DRAFT for Comment

U. S. NUCLEAR REGULATORY COMMISSION

DESIGN-SPECIFIC REVIEW STANDARD FOR mPower™ iPWR DESIGN

7.1 Fundamental Design Principles

REVIEW RESPONSIBILITIES

Primary—Organization responsible for the review of I&C

Secondary—None

The organization responsible for the review of instrumentation and controls (I&C) should evaluate whether the equipment will be able to perform the required safety functions described in section 7.3, "System Design." To this end, the reviewer should ensure that the application contained sufficiently detailed functional diagrams and explanations to ensure that the hardware and software for digital I&C architectures comprise the fundamental design principles, namely independence; redundancy; determinism; defense-in-depth and diversity; and simplicity.

Level of review applied to the review of digital I&C systems:

As stated in SECY-11-0024, the level of review for a particular system, structure, or component (SSC) is derived from both the SSC's safety importance (i.e., safety-related or nonsafety-related) and risk significance. The Introduction to NUREG-0800, Part II, describes the licensing review philosophy and framework to be applied by the staff for new iPWR design certification and combined license applications under 10 CFR Part 52. The introduction states that the risk-informed review framework is applicable to the review of all SSCs, but may not apply to the review of programmatic, procedural, organizational, or other topics that, due to their safety or risk significance, are reviewed at the appropriate level as determined by the technical branches performing the reviews. For example, the program or topical area may address regulatory requirements that are not amenable to a risk-informed approach (e.g., waste management systems). In the case of digital I&C, the review framework of digital I&C systems involves detailed analysis and in-depth evaluation techniques to satisfy the DSRS acceptance criteria applicable to digital I&C systems, which are deterministic and do not incorporate risk significance.

The staff previously addressed the use of risk information in the review of digital I&C systems in SECY-09-0061, "Status of the Nuclear Regulatory Commission Staff Efforts to Improve the Predictability and Effectiveness of Digital Instrumentation and Control Reviews," dated April 14, 2009. In SECY-09-0061, the staff explained that currently there is insufficient knowledge of digital I&C failure modes and reliability data to support a recommendation that the Commission modify its policy on the need for diversity and defense-in-depth in digital I&C systems. The staff based this conclusion on inputs from the Advisory Committee on Reactor Safeguards, its own research program in this area, and the preponderance of the technical literature in this field. Because the current state-of-the-art and available data are insufficient to support risk-informed digital I&C licensing actions at this time, for the digital I&C guidance developed herein, the staff will use a traditional deterministic review approach for review of the mPower™ iPWR design.

7.1.1 Independence

I. Areas of Review

The reviewer will evaluate whether the proposed I&C system design exhibits independence (1) among safety divisions, (2) between redundant portions of a safety system, (3) between safety systems and the effects of a design-basis event (DBE), and (4) between safety systems and other systems, as required by 10 CFR 50.55a(h). The review covers physical independence, electrical independence, and communications independence.

Review Interfaces

Other fundamental design principles, such as redundancy, diversity and defense-in-depth, and determinism, inform the review of independence. In addition, the Appendices to DSRS 7.1 provide guidance describing how the reviewer shall consider the architecture, hazard analysis, and simplicity of the I&C system, and how these attributes inform the staff's review of the system's independence.

II. Acceptance Criteria

Requirements

1. The regulation at 10 CFR 50.55a(h) requires compliance with IEEE Std. 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," Clause 5.6, "Independence." In accordance with 10 CFR 50.55a(a)(3), an applicant can propose alternatives to the requirements of paragraph (h) of this section, but the alternative must provide an acceptable level of quality and safety and be addressed in the application accordingly.

2. General design criterion (GDC) 21, "Protection system reliability and testability," of Appendix A, "General Design Criteria for Nuclear Power Plants," to 10 CFR Part 50, "Domestic Licensing of Production and Utilization Facilities," requires, in part, that the redundancy and independence designed into the protection system shall be sufficient to assure that no single failure results in loss of the protection function.

3. GDC 22, "Protection System Independence," requires, in part, that the protection system shall be designed to assure that the effects of natural phenomena, and of normal operating, maintenance, testing, and postulated accident conditions on redundant channels do not result in loss of the protection function, or shall be demonstrated to be acceptable on some other defined basis.

4. GDC 24, "Separation of Protection and Control Systems," requires that the protection system shall be separated from control systems to the extent that failure of any single control system component or channel, or failure or removal from service of any single protection system component or channel which is common to the control and protection systems leaves intact a system satisfying all reliability, redundancy and independence requirements of the protection system. Interconnection of the protection and control systems shall be limited so as to assure that safety is not significantly impaired.

DSRS Acceptance Criteria

1. The system should conform to the independence requirements in Clause 5.6 of IEEE Std. 603-1991.

2. The system should conform to the physical and electrical independence guidance contained in the version of Regulatory Guide (RG) 1.75, "Criteria for Independence of Electrical Safety Systems," in place 6 months before the docket date of the application. This RG endorses IEEE Std. 384-1992, "IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits." To the extent that the applicable version of RG 1.75 endorses IEEE Std. 384, the design should also conform to the guidance in IEEE Std. 384.

3. The system should conform to the communication independence guidance in Clause 5.6 of IEEE Std. 7-4.3.2-2003, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations," as endorsed by the version of RG 1.152, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants." To the extent that the applicable version of RG 1.152 endorses IEEE Std. 7-4.3.2, the design should also conform to the guidance in IEEE Std. 7-4.3.2.

4. The system should conform to the single random failure guidance in Clause 5.6.3.3 of IEEE Std. 603-1991. The version of RG 1.53, "Application of the Single-Failure Criterion to Nuclear Power Plant Protection Systems," in place 6 months before the docket date of the application, provides additional guidance for the application of this requirement. To the extent that the applicable version of RG 1.53 endorses IEEE Std. 379-2000, the design should also conform to the guidance in IEEE Std. 379-2000.

III. Review Procedures

Specific DSRS acceptance criteria acceptable to meet the relevant requirements of the NRC's regulations identified above are as follows for review described in this DSRS section. The DSRS is not a substitute for the NRC's regulations, and compliance with it is not required. Identifying the differences between this DSRS section and the design features, analytical techniques, and procedural measures proposed for the facility, and discussing how the proposed alternative provides an acceptable method of complying with the regulations that underlie the DSRS acceptance criteria, is sufficient to meet the intent of 10 CFR 52.47(a)(9), "Contents of applications; technical information."

To determine whether the description of the I&C system in the application meets the independence requirements of GDC 21, 22, 24, and Clause 5.6 of IEEE Std. 603-1991, the review should evaluate whether it demonstrates independence between (1) safety divisions (2) redundant portions of a safety system, (3) safety systems and the effects of DBEs, and (4) safety systems and other systems. For each of these areas, the review should evaluate, at a minimum, the following:

1. Physical independence
2. Electrical independence
3. Communications independence
4. Functional independence

Using engineering judgment, the reviewer evaluates the design to determine whether other potential dependencies might include systemic dependencies resulting from the development process or dependencies between power and control signals.

Physical Independence

Physical independence is attained by physical separation and physical barriers. The reviewer should consider whether the application demonstrates the separation of (1) redundant portions of the safety system and (2) protection and control systems to confirm that all interfaces among redundant portions of the safety system and between control systems and protection systems have been properly identified and addressed. Note that the review of physical separation of electrical cables is part of Chapter 8, titled "Electric Power," and it is not reviewed in Chapter 7.

The review of physical independence should confirm that the I&C systems conform to the physical independence guidance in the version of RG 1.75 in place 6 months before the docket date of the application. To the extent that the applicable version of RG 1.75 endorses IEEE Std. 384, the design should also conform to the guidance in IEEE Std. 384. The relevant guidance includes physical separation requirements for circuits and electrical equipment that comprise or are associated with safety systems.

Electrical Independence

The review of electrical independence should confirm that the I&C systems conform to the guidance in the version of RG 1.75 in place 6 months before the docket date of the application. The relevant guidance includes electrical isolation requirements for circuits and electrical equipment that comprise or are associated with safety systems. In addition, the reviewer should evaluate the following when assessing electrical independence:

A. The I&C evaluation of electrical independence is limited to the review of components and electrical wiring inside racks, panels, and control boards for safety systems. Note that the evaluation of physical separation of electrical cables is part of Chapter 8, titled "Electric Power," and it is not reviewed in this Chapter.

B. The reviewer will evaluate that the safety system design considered electrical independence, including the use of redundant power sources. Note that the evaluation of qualification of the independent power sources is part of Chapter 8, titled "Electric Power," and it is not reviewed in this Chapter.

