assessment	PRA	Section X.2.1.2	The review of the quantitative reliability assessment should be coordinated with the organization responsible for reviewing the PRA model for the overall plant.
Diversity and Defense-in-Depth	Human Factors Reactor Systems	Section X.2.2.1.3	The review should be coordinated with the organization responsible for reviewing human factors to evaluate whether the manual operator actions as a diverse means of coping with transients and accident conditions that are concurrent with a software CCF of the digital I&C protection system are acceptable. The review of diversity in support of DID should be coordinated with the organization responsible for the review of transient and accident analysis of the application. The reviewer should confirm with the organization responsible for the review of reactor systems that the analytical basis detailed in the diversity in support of DID assessment is acceptable and consistent with the transient and accident analysis and that the design of the mechanical systems used for anticipated transient without scram (ATWS) mitigation is acceptable.
Quality	Vendor Inspection	Section X.2.2.2.1	The review should be coordinated with the branch responsible for review of QA. See Section

Review Interface Topic	Interface Discipline	DRG I&C Section Reference	Review Interface Guidance
			X.2.2.2.1 of this review guide for I&C systems review responsibilities for this topic.
Equipment Qualification	Structural Engineering, Electrical Engineering	Section X.2.2.2.2	The organization responsible for the review of seismic qualification verifies the methods of testing and analysis employed to ensure the functionality of mechanical and electrical equipment (including I&C) under the full range of normal and accident loadings. In addition, the organization responsible for the review of environmental qualification of I&C systems reviews mild and harsh environment qualification.
Operating and Maintenance Bypasses	Technical Specifications	Appendix A, Section A.1	The review of operating and maintenance bypasses should be coordinated with the organization responsible for reviewing the TS portion of the application to confirm that the proposed TS required actions reflect the provisions for these bypasses.
Interlocks	Reactor Systems	Appendix A, Section A.2	The reviewer should coordinate the review of interlocks that are credited in the design bases accident analyses.
Derivation of System Inputs	Reactor Systems	Appendix A, Section A.3	The review of system inputs should be coordinated with the review of the transient and accident analysis of the application to ensure that system inputs are direct measures of specified process variables in the design basis, to the extent feasible and practicable.
Setpoints	Technical Specifications, Reactor Systems	Appendix A, Section A.4	The reviewer should coordinate the setpoint methodology review with the organization responsible for TS and basis sections of the application, including the setpoint control program, and the organization responsible for review of the transient and accident analysis.
Auxiliary Features	Balance of Plant	Appendix A, Section A.5	The I&C aspects of auxiliary supporting features and other auxiliary features are addressed in

Review Interface Topic	Interface Discipline	DRG I&C Section Reference	Review Interface Guidance
			the review of those application sections that discuss the systems that provide these features, which may include electric power systems; diesel generator fuel storage and transfer systems; instrument air systems; heating, ventilating, and air conditioning systems; and essential service water and component cooling water systems. I&C reviews of auxiliary features should be coordinated with the organizations responsible for the reviews of these features to ensure that they are appropriately addressed.
Identification	Human Factors, Electrical Engineering	Appendix A, Section A.6	The review of any proposed identification of SSCs that are used for operator control and remote shutdown functions should be coordinated with the organization responsible for reviewing human factors. Similarly, the review of any proposed identification concerning the electrical power supply for I&C systems should be coordinated with the organization responsible for electrical engineering.
Multi-Unit Station	Human Factors, Electrical Engineering	Appendix A, Section A.8	If the application proposes multi-unit shared displays and controls, the review should be coordinated with the organization responsible for reviewing human factors to confirm that shared user interfaces are sufficient to support the operator needs for each of the shared units. The review of any proposed sharing of electrical power in multi-unit NPPs or proposed capability for manual connection for sharing of electrical power should be coordinated with the organization responsible for electrical engineering.
Automatic and Manual Control	Human Factors	Appendix A, Section A.9	The review of automatic and manual controls should be coordinated with the organization responsible for the review of human

Review Interface Topic	Interface Discipline	DRG I&C Section Reference	Review Interface Guidance
			factors to confirm that the functions and the characteristics of the controls allow plant operators to take appropriate manual actions.
Post-Accident Monitoring Variables	Human Factors, Reactor Systems, Electrical Engineering, Radiation Monitoring, PRA, Operator Licensing	Appendix A, Section A.10	The review of information displays should be coordinated with the following organizations: 1. Human factors to confirm that the information displays and the characteristics of the displays (e.g., location, range, type, and resolution) (a) support the system design; and (b) incorporate human factors principles. 2. Reactor systems to confirm that information displays conform to the analyses of transient and accident conditions. 3. Electrical engineering to confirm that the power for safety-significant SSCs, such as level indication or pressure relief valve indication, is supplied from a reliable source of emergency power in the event of a loss of offsite power. Furthermore, the staff should evaluate each design to identify vulnerabilities that may warrant the electrical engineering branch attention. 4. Radiation monitoring to confirm that the information displays support radiation monitoring 5. Severe accident and PRA evaluations in the application to confirm that information displays conform to analyses of severe accidents, plant-specific vulnerabilities, and any applicable Fukushima-related requirements. In addition, the appropriate staff should be consulted to determine if any operating experience relevant

Review Interface Topic	Interface Discipline	DRG I&C Section Reference	Review Interface Guidance
			to displays and monitoring could inform the staff's review of this section.
Capability for Testing and Calibration	Technical Specifications	Appendix A, Section A.11	The review of testing and calibration provisions should be coordinated with the organization responsible for reviewing TS.
Inspections, Tests, Analyses, and Acceptance Criteria (ITAAC) and Tier 1 certified design material for 10 CFR Part 52 applications	Tier 1 and ITAAC	X.1	The type of ITAAC-related information and the level of detail in Tier 1 material is based on a graded approach commensurate with the safety significance of SSCs. ITAAC requirements are included in 10 CFR Part 52 licensing processes to provide reasonable assurance that, if the inspections, tests, and analyses are performed and the acceptance criteria met, the facility has been constructed and will be operated in conformity with the license, the provisions of the Atomic Energy Act, and the NRC's regulations.

APPENDIX C REFERENCES

1. United States (U.S.) Nuclear Regulatory Commission (NRC), SECY-11-093, “Near-Term Task Force Review of Insights from the Fukushima Dai-ichi Accident,” July 2011, (Agencywide Documents Access and Management System (ADAMS) Accession No. ML111861807).

2. U.S. NRC, Staff Requirements Memorandum (SRM) to SECY-11-0024, “Use of Risk Insights to Enhance the Safety Focus of Small Modular Reactor Reviews,” May 2011, (ADAMS Accession No. ML111320551).

3. U.S. NRC Design-Specific Review Standard for NuScale SMR Design, Chapter 7, “Instrumentation and Controls,” July 2016, (ADAMS Accession No. ML15356A416).

4. U.S. NRC, “Vision and Strategy: Safely Achieving Effective and Efficient Non-Light Water Reactor Mission Readiness,” December 2016, (ADAMS Accession No. ML16356A670).

5. U.S. NRC, “Non-LWR Vision and Strategy Near-Term Implementation Action Plans,” July 2017, (ADAMS Accession No. ML17165A069).

6. Regulatory Guide (RG) 1.233, “Guidance for Technology-Inclusive, Risk-Informed, and Performance-Based Approach to Inform the Licensing Basis and Content of Applications for Licenses, Certifications, and Approvals for Non-Light-Water Reactors,” June 2020, (ADAMS Accession No. ML20091L698).

7. Nuclear Energy Institute, NEI 18-04, “Risk-Informed Performance-Based Technology-Inclusive Guidance for Non-Light Water Reactor Licensing Basis Development,” August 2019, (ADAMS Accession No. ML19241A472).

8. U.S. NRC, SECY-19-0117, “Technology-Inclusive, Risk-Informed, and Performance-Based Methodology to Inform the Licensing Basis and Content of Applications for Licenses, Certifications, and Approvals for Non-Light-Water Reactors,” December 2019, (ADAMS Accession No. ML18311A264).