C. The reviewer will verify that isolation devices are used to transmit signals between independent divisions. Isolation devices should be classified as part of the safety system and powered in accordance with the criteria of IEEE Std. 603-1991 and the guidelines contained in the version of RG 1.75 in place 6 months before the docket date of the application. The reviewer will verify that the isolation device is powered by a safety power source to perform its safety related isolation function.

Communications Independence

The review of communications independence should evaluate communication independence (1) among redundant portions of the safety system, and (2) between safety and nonsafety systems. The review should confirm that the design of the data communication meets the requirements of IEEE Std. 603-1991, Clause 5.6. The review should also confirm that data

communication conforms to the guidance in Clause 5.6 and guidance for the separation and isolation of data processing functions of interconnected computers of IEEE Std. 7-4.3.2-2003.

The determination of communications independence is self-evident if one way communication is used among redundant channels or divisions and between safety and nonsafety systems. In addition, data flows between redundant portions of safety systems should be limited to those required for coincidence logic voting for actuation and interlocks required for the performance of safety functions.

Functional Independence

If divisions share plant data parameters (e.g., reactor power or reactor pressures) to implement a safety function, the review should evaluate functional independence among those divisions. The review should confirm that data communication functions meet the requirements of IEEE Std. 603-1991, Clause 5.6.

IV. Evaluation Findings

Based on this review, the staff concludes that the application satisfies the requirements for independence. The design of the I&C systems adequately addressed the fundamental design principle of independence among safety divisions, between redundant portions of a safety system, between safety systems and the effects of a DBE, and between safety systems and other systems. Therefore, the design of the I&C systems satisfies the independence requirements of GDC 21, 22, 24, and IEEE Std. 603-1991, Clause 5.6.

The design of the I&C systems adequately addressed physical separation and electrical isolation requirements for circuits and electrical equipment that comprise or are associated with safety systems. Therefore, the design of the I&C systems conforms to the guidelines in the version of RG 1.75 in place 6 months before the docket date of the application, with regard to physical and electrical independence.

The design of the I&C systems adequately addressed data communication independence. Therefore, the design of the I&C systems satisfies requirement of Clause 5.6 of IEEE Std. 603-1991 and conforms to the guidelines in IEEE Std. 7-4.3.2-2003

The design of the I&C systems adequately addressed functional communication independence. Therefore, the design of the I&C systems satisfies requirements of Clause 5.6 of IEEE Std. 603-1991.

V. Implementation

The staff will use this DSRS section in performing safety evaluations of mPower^{TM}-specific design certification (DC), combined license (COL), or early site permit (ESP) applications submitted by applicants pursuant to 10 CFR Part 52. The staff will use the method described herein to evaluate conformance with Commission regulations.

Because of the numerous design differences between the mPower^{TM} and large light-water nuclear reactor power plants, and in accordance with the direction given by the Commission in SRM- COMGBJ-10-0004/COMGEA-10-0001, “Use of Risk Insights to Enhance the Safety Focus of Small Modular Reactor Reviews,” dated August 31, 2010 (ML102510405), to develop risk-informed licensing review plans for each of the small modular reactor (SMR) reviews

including the associated pre-application activities, the staff has developed the content of this DSRS section as an alternative method for mPower™ -specific DC, COL, or ESP applications submitted pursuant to 10 CFR Part 52 to comply with 10 CFR 52.47(a)(9), "Contents of applications; technical information."

This regulation states, in part, that the application must contain "an evaluation of the standard plant design against the Standard Review Plan (SRP) revision in effect 6 months before the docket date of the application." The content of this DSRS section has been accepted as an alternative method for complying with 10 CFR 52.47(a)(9) as long as the mPower™ DCD FSAR does not deviate significantly from the design assumptions made by the NRC staff while preparing this DSRS section. The application must identify and describe all differences between the standard plant design and this DSRS section, and discuss how the proposed alternative provides an acceptable method of complying with the regulations that underlie the DSRS acceptance criteria. If the design assumptions in the DC application deviate significantly from the DSRS, the staff will use the SRP as specified in 10 CFR 52.47 (a)(9). Alternatively, the staff may revise the DSRS section in order to address new design assumptions. The same approach may be used to meet the requirements of 10 CFR 52.17 (a)(1)(xii) and 10 CFR 52.79(a)(41), for ESP and COL applications, respectively.

Just as the SRP is not substitute for the regulations and compliance with the SRP is not a requirement, the DSRS is not a substitute for the regulations and compliance with the DSRS is not a requirement. If the applicant proposes an alternative method for complying with specified portions of the Commission's regulations, the applicant must demonstrate the acceptability of its alternate method.

VI. References

All of the references in this DSRS Chapter 7, "Instrumentation and Controls," may be found in Appendix D, of this Chapter.

7.1.2 Redundancy

I. Areas of Review

Redundancy is commonly used in I&C safety systems to achieve system reliability goals and conformity with the single failure criterion. The reviewer should evaluate the I&C architecture for redundancy. The application, based on the design/design constraints, should provide information that describes what level of redundancy is required to assure that: (1) no single failure results in loss of the protection function, and (2) removal from service of any component or channel does not result in loss of the required minimum redundancy unless the acceptable reliability of operation of the protection system can be otherwise demonstrated.

Review Interfaces

Other fundamental design principles, such as independence, diversity and defense-in-depth, and determinism, inform the review of redundancy. In addition, the Appendices to DSRS 7.1 provide guidance describing how the reviewer shall consider the architecture, hazard analysis, and simplicity of the I&C system, and how these attributes inform the staff's review of the system's redundancy.

II. Acceptance Criteria

Requirements

1. The regulation at 10 CFR 50.55a(h) requires compliance with IEEE Std. 603-1991, Clause 5.1, "Single Failure Protection." In accordance with 10 CFR 50.55a(a)(3), an applicant can propose alternatives to the requirements of paragraph (h) of this section, but the alternative must provide an acceptable level of quality and safety and be addressed in the application accordingly.

2. GDC 21*, "*Protection system reliability and testability*,"* requires that the protection system shall be designed for high functional reliability and inservice testability commensurate with the safety functions to be performed. Redundancy and independence designed into the protection system shall be sufficient to assure that (1) no single failure results in loss of the protection function and (2) removal from service of any component or channel does not result in loss of the required minimum redundancy unless the acceptable reliability of operation of the protection system can be otherwise demonstrated. The protection system shall be designed to permit periodic testing of its functioning when the reactor is in operation, including a capability to test channels independently to determine failures and losses of redundancy that may have occurred.

3. GDC 24, "Separation of protection and Control Systems," requires that "[t]he protection system shall be separated from control systems to the extent that failure of any single control system component or channel, or failure or removal from service of any single protection system component or channel which is common to the control and protection systems leaves intact a system satisfying all reliability, redundancy, and independence requirements of the protection system. Interconnection of the protection and control systems shall be limited so as to assure that safety is not significantly impaired."

DSRS Acceptance Criteria

1. Conformance to the single-failure requirements in Clause 5.1 of IEEE Std. 603-1991 and GDC 21 is demonstrated by the conformance to IEEE Std. 379, as endorsed by the version of RG 1.53, "Application of the Single-Failure Criterion to Safety Systems," in place 6 months before the docket date of the application. To the extent that the applicable version of RG 1.53 endorses IEEE Std. 379, the design should also conform to the guidance in IEEE Std. 379. In addition, IEEE Std. 379 allows for a failure modes and effects analysis (FMEA) to be used to demonstrate compliance with the single failure criterion.

2. The system should conform to the single-failure criterion as stated in the version of RG 1.53 in place 6 months before the docket date of the application, which clarifies the application of the single-failure criterion (GDC 21) and endorses IEEE Std. 379, providing supplements and an interpretation. To the extent that the applicable version of RG 1.53 endorses IEEE Std. 379, the design should also conform to the guidance in IEEE Std. 379. IEEE Std. 379, Clause 6.1, identifies logic failures as a type of failure to be considered when applying the single-failure criterion.

Technical Rationale

In applying the single-failure criterion to the design of safety systems, the following conditions are implicit:

1. Independence and Redundancy

   The design of a safety system shall be such that no single failure of a component will interfere with the proper operation of an independent redundant component or system.

2. Nondetectable Failure

   Detectability is a function of the system design and the specified tests. A failure that cannot be detected through periodic testing, or revealed by alarm or anomalous indication, is not detectable.

3. Cascaded Failures

   Whenever the design is such that additional failures could be expected from the occurrence of a single failure from any source, these cascaded failures, collectively, shall be considered to be a single failure.

4. Design-Basis Events

   A DBE that results in the need for safety functions may cause failure of system components, modules, or channels. Equipment should be designed, qualified, and installed so as to be immune to such anticipated challenges. When analysis indicates that failures in a safety system can result from DBEs, these failures shall be considered a consequence of the event.

III. Review Procedures

Specific DSRS acceptance criteria acceptable to meet the relevant requirements of the NRC's regulations identified above are as follows for review described in this DSRS section. The

DSRS is not a substitute for the NRC's regulations, and compliance with it is not required. Identifying the differences between this DSRS section and the design features, analytical techniques, and procedural measures proposed for the facility, and discussing how the proposed alternative provides an acceptable method of complying with the regulations that underlie the DSRS acceptance criteria, is sufficient to meet the intent of 10 CFR 52.47(a)(9), "Contents of applications; technical information."

The reviewer should confirm that the application cites conformance with IEEE Std. 379 and provides a detailed discussion of how the safety I&C systems address the single failure criterion. In addition, the reviewer should evaluate the following when assessing redundancy:

1. The application should provide a single-failure analysis in accordance with Clause 5.1 of IEEE 603 and IEEE Std. 379. In addition, the I&C architecture description should describe how redundancy is implemented in the I&C system design.

2. The reviewer will confirm if: (1) an evaluation of the effects of each component failure mode on the overall system is performed, (2) any component failure mode that could contribute to a failure of the safety system is identified, and (3) necessary action is taken to eliminate, prevent, or control failure modes. Additional guidance on failure modes and hazards is contained in Appendix A, "Hazard Analysis."

3. The reviewer should confirm that the application provides information to demonstrate that all SSCs needed for safe shutdown have sufficient redundancy to conform to the single-failure criterion. The use of data communication systems as single paths for multiple signals or data raises particular concern about extensive consequential failures as the result of a single failure. This review should confirm that channel assignments to individual communication subsystems can ensure that both redundancy and diversity requirements within the supported systems are met. NUREG/CR-6082, "Data Communications," provides additional guidance for issues that need to be considered for single failure when reviewing data communication designs (e.g., layering, encapsulation, protocol, multiplexing, error detection, etc.) and how redundancy may be used.

4. Removal from service of any single safety system component should not result in a loss of the required minimum redundancy unless the reliable operation of the system can be adequately demonstrated. The application must demonstrate how redundancy of channels, criterion for channels out of service (or bypassed), and technical specification limits conform to single-failure criteria, as addressed in GDC 24.

IV. Evaluation Findings

The reviewer must verify that the information provided in the application demonstrates that the design has sufficient redundancy to ensure that: (1) no single failure results in loss of the protection function, and (2) removal from service of any component or channel does not result in loss of the required minimum redundancy unless the acceptable reliability of operation of the protection system can be otherwise demonstrated. The reviewer also must provide the bases for conclusions to be included in the staff's safety evaluation report.

V. Implementation

The staff will use this DSRS section in performing safety evaluations of mPower™-specific design certification (DC), combined license (COL), or early site permit (ESP) applications submitted by applicants pursuant to 10 CFR Part 52. The staff will use the method described herein to evaluate conformance with Commission regulations.

Because of the numerous design differences between the mPower™ and large light-water nuclear reactor power plants, and in accordance with the direction given by the Commission in SRM- COMGBJ-10-0004/COMGEA-10-0001, "Use of Risk Insights to Enhance the Safety Focus of Small Modular Reactor Reviews," dated August 31, 2010 (ML102510405), to develop risk-informed licensing review plans for each of the small modular reactor (SMR) reviews including the associated pre-application activities, the staff has developed the content of this DSRS section as an alternative method for mPower™ -specific DC, COL, or ESP applications submitted pursuant to 10 CFR Part 52 to comply with 10 CFR 52.47(a)(9), "Contents of applications; technical information."

This regulation states, in part, that the application must contain "an evaluation of the standard plant design against the Standard Review Plan (SRP) revision in effect 6 months before the docket date of the application." The content of this DSRS section has been accepted as an alternative method for complying with 10 CFR 52.47(a)(9) as long as the mPower™ DCD FSAR does not deviate significantly from the design assumptions made by the NRC staff while preparing this DSRS section. The application must identify and describe all differences between the standard plant design and this DSRS section, and discuss how the proposed alternative provides an acceptable method of complying with the regulations that underlie the DSRS acceptance criteria. If the design assumptions in the DC application deviate significantly from the DSRS, the staff will use the SRP as specified in 10 CFR 52.47 (a)(9). Alternatively, the staff may revise the DSRS section in order to address new design assumptions. The same approach may be used to meet the requirements of 10 CFR 52.17 (a)(1)(xii) and 10 CFR 52.79 (a)(41), for ESP and COL applications, respectively.

Just as the SRP is not substitute for the regulations and compliance with the SRP is not a requirement, the DSRS is not a substitute for the regulations and compliance with the DSRS is not a requirement. If the applicant proposes an alternative method for complying with specified portions of the Commission's regulations, the applicant must demonstrate the acceptability of its alternate method.

VI. References

All of the references in this DSRS Chapter 7, "Instrumentation and Controls," may be found in Appendix D, of this Chapter.

7.1.3 Determinism

In digital I&C systems, the phrase "deterministic behavior" refers to a property of a computer or data communications system such that the time delay between stimulus and response has a guaranteed maximum and minimum.

I. Areas of Review

The reviewer should evaluate the functional requirements for each I&C system against the requirements of 10 CFR Part 50. For digital systems, the reviewer should specifically evaluate the real-time deterministic performance of the digital I&C platforms and data communications systems. The objective of this review is to (1) verify that system timing requirements calculated from the DBEs and other criteria have been allocated to the digital I&C system architecture as appropriate and have been satisfied in the digital system design, and (2) determine that the application has satisfactorily demonstrated conformance to the applicable requirements of 10 CFR 50.55a(h) and GDC 29.

Review Interfaces

Other fundamental design principles, such as independence, diversity and defense-in-depth, and redundancy, inform the review of determinism. In addition, the Appendices to DSRS 7.1 provide guidance describing how the reviewer shall consider the architecture, hazard analysis, and simplicity of the I&C system, and how these attributes inform the staff's review of the system's determinism.

II. Acceptance Criteria

Requirements

The reviewer will use the following specific regulations and guidance documents to evaluate the deterministic performance of a safety digital I&C system:

1. GDC 29, "Protection against Anticipated Operational Occurrences," requires that the protection and reactivity control systems shall be designed to assure an extremely high probability of accomplishing their safety functions in the event of anticipated operational occurrences.

2. The system's real-time performance must be adequate to ensure completion of protective action within the critical points of time identified in Section 4f of IEEE Std. 603-1991.

3. Hardware and software requirements must appropriately reflect the functional requirements to satisfy IEEE Std. 603-1991, Clauses 6.1 and 7.1. In addition, the system's real-time performance must be deterministic and known.

DSRS Acceptance Criteria

1. The system's real-time performance must be adequate to ensure completion of protective action within the critical points of time identified in Clause 4j of IEEE Std. 603-1991.

2. To comply with IEEE Std. 603-1991, Clauses 6.1 and 7.1, hardware and software requirements must appropriately reflect the functional requirements.

3. The digital I&C system's real-time performance is deterministic and known.

4. Data communications system timing is deterministic or bounded.

5. Risky design practices, such as nondeterministic data communications, nondeterministic computation, use of interrupts, multitasking, dynamic scheduling, and event-driven design should be avoided. If such practices are used, the application must describe the methods used for controlling the associated risk.

Technical Rationale

Digital system architecture affects performance because communication between components of the system takes time, and allocation of functions to various system components affects timing. The architecture may also affect timing because an arrangement of otherwise simple components may have unexpected interactions. Requirements for redundancy and diversity may complicate timing analysis because they result in additional components and interconnections.

Specific timing requirements may affect 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. Timing requirements may also increase complexity, either by fragmenting the system into multiple processors or by code tuning, which makes the software product harder to understand, verify, or maintain.

The digital instrumentation loop often includes the sensor, transmitter, analog-to-digital converter, multiplexer, data communication equipment, demultiplexer, computers, memory devices, controls, and displays. The timing analysis should consider the entire loop.

III. Review Procedures

Specific DSRS acceptance criteria acceptable to meet the relevant requirements of the NRC's regulations identified above are as follows for review described in this DSRS section. The DSRS is not a substitute for the NRC's regulations, and compliance with it is not required. Identifying the differences between this DSRS section and the design features, analytical techniques, and procedural measures proposed for the facility, and discussing how the proposed alternative provides an acceptable method of complying with the regulations that underlie the DSRS acceptance criteria, is sufficient to meet the intent of 10 CFR 52.47(a)(9), "Contents of applications; technical information."

These review procedures are based on the identified DSRS acceptance criteria. Additionally, Appendix B provides guidance on how the reviewer shall consider the architecture of the I&C system in terms of how the system meets the requirements for determinism. Using engineering judgment and depending on the design approach described in the application, the reviewer will select and emphasize material from the procedures described below.

1. Review the I&C architecture information described in Chapter 7 of the application. Ensure that the I&C design includes information to verify limiting response times, digital computer timing requirements, architecture, and design commitments.

2. Verify that system timing requirements calculated from the DBEs and other criteria have been allocated to the digital computer portion of the system, as appropriate, and have been satisfied in the digital system architectural design.

3. Verify that data communications system timing is deterministic or bounded. Consider data rates, data bandwidths, and data precision requirements for normal and off-normal operation, including the impact of environmental extremes. Make note of any nondeterministic delays and provide a basis to conclude that such delays are neither part of any safety functions nor can impede any protective action. Excess capacity margins should be sufficient to accommodate likely future increases in data communications system demands or software or hardware changes to equipment attached to the data communications systems. Confirm that the error performance is specified.

4. Include a concurrent review of the remaining fundamental design principles of redundancy, independence, diversity, and simplicity in Chapter 7 of the application. Ensure that the I&C architecture performance is deterministic and does not diminish the design's conformance with the fundamental design principles. Confirm that the overall I&C design supports appropriate defense-in-depth for postulated hazards.

IV. Evaluation Findings

The reviewer must verify that the application contains sufficient information to demonstrate that the I&C system's real-time performance is adequate to ensure compliance with IEEE 603-1991. Specifically, the application must provide sufficient information to ensure the following:

1. Hardware and software requirements reflect functional timing requirements.

2. The digital I&C system's real-time performance is deterministic and known.

3. Data communications system timing is deterministic or bounded.

4. Any nondeterministic delays have been noted and a basis provided to conclude that such delays are not part of any safety functions. No delay can impede any protective action.

5. Risky design practices should be avoided. If such practices are used, the application must describe the methods used for controlling the associated risk.

V. Implementation

The staff will use this DSRS section in performing safety evaluations of mPower^{TM}-specific design certification (DC), combined license (COL), or early site permit (ESP) applications submitted by applicants pursuant to 10 CFR Part 52. The staff will use the method described herein to evaluate conformance with Commission regulations.

Because of the numerous design differences between the mPower™ and large light-water nuclear reactor power plants, and in accordance with the direction given by the Commission in SRM- COMGBJ-10-0004/COMGEA-10-0001, "Use of Risk Insights to Enhance the Safety Focus of Small Modular Reactor Reviews," dated August 31, 2010 (ML102510405), to develop risk-informed licensing review plans for each of the small modular reactor (SMR) reviews including the associated pre-application activities, the staff has developed the content of this DSRS section as an alternative method for mPower™ -specific DC, COL, or ESP applications submitted pursuant to 10 CFR Part 52 to comply with 10 CFR 52.47(a)(9), "Contents of applications; technical information."

This regulation states, in part, that the application must contain "an evaluation of the standard plant design against the Standard Review Plan (SRP) revision in effect 6 months before the docket date of the application." The content of this DSRS section has been accepted as an alternative method for complying with 10 CFR 52.47(a)(9) as long as the mPower™ DCD FSAR does not deviate significantly from the design assumptions made by the NRC staff while preparing this DSRS section. The application must identify and describe all differences between the standard plant design and this DSRS section, and discuss how the proposed alternative provides an acceptable method of complying with the regulations that underlie the DSRS acceptance criteria. If the design assumptions in the DC application deviate significantly from the DSRS, the staff will use the SRP as specified in 10 CFR 52.47 (a)(9). Alternatively, the staff may revise the DSRS section in order to address new design assumptions. The same approach may be used to meet the requirements of 10 CFR 52.17 (a)(1)(xii) and 10 CFR 52.79 (a)(41), for ESP and COL applications, respectively.

Just as the SRP is not substitute for the regulations and compliance with the SRP is not a requirement, the DSRS is not a substitute for the regulations and compliance with the DSRS is not a requirement. If the applicant proposes an alternative method for complying with specified portions of the Commission's regulations, the applicant must demonstrate the acceptability of its alternate method.

VI. References

All of the references in this DSRS Chapter 7, "Instrumentation and Controls," may be found in Appendix D, of this Chapter.

7.1.4 Diversity and Defense-in-Depth

Diversity is one method of achieving defense-in-depth. Diversity and defense-in-depth (D3) can assure that a safety task will be accomplished when necessary to mitigate plant anticipated operational occurrences (AOOs) and postulated accidents (PAs), while also providing a defense against common cause failures (CCFs).

Defense-in-depth is the principle of providing multiple layers of barriers to any credible failure to avoid or tolerate faults that would prevent a function from achieving its objective. Diversity, in the context of digital I&C, is the principle of using different technologies, equipment manufacturers, logic processing equipment, signals, logic and algorithms, development teams and personnel, and functions to provide a diverse means of accomplishing a safety function. Diversity complements defense-in-depth by decreasing the probability that a particular function will fail to achieve its objective.

For designs that use digital safety systems, the NRC has established a four-point position on D3 for new reactor designs and for digital system modifications to operating plants. The staff requirements memorandum (SRM), dated July 21, 1993, to SECY-93-087, "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs," dated April 2, 1993, and particularly Item 18.II.Q, "Defense Against Common-Mode Failures in Digital Instrumentation and Control Systems," form the foundation of this position.

I. Areas of Review

The I&C safety systems should have a level of D3 such that the presence of two or more redundant systems or components will be able to perform identified functions and the different systems or components will have different attributes so as to reduce the possibility of CCF. While the NRC considers CCF in digital systems to be beyond design basis, the digital reactor protection system (RPS) should be protected against CCFs and the plant should be designed to be protected against the effects of a potential CCF, as well as the effects of AOOs and PAs with a concurrent CCF in the digital protection system.

Software-based or software-logic-based digital system development errors are a credible source of CCF. (Common software includes software, firmware, and logic developed from software-based development systems.) Generally, digital systems cannot be proven to be error free; thus, they are considered susceptible to CCF because identical copies of the software-based logic and architecture are present in redundant divisions of safety-related systems.

Review Interfaces

Other fundamental design principles, such as independence, determinism, and redundancy, inform the review of diversity and defense-in-depth. In addition, the Appendices to DSRS 7.1 provide guidance describing how the reviewer shall consider the architecture, hazard analysis, and simplicity of the I&C system, and how these attributes inform the staff's review of the system's determinism.

1. DSRS Chapter 18 defines a methodology, applicable to new reactors, for evaluating manual operator actions as all or part of a diverse means of coping with AOOs and PAs that are concurrent with a software CCF of the digital I&C protection system. Section 3 of DI&C-ISG-05, "Task Working Group #5: Highly-Integrated Control Rooms—Human Factors Issues," offers additional guidance.

2. The reviewer should confirm that the anticipated transient without scram (ATWS) mitigation protective functions are consistent with the requirements of 10 CFR 50.62, "Requirements for Reduction of Risk from Anticipated Transients without Scram (ATWS) Events for Light-Water-Cooled Nuclear Power Plants," and the ATWS analysis referenced in Chapter 15 of the application for AOOs. The reviewer should also verify the adequacy of the design of mechanical systems used to mitigate ATWS.

3. The reviewer should confirm that the adequacy of the set of manual control and display conforms to the D3 strategy.

II. Acceptance Criteria

Requirements

1. 10 CFR 50.55a(h), which requires compliance with the following sections of IEEE Std. 603-1991:

   A. Clause 6.2, "Manual Control" as it relates to the required manual initiation being inhibited by a CCF of the automated protection functions;
   B. Clause 7.2, "Manual Control" as it relates to the required manual initiation being inhibited by a CCF of the automated protection functions.

2. 10 CFR 50.62, which identifies design requirements for ATWS mitigation systems and equipment.

DSRS Acceptance Criteria

1. NUREG/CR-6303, "Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems," issued December 1994, which summarizes several D3 analyses performed after 1990 and presents an acceptable method for performing such analyses.

2. NUREG/CR-7007, "Diversity Strategies for Nuclear Power Plant Instrumentation and Control Systems," issued February 2010, provides additional information that may be helpful in performing a D3 analysis and in determining how much diversity is enough.

3. SRM to SECY-93-087, which describes the NRC position on defense-in-depth in Item 18.II.Q.

4. Generic Letter (GL) 85-06, "Quality Assurance Guidance for ATWS Equipment That Is Not Safety-Related," dated April 16, 1985, which provides quality assurance guidance for nonsafety-related ATWS equipment.

5. IEEE Std. 379-2000, Clause 5.5, which establishes the relationship between CCF and single failures by defining criteria for CCFs that are not subject to single-failure analysis and identifies defense-in-depth as a technique for addressing CCF.

6. The version of RG 1.62, "Manual Initiation of Protective Actions," in place 6 months before the docket date of the application, includes information on diverse manual initiation of protective action.

7. IEEE Std. 7-4.3.2-2003 provides guidance on performing an engineering evaluation of software CCF, including use of manual action and nonsafety-related systems, or components, or both, to provide means to accomplish the function that would otherwise be defeated by the CCF.

Information Needed

As set forth in Points 1, 2, and 3 of the NRC's position on D3, the application should perform a D3 assessment of the proposed digital I&C system to demonstrate that it has adequately addressed vulnerabilities to CCF.

If this assessment identifies a postulated CCF that could disable a safety function that is credited in the safety analysis to respond to the DBE being analyzed, a diverse means of effective response (with documented basis) is necessary.

The D3 analysis should be documented to enable the NRC staff to independently conclude that the plant I&C systems are sufficiently robust against CCF. The NRC staff should evaluate the proposed diversity evaluation using the agency's position on D3. The application should include the following:

1. Description and analysis of the diversity credited within the safety system or diverse means.

2. A best-estimate (e.g., normal operating plant conditions for the event being analyzed) evaluation of each AOO and PA event in the design basis occurring in conjunction with each single postulated CCF.

3. A description and demonstration of components credited to have no potential for CCF and the plan for demonstrating no potential for CCF (i.e., sufficient diversity or fully tested).

4. An evaluation of all common elements or signal sources shared by two or more system echelons, which should include identification of all interconnections between the safety systems and nonsafety systems provided for system interlocks and a justification that functions required by 10 CFR 50.62 are not impaired by the interconnections.

5. A detailed justification of all manual actions used in credited operator actions that are used as part of or all of the diverse means.

Technical Rationale

The NRC staff will focus its review of D3 in digital I&C systems on whether the safety functions can be achieved in the event of a postulated CCF in the digital I&C system.

III. Review Procedures

Specific DSRS acceptance criteria acceptable to meet the relevant requirements of the NRC's regulations identified above are as follows for review described in this DSRS section. The DSRS is not a substitute for the NRC's regulations, and compliance with it is not required. Identifying the differences between this DSRS section and the design features, analytical

techniques, and procedural measures proposed for the facility, and discussing how the proposed alternative provides an acceptable method of complying with the regulations that underlie the DSRS acceptance criteria, is sufficient to meet the intent of 10 CFR 52.47(a)(9), "Contents of applications; technical information."

The purpose of this section is to confirm that the application has addressed vulnerabilities to CCF in accordance with the NRC position on D3 described in Item 18.II.Q of the SRM to SECY-93-087.

1. Design Attributes To Eliminate Consideration of CCF

   A. For each AOO and PA in the design basis occurring in conjunction with each single postulated CCF, the plant response (calculated using realistic assumptions) should not result in a radiation release exceeding 10 percent of the applicable siting dose guideline values or violate the integrity of the primary coolant pressure boundary. The application should (1) demonstrate that sufficient diversity exists to achieve these goals, (2) identify the vulnerabilities discovered and the corrective actions taken, or (3) identify the vulnerabilities discovered and provide a documented basis that justifies taking no action.

   B. When a failure of a common element or signal source shared by the control system and reactor trip system (RTS) is postulated and the CCF results in a plant response for which the safety analysis credits reactor trip and also impairs the trip function, then diverse means that are not subject to or failed by the postulated failure should be provided to perform the RTS function. The diverse means should ensure that the plant response calculated using realistic assumptions and analyses does not result in a radiation release exceeding 10 percent of the applicable siting dose guideline values or violate the integrity of the primary coolant pressure boundary.

   C. When a CCF results in a plant response for which the safety analysis credits engineered safety feature (ESF) actuation and also impairs the ESF function, a diverse means not subject to or failed by the postulated failure should be provided to perform the ESF function. The diverse means should ensure that the plant response calculated using realistic assumptions and analyses does not result in a radiation release exceeding 10 percent of the applicable siting dose guideline values or violate the integrity of the primary coolant pressure boundary.

   D. No failure of monitoring or display systems should influence the functioning of the RTS or ESF. If a plant monitoring system failure induces operators to attempt to operate the plant outside safety limits or in violation of the limiting conditions of operation, the analysis should demonstrate that the protection system function will compensate for such operator-induced transients.

   E. To satisfy IEEE Std. 603-1991, Clauses 6.2 and 7.2, a safety-related means shall be provided in the control room to implement manual initiation of the automatically initiated protective actions at the system level or division level (depending on the design) of the RTS and ESF functions.

      i. This safety-related manual means shall minimize the number of discrete operator manual manipulations.

ii. This safety-related manual means shall depend on operation of a minimum amount of equipment.

iii. If a D3 analysis indicates that the safety-related manual initiation would be subject to the same potential CCF as the automatically initiated protective action, then a diverse manual means of initiating protective action would be needed (i.e., two manual initiation means would be needed).

F. Prioritization between safety and diverse nonsafety systems is necessary to ensure that the credited safety function can be accomplished by either system.

i. Diverse actuation signals should be applied to plant equipment control circuits downstream of the digital system to which they are diverse to ensure that the diverse actuation will be unaffected by digital system failures and malfunctions. Accordingly, the priority modules that combine the diverse actuation signals with the actuation signals generated by the digital system should not be executed in digital system software that may be subject to CCF.

ii. Safety-related commands that direct a component to a safe state must always have the highest priority and must override all other commands.

iii. Commands that originate in a safety-related channel, but which only cancel or enable cancellation of the effect of the safe-state command (i.e., a consequence of a CCF in the primary system that erroneously forces the plant equipment to a state that differs from the designated safe state) and which do not directly support any safety function, have lower priority and may be overridden by other commands.

iv. The reasoning behind the proposed priority ranking should be explained in detail. The reviewer should refer the proposed priority ranking and its explanation to appropriate systems experts for review.

v. The priority module itself should be shown to apply the commands correctly in order of their priority rankings and should meet all other applicable guidance. The application should demonstrate that the unavailability or spurious operation of the actuated device is accounted for in, or bounded by, the plant safety analysis.

G. While the D3 assessment should consider failure of the protection system to actuate a safety function when plant conditions require a trip or actuation in response to a CCF of the automated protection system, failures of the automated protection system stemming from a software CCF may cause spurious actuations. The plant design basis addresses the effects of certain spurious actuations caused by a software CCF.

i. The overall D3 strategy of a plant should prevent or mitigate the effects of credible spurious actuations caused by a software CCF that

have the potential to place a plant in a configuration that is not bounded by the plant's design basis.

ii. The effects of some credible postulated spurious actuations caused by a software CCF in the automated protection system may not be evaluated in the design basis accident analyses. In these cases, an analysis should be performed to determine whether these postulated spurious actuations could result in a plant response that results in conditions that do not fall within those established as bounding for plant design. The analysis should also identify whether coping strategies—whether for prevention or mitigation—exist for these postulated spurious actuations (e.g., emergency, normal, and diverse equipment and systems, controls, displays, procedures, and the reactor operations team) and consider adequacy of such strategies.

iii. If existing coping strategies are not effective for responding to the credible postulated spurious actuations that result in the plant exceeding its design basis, the application should develop and present additional coping strategies.

iv. The reviewer should confirm that the application's analysis identified a coping strategy for the effects of credible spurious actuations caused by a CCF that have the potential to place the plant in a configuration that is not bounded by the plant's design-basis accident analyses.

2. Conformance with 10 CFR 50.62

   The reviewer should verify that the diverse actuation system functions are independent and diverse from the RTS and engineered safety features actuation system (ESFAS). ATWS mitigation systems should be diverse from the RTS. For ATWS mitigation systems, 10 CFR 50.62 requires diversity from the sensor output to the final actuation device.

3. Considerations

   A. Since CCF is not classified as a single failure (as defined in RG 1.53), design-basis evaluations need not assume that a postulated CCF is a single failure. Consequently, analyses can employ realistic assumptions to evaluate the effect of CCF coincident with DBEs.

   B. In reviewing the D3 analysis using the above acceptance criteria, the reviewer should find that the analysis of the D3 design features conforms to the guidance of NUREG/CR-6303.

IV. Evaluation Findings

The I&C systems (1) satisfy the requirement of IEEE Std. 603-1991 with regard to D3 and (2) conform to the guidelines in the SRM to SECY-93-087 and NUREG/CR-6303 with regard to D3. Based on its review of these analyses, the staff concludes that the system is designed with sufficient diversity to cope with a DBE concurrent with a CCF that disables the safety function and the application adequately addressed the requirements for D3.

V. Implementation

The staff will use this DSRS section in performing safety evaluations of mPower™-specific design certification (DC), combined license (COL), or early site permit (ESP) applications submitted by applicants pursuant to 10 CFR Part 52. The staff will use the method described herein to evaluate conformance with Commission regulations.

Because of the numerous design differences between the mPower™ and large light-water nuclear reactor power plants, and in accordance with the direction given by the Commission in SRM- COMGBJ-10-0004/COMGEA-10-0001, "Use of Risk Insights to Enhance the Safety Focus of Small Modular Reactor Reviews," dated August 31, 2010 (ML102510405), to develop risk-informed licensing review plans for each of the small modular reactor (SMR) reviews including the associated pre-application activities, the staff has developed the content of this DSRS section as an alternative method for mPower™ -specific DC, COL, or ESP applications submitted pursuant to 10 CFR Part 52 to comply with 10 CFR 52.47(a)(9), "Contents of applications; technical information."

This regulation states, in part, that the application must contain "an evaluation of the standard plant design against the Standard Review Plan (SRP) revision in effect 6 months before the docket date of the application." The content of this DSRS section has been accepted as an alternative method for complying with 10 CFR 52.47(a)(9) as long as the mPower™ DCD FSAR does not deviate significantly from the design assumptions made by the NRC staff while preparing this DSRS section. The application must identify and describe all differences between the standard plant design and this DSRS section, and discuss how the proposed alternative provides an acceptable method of complying with the regulations that underlie the DSRS acceptance criteria. If the design assumptions in the DC application deviate significantly from the DSRS, the staff will use the SRP as specified in 10 CFR 52.47 (a)(9). Alternatively, the staff may revise the DSRS section in order to address new design assumptions. The same approach may be used to meet the requirements of 10 CFR 52.17 (a)(1)(xii) and 10 CFR 52.79 (a)(41), for ESP and COL applications, respectively.

Just as the SRP is not substitute for the regulations and compliance with the SRP is not a requirement, the DSRS is not a substitute for the regulations and compliance with the DSRS is not a requirement. If the applicant proposes an alternative method for complying with specified portions of the Commission's regulations, the applicant must demonstrate the acceptability of its alternate method.

VI. References

All of the references in this DSRS Chapter 7, "Instrumentation and Controls," may be found in Appendix D, of this Chapter.

Appendix A

Evaluation of Hazard Analysis

[Reserved]

Appendix B

I&C System Architecture

Introduction

The I&C system architecture provides high-level definition of I&C systems, the assignment of I&C functions to these systems, and the communications between I&C systems. The implementation of the defense-in-depth concept for I&C is achieved mostly at the I&C architectural level. This section provides an approach to describe the I&C system architecture and identifies relevant information to assess the design's conformance to the defense-in-depth concept and the relevant regulations (e.g., 10 CFR 50.55a(h)).

DSRS Chapter 7 sections on the fundamental design principles discuss more specific areas of staff review that take into account the overall I&C architecture. In addition, the actual system development process typically includes, as part its development life cycle, the development of system architecture descriptions. The application should contain sufficient information on architecture, whether or not a specific platform or technology has been selected, to support the staff's determination of reasonable assurance of safety from the perspective of the fundamental design principles: independence, diversity and defense-in-depth, redundancy, and determinism.

Without the information related to the overall I&C system architecture, the review of the fundamental design principles may take on a more segmented review approach resulting in a less streamlined, more complicated, and more resource-intensive review effort.

Relevant Information to Support Consideration of I&C Architecture during Design Review

Clause 4 of IEEE 603 requires in part that a specific basis be established for the design of each safety system, including all system functions necessary to fulfill the system's safety intent. The architecture description provides a representation of the I&C system's properties, elements, functions, and the relationship among them. The architectural description should also contain the rationale, justification, or reasoning about architecture decisions that have been made, including potential consequences of such decisions.

The reviewer should consider the I&C system overall architecture in concert with the sections relating to the fundamental design principles. In addition, the reviewer should consider other sections of the DSRS that discuss the I&C system design basis, provide I&C system descriptions, and identify I&C system functions for consistency and additional information.

The reviewer, using engineering judgment that is corroborated in the review of each of the sections of this chapter, should verify that the application contained sufficient information at the architectural level to support a more streamlined and less complicated review.

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

1. Description of the I&C system architecture
2. All I&C functions that are part of the design basis
3. Diagrams of the overall architecture

4. Description of systems necessary to support the defense-in-depth concept of the plant, which provides layers of defensive capabilities to mitigate or prevent potential hazards, including the following:

    A. Interfaces between the individual I&C safety systems

    B. all safety to nonsafety interfaces

    C. End-to-end signal flows and their descriptions (e.g., signal direction, signal authentication schemes, error checking features, failure consequences)

    D. 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

    E. Simplified logic diagrams

    F. Signal processing block diagrams and their descriptions

    G. When a vendor's design includes a prioritization scheme that is used to signal selections, the priority functions and their descriptions

    H. Interfaces and comparisons of electrical and I&C diagrams

Appendix C

Simplicity

Introduction

Simplicity is considered to be a cross-cutting principle that affects the fundamental design principles. For safety I&C systems, designers and regulators are faced with the question of what measures should be in place in order to maintain other design principles such as independence and defense-in-depth with reasonable confidence. At a generic level, it is difficult to define and control simplicity/complexity for digital safety I&C systems. When faced with several design options on how to implement a function, from a safety perspective, the more simple design options are those that accomplish the function and address potential hazards with the most confidence and clarity. Additional guidance on hazards is contained in Appendix A, "Hazard Analysis."

This Appendix provides an approach to evaluate whether simplicity has been considered in the design of the digital I&C system. Although there are no regulations, standards, or guidance to address the aspect of simplicity for digital I&C systems, recent experience in reviews of light water reactor applications has shown that complex I&C systems challenge the demonstration of conformance with safety system design criteria such as independence. In this context, the NRC considers simplicity as supporting all fundamental design principles for developing safety systems with high reliability. The application should contain sufficient information on the simplicity of the design to support the staff's determination of reasonable assurance of safety from the perspective of the fundamental design principles: independence, diversity and defense-in-depth, redundancy, and determinism. The reviewer should verify that the approach described in the application addresses specific effects of simplicity such as testability or proof-of-determinism.

Without the information related to the simplicity of the I&C system, the review of the fundamental design principles may take on a more segmented review approach resulting in a less streamlined, more complicated, and more resource-intensive review effort.

Relevant Information to Support Consideration of I&C Architecture during Design Review

The application should provide sufficient information to demonstrate that the design of the I&C systems considered simplicity both in the functionality of the system, as well as, in its implementation. With this information, the reviewer should confirm that simplicity attributes such as single function, fixed number of inputs and outputs, fewer configuration parameters, high testability, software architecture with no branching and minimal interrupts, etc. , are considered and incorporated in the design. These attributes help contribute to simplicity and enable high efficiency in the design.

The following areas related to the design of a plant's I&C systems should be considered in order to demonstrate that such systems meet the fundamental design principle of simplicity:

1. I&C system architecture.
2. Hazards analysis.
3. Independence.
4. Redundancy.
5. Determinism.

6. Diversity and defense-in-depth.

The staff should consider whether: (1) the I&C design is as simple as practical, and (2) that any added complexity does not diminish the design's conformance to the fundamental design principles. For those areas that exhibit complexity, the application should provide a full description regarding any complexity added to the I&C system design, as well as, a justification necessary to directly support the safety function. More complex design alternatives require a more resource intensive review by the staff and could potentially lengthen the review.

The reviewer should consider the following items in evaluating simplicity in an I&C system design:

1. This review is concurrent with the other fundamental design principles of redundancy, independence, diversity, and determinism contained in Chapter 7.1.

2. I&C System Architecture: The I&C architecture information described in Appendix B of Chapter 7 should be carefully considered to determine if the I&C design includes unnecessary or nonessential features that are not part of the safety function. The reviewer should also consider the following:

   A. The application should provide a top-down decomposition of the I&C system. This decomposition facilitates a logical, modular description of interactions, signal flows, help with the definition of interfaces, and allows a more effective review.

   B. The selected architecture should provide a demonstration of a balance between simplicity in concept and the capacity to satisfy regulatory and performance requirements. This includes deterministic behavior, independence, and redundancy.

   C. A safety benefit should be independently verifiable and should outweigh any concerns associated with the complexity it may introduce in the design.

   D. Digital I&C system and software components should be organized in a manner that promotes design simplicity.

   E. After reviewing information related to the I&C system's architecture, the reviewer should consider whether:

      a. A structured and modular architecture is applied.
      b. The system, hardware and software elements, all relationships among them, as well as properties of both are fully described and address relevant requirements

3. Independence: Material from the independence section may be used by the reviewer to identify how simplicity is addressed in the design while considering IEEE 603. Specifically, the reviewer should consider the following:

   A. Whether inter-channel communications or communications between a safety and a non-safety system exist in this design.

B. Whether simplicity is implemented to reduce or eliminate inter-divisional communication, or implemented physical uni-directional communication in function processing and critical signal paths.

C. Whether the design maintains separation or segregation among I&C functions within the circuitry, as it enhances simplicity, verifiability and testability of individual functions.

The reviewer should consider whether the application proposed simple design options in the approach to address IEEE Std. 603. The following design attributes support this approach:

A. There is adequate separation or segregation among I&C functions.

B. There are no unnecessary inter-channel communications.

C. There are no unnecessary communications between a safety and a nonsafety system unless the safety system is out of service.

4. Redundancy: Material from the redundancy section may be used by the reviewer to identify how the design achieved redundancy and avoided unnecessary complexity. Specifically, the reviewer may consider the following areas that could help identify unnecessary complexity:

   A. Ancillary, more complex functions are kept independent of the primary I&C safety functions.

   B. The design provides simple connections between redundant trains.

   C. The proposed design did not consider inter-channel communications.

   D. There are no communications between a safety and a non-safety system, unless the safety system is out of service.

   Through the review of redundancy, the reviewer may:

   A. Consider whether simplicity is factored in the design, particularly for the primary I&C functions.

   B. Consider whether complex functions are kept independent of the primary I&C safety functions.

5. Determinism: Material from the determinism section may be used by the reviewer to identify how simplicity is addressed to demonstrate deterministic behavior. Specifically, the reviewer may consider the following:

   A. Simple algorithms are considered in the design of system modules. In general, simplicity should not be sacrificed to achieve performance that is not required.

   B. I&C systems are designed using a finite state machine approach with all states well defined.

Through the review of determinism, the reviewer may:

A. Consider whether non-safety features are segregated from the main safety signal path.

B. Consider whether there are interrupt functions that could interfere with the performance of the safety function.

C. Consider whether early detection of failures is facilitated by the self-diagnostic functions.

6. Diversity and Defense-in-Depth: Simplicity of a software structure is promoted through simple logic, cyclical execution, static resource usage, and avoidance of external interrupts. Material from the diversity and defense-in-depth section may be used by the reviewer to identify how simplicity is addressed to demonstrate diversity. Specifically, the reviewer may consider the following:

   A. How potential common cause failures (CCFs) are addressed and how simplicity is considered to address failures.

   B. If basic software and application software are separated, and if it is implemented in a high level programming language.

   C. If basic software performs only the minimal necessary functions, such as initialization, periodic execution of required functions, and error handling.

   D. If application software is described in a graphically symbolized manner, so that functions can be easily understood, verified and validated.

   E. If the design is proposing dynamic allocation of memory.

   Through the review of diversity and defense-in-depth, the reviewer may:

   A. Consider whether basic software and application software are separated.

   B. Consider whether basic software is implemented in a high level programming language.

   C. Consider whether basic software performs only the minimal necessary functions, such as initialization, periodic execution of required functions, and error handling.

   D. Consider whether application software is described in a graphically symbolized manner, so that functions can be easily understood, verified and validated.

   E. Consider whether there is dynamic allocation of memory.

7. The following are additional examples of system features that could introduce unnecessary complexity to the I&C design and should also be carefully considered:

   A. Features or functionalities added to operational enhancement.

B. Features added that could introduce interrupts to the critical safety system performance.

C. Features added to cope with particular types of hazards that could negatively impact other safety design features.

D. Excessive use of self-diagnostics or use of self-diagnostics that significantly increase risk of module failure over any substantial benefit to reliability.

E. Provisions for troubleshooting and maintenance, including built-in self-test features, and external testing of circuit boards if necessary - consider accessibility of test points, need for special test equipment, and coverage of built-in self-testing and diagnostics.

Appendix D

References

1. ANSI Std C84.1-1989, American National Standard for Electric Power Systems and Equipment C Voltage Ratings (60 Hz)

2. ANSI/ANS Std. 4.5-1980, Criteria for Accident Monitoring Functions in Light Water Cooled Reactors

3. ANSI/ASME NQA-1-1983, Quality Assurance Program Requirements for Nuclear Facilities

4. ANSI/ASME NQA-1a-1983 Addenda, Addenda to ANSI/ASME NQA-1-1983, Quality Assurance Program Requirements for Nuclear Facilities

5. ANSI/NCSL Std. Z540 1-1994, Calibration Laboratories and Measuring and Test Equipment General Requirements

6. ASME Std. NQA 1-1994, Quality Assurance Requirements for Nuclear Facility Applications

7. BAW 1564, Integrated Control System Reliability Analysis. Babcock and Wilcox, August 17, 1979

8. BTP ICSB 18 (PSB)

9. EPRI NP-5652, Guideline for the Utilization of Commercial Grade Items in Nuclear Safety-related Applications, June 1988

10. GL 85 06, Quality Assurance Guidance for ATWS Equipment That Is Not Safety-related, April 16, 1986

11. GL 87-12, Loss of Residual Heat Removal (RHR) While the Reactor Coolant System (RCS) is Partially Filled

12. GL 88-17, Loss of Decay Heat Removal

13. GL 88-20, Individual Plant Examination for Severe Accident Vulnerabilities, November 23, 1988

14. GL 89-02, Actions to Improve the Detection of Counterfeit and Fraudulently Marketed Products, 1989

15. GL 91 05, Licensee Commercial Grade Procurement and Dedication Programs, 1991

16. GL 91-04, Guidance on Preparation of a Licensee Amendment Request for Changes in Surveillance Intervals to Accommodate a 24 Month Fuel Cycle, April 2, 1991

17. IEC 60880-2, Software for Computers Important to Safety for Nuclear Power Plants Part 2: Software Aspects of Defense Against Common Cause Failures, Use of Software Tools and of Pre Developed Software, 2000

18. IEC 61000-3-2, Electromagnetic Compatibility (EMC) Part 3 2: Limits for Harmonic Current Emissions, International Electrotechnical, Commission, 2001

19. IEC 61000-3-4, Electromagnetic Compatibility (EMC) Part 3 4: Limits Limitation of Emission of Harmonic Currents in Low Voltage Power Supply Systems for Equipment with Rated Current Greater than 16 A, 1998

20. IEC 61000-4-1, Electromagnetic Compatibility (EMC) Part 4: Testing and Measurement Techniques, Section 1: Overview of Immunity Tests, 1992

21. IEC 61000-4-10, Electromagnetic Compatibility (EMC) Part 4: Testing and Measurement Techniques, Section 10: Damped Oscillatory Magnetic Field Immunity Test, 1993

22. IEC 61000-4-11, Electromagnetic Compatibility (EMC) Part 4: Testing and Measurement Techniques, Section 11: Voltage Dips, Short Interruptions, and Voltage Variations Immunity Test, 1994

23. IEC 61000-4-12, Electromagnetic Compatibility (EMC) Part 4: Testing and Measurement Techniques, Section 12: Oscillatory Waves Immunity Tests, 1996

24. IEC 61000-4-13, Electromagnetic Compatibility (EMC) Part 4: Testing and Measurement Techniques, Section 13: Immunity to Harmonics and Interharmonics, 1998

25. IEC 61000-4-16, Electromagnetic Compatibility (EMC) Part 4: Testing and Measurement Techniques, Section 16: Test for Immunity to Conducted, Common Mode Disturbances in the Frequency Range 0 Hz to 150 kHz, 1998

26. IEC 61000-4-2, Electromagnetic Compatibility (EMC) Part 4: Testing and Measurement Techniques, Section 2: Electrostatic Discharge Immunity Test, 1995

27. IEC 61000-4-3, Electromagnetic Compatibility (EMC) Part 4: Testing and Measurement Techniques, Section 3: Radiated, Radio Frequency, Electromagnetic Field Immunity Test, 1995

28. IEC 61000-4-4, Electromagnetic Compatibility (EMC) Part 4: Testing and Measurement Techniques, Section 4: Electrical Fast Transient/Burst Immunity Test, 1995

29. IEC 61000-4-5, Electromagnetic Compatibility (EMC) Part 4: Testing and Measurement Techniques, Section 5: Surge Immunity Test, 1995

30. IEC 61000-4-6, Electromagnetic Compatibility (EMC) Part 4: Testing and Measurement Techniques, Section 6: Immunity to Conducted Disturbances, Induced by Radio Frequency Fields, 1996

31. IEC 61000-4-7, IEC 61000-4-7, Electromagnetic Compatibility (EMC) Part 4: Testing and Measurement Techniques, Section 7: General Guide on Harmonics and Interharmonics

Measurements and Instrumentation, for Power Supply Systems and Equipment Connected Thereto, 1991

32. IEC 61000-4-8, Electromagnetic Compatibility (EMC) Part 4: Testing and Measurement Techniques, Section 8: Power Frequency Magnetic Field Immunity Test, 1993

33. IEC 61000-4-9, Electromagnetic Compatibility (EMC) Part 4: Testing and Measurement Techniques, Section 9: Pulse Magnetic Field Immunity Test, 1993

34. IEC 61000-6-4, Electromagnetic Compatibility (EMC) Part 6: Generic Standards, Section 4: Emission Standard for Industrial Environments, 1997

35. IEEE Std 100-2000, The Authoritative Dictionary of IEEE Standards Terms 7th Edition

36. IEEE Std 1058.1-1991, IEEE Standard for Software Project Management Plans

37. IEEE Std 1058-1998, IEEE Standard for Software Project Management Plans

38. IEEE Std 1061-1998, IEEE Standard for a Software Quality Metrics Methodology

39. IEEE Std 12207.0-1996, IEEE/EIA Standard - Industry Implementation of International Standard ISO/IEC 12207:1995 (ISO/IEC 12207), Standard for Information Technology - Software Life Cycle Processes

40. IEEE Std 1228-1994, IEEE Standard for Software Safety Plans

41. IEEE Std 1540-2001, IEEE Standard for Life Cycle Processes B Risk Management

42. IEEE Std C37.90.1-2002, IEEE Standard for Surge Withstand Capability (SWC) Tests for Relays and Relay Systems Associated with Electric Power Apparatus

43. IEEE Std C62.36 2000, IEEE Standard Test Methods for Surge Protectors Used in Low Voltage Data, Communications, and Signaling Circuits

44. IEEE Std. 1008-1987, IEEE Standard for Software Unit Testing

45. IEEE Std. 1012-1998, IEEE Standard for Software Verification and Validation

46. IEEE Std. 1028-1988, IEEE Standard for Software Reviews and Audits

47. IEEE Std. 1028-1997, IEEE Standard for Software Reviews

48. IEEE Std. 1042-1987, IEEE Standard for Software Reviews, IEEE Guide to Software Configuration Management

49. IEEE Std. 1050-1996, IEEE Guide for Instrumentation and Control Equipment Grounding in Generating Stations

50. IEEE Std. 1074-1995, IEEE Standard for Developing Software Life Cycle Processes

51. IEEE Std. 1100-1999, IEEE Recommended Practice for Powering and Grounding Electronic Equipment (IEEE Emerald Book)

52. IEEE Std. 142 -1991, IEEE Recommended Practice for Grounding of Industrial and Commercial Power Systems (IEEE Green Book)

53. IEEE Std. 323-1974, IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations

54. IEEE Std. 338- 1987, Standard Criteria for the Periodic Surveillance Testing of Nuclear Power Generating Station Safety Systems

55. IEEE Std. 367-1996, IEEE Recommended Practice for Determining the Electric Power Station Ground Potential Rise and Induced Voltage from a Power Fault

56. IEEE Std. 379-2000, Standard Application of the Single Failure Criterion to Nuclear Power Generating Station Safety Systems, (R2008)

57. IEEE Std. 384-1992, IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits

58. IEEE Std. 473-1985, IEEE Recommended Practice for an Electromagnetic Site Survey (10 kHz to 10 GHz), Institute of Electrical and Electronics Engineers, reaffirmed 1997

59. IEEE Std. 487-2000, IEEE Recommended Practice for the Protection of Wire Line Communication Facilities Serving Electric Supply Locations

60. IEEE Std. 497-2002, IEEE Standard Criteria for Accident Monitoring Instrumentation for Nuclear Power Generating Stations

61. IEEE Std. 498-1990, IEEE Standard Requirements for the Calibration and Control of Measuring and Test Equipment Used in Nuclear Facilities

62. IEEE Std. 518-1982, IEEE Guide for the Installation of Electrical Equipment to Minimize Noise Inputs to Controllers from External Sources, Institute of Electrical and Electronics Engineers, reaffirmed 1996

63. IEEE Std. 610.12-1990, IEEE Standard Glossary of Software Engineering Terminology

64. IEEE Std. 665-1995, IEEE Guide for Generating Station Grounding, Institute of Electrical and Electronics Engineers (reaffirmed 2001)

65. IEEE Std. 666-1991, IEEE Design Guide for Electrical Power Service Systems for Generating Stations, (reaffirmed 1996)

66. IEEE Std. 7-4.3.2-2003, IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations

67. IEEE Std. 80-2000, IEEE Guide for Safety in AC Substation Grounding

68. IEEE Std. 81.2-1991, IEEE Guide for Measurement of Impedance and Safety Characteristics of Large, Extended or Interconnected Grounding Systems

69. IEEE Std. 81-1983, IEEE Guide for Measuring Earth Resistivity, Ground Impedance, and Earth Surface Potentials of a Ground System

70. IEEE Std. 828-1990, IEEE Standard for Software Configuration Management Plans

71. IEEE Std. 829-1983, IEEE Standard for Software Test Documentation

72. IEEE Std. 830-1993, IEEE Recommended Practice for Software Requirements Specifications

73. IEEE Std. 934-1987, Requirements for Replacement Parts for Class 1E Equipment in Nuclear Power Generating Stations

74. IEEE Std. C37.1 1994, IEEE Standard Definition, Specification, and Analysis of Systems Used for Supervisory Control, Data Acquisition, and Automatic Control

75. IEEE Std. C37.101-1993, IEEE Guide for Generator Ground Protection

76. IEEE Std. C57.13.3-1983, IEEE Guide for the Grounding of Instrument Transformer Secondary Circuits and Cases (reaffirmed 1990)

77. IEEE Std. C62.23-1995, IEEE Application Guide for Surge Protection of Electric Generating Plants, (reaffirmed 2001)

78. IEEE Std. C62.41.1-2002, IEEE Guide on the Surge Environment in Low Voltage (1000 V and Less) AC Power Circuits

79. IEEE Std. C62.41.2-2002, IEEE Recommended Practice on Characterization of Surges in Low Voltage (1000 V and Less) AC Power Circuits

80. IEEE Std. C62.41-1991, IEEE Recommended Practice on Surge Voltages in Low Voltage AC Power Circuits, reaffirmed 1995

81. IEEE Std. C62.45-1992, IEEE Guide on Surge Testing for Equipment Connected to Low Voltage AC Power Circuits, reaffirmed 1997

82. IEEE Std. C62.45-2002, IEEE Recommended Practice on Surge Testing for Equipment Connected to Low Voltage (1000 V and Less) AC Power Circuits

83. IEEE Std. C62.92.1-2000, IEEE Guide for the Application of Neutral Grounding in Electrical Utility Systems, Part I – Introduction

84. IEEE Std. C62.92.2-1989, IEEE Guide for the Application of Neutral Grounding in Electrical Utility Systems, Part II - Grounding of Synchronous Generator Systems(reaffirmed 2001)

85. IEEE Std. C62.92.3-1993, IEEE Guide for the Application of Neutral Grounding in Electrical Utility Systems, Part III - Generator Auxiliary Systems (reaffirmed 2000)

86. ISA S67.02-1980, Nuclear Safety-related Instrument Sensing Line Piping and Tubing Standards for Use in Nuclear Power Plants

87. ISA S67.04 1994, Part II, Methodology for the Determination of Setpoints for Nuclear Safety-related Instrumentation

88. ISA S67.04, Part I-1994, Setpoints for Nuclear Safety-related Instrumentation

89. MIL Std. 461C, Electromagnetic Emission and Susceptibility Requirements for the Control of Electromagnetic Interference

90. MIL Std. 461D, Electromagnetic Emission and Susceptibility Requirement for the Control of Electromagnetic Interference

91. MIL Std. 461E, Requirements for the Control of Electromagnetic Interference Characteristics of Subsystems and Equipment

92. MIL Std. 462, Measurement of Electromagnetic Interference Characteristics

93. MIL Std. 462D, Measurement of Electromagnetic Interference Characteristics

94. NEDO 33160 A, Revision 1, Regulatory