9. U.S. NRC, SECY-19-0009, “Advanced Reactor Program Status,” February 2019, (ADAMS Accession No. ML18346A075)

10. U.S. NRC, Research Information Letter (RIL)-1101, “Technical Basis to Review Hazard Analysis of Digital Safety Systems,” February 2015, (ADAMS Accession No. ML14237A359)

11. U.S. NRC, “Design Review Guide (DRG): Instrumentation and Controls for Non-LWR Reviews – Analysis of Public Comments,” October 8, 2020, (ADAMS Accession No. ML20238B943)

12. Nuclear Energy Institute, NEI Supplemental Industry Comments on draft DRG: Instrumentation and Controls for Non-LWR Reviews with Attachment, February 11, 2021, (ADAMS Accession No. ML21057A281)

13. Advisory Committee on Reactor Safeguards, Design Review Guide: Instrumentation and Controls for Non-Light-Water Reactor Reviews, December 16, 2020, (ADAMS Accession No. ML20349E838)

APPENDIX D ACRONYMS LIST

ADAMS - Agencywide Documents Access and Management System
AL - analytical limit
ATWS - anticipated transient without scram
CCFs - common cause failures
CFR - Code of Federal Regulations
DID - defense-in-depth
DRG - Design Review Guide
DSRS - design-specific review standard
EMI/RFI - electromagnetic and radio-frequency interference
I&C - instrumentation and controls
IEEE - Institute for Electrical and Electronics Engineering
ITAAC - Inspections, Tests, Analyses, and Acceptance Criteria
LBE - licensing basis event
LWR - light water reactor
NEI - Nuclear Energy Institute
non-LWR - non-light water reactor
NPP - nuclear power plant
PDC - principal design criteria
PRA - probabilistic risk assessment
QA - quality assurance
RG - regulatory guide
RIL - research information letter
SL - safety limit
SMR - small modular reactor
SRM - staff requirements memorandum
SSCs - structures, systems, and components
Std - standard
STPA - systems theoretic process analysis
TS - technical specifications

DESIGN REVIEW GUIDE (DRG): INSTRUMENTATIONS AND CONTROLS FOR NON-LIGHT WATER REACTOR REVIEWS

DISTRIBUTION:
PUBLIC
RidsNrrDanuUarp Resource
RidsNrrDanuUart Resource
RidsNrrDanuUarl Resource
RidsOgcMailCenter
RidsAcrsMailCenter
JSegala, NRR
JHoellman, NRR
MHayes, NRR
BBeasley, NRR
JJohnston, NRR
IGarcia, NRR
JAshcraft, NRR
DTaneja, NRR

ADAMS Accession No.: ML21011A140 ***via email** **NRR-106**

OFFICE	DANU/UARP: PM	DANU/UART: BC	DANU/UARP: BC
NAME	JHoellman	MHayes	JSegala
DATE	1/29/2021*	2/3/2021*	2/2/2021*
OFFICE	DEX/ELTB: BC	OGC: NLO	DEX: DD
NAME	JJohnston (DTaneja for)	RWeisman	EBenner
DATE	2/2/2021*	2/5/2021*	2/8/2021*
OFFICE	DANU		
NAME	MShams		
DATE	2/8/2021*		

OFFICIAL RECORD COPY

Paperwork Reduction Act

This Design Review Guide provides voluntary guidance for implementing the mandatory information collections in 10 CFR Parts 50 and 52 that are subject to the Paperwork Reduction Act of 1995 (44 U.S.C. 3501 et. seq.). These information collections were approved by the Office of Management and Budget, approval numbers 3150-0011 and 3150-0151. Send comments regarding this information collection to the FOIA, Library, and Information Collections Branch (T-6 A10M), U.S. Nuclear Regulatory Commission, Washington, DC 20555-0001, or by e-mail to Infocollects.Resource@nrc.gov, and to the OMB reviewer at: OMB Office of Information and Regulatory Affairs (3150-0011 and 3150-0151), Attn: Desk Officer for the Nuclear Regulatory Commission, 725 17th Street, NW Washington, DC 20503; e-mail: oira_submission@omb.eop.gov.

Public Protection Notification

The NRC may not conduct or sponsor, and a person is not required to respond to, a collection of information unless the document requesting or requiring the collection displays a currently valid OMB control number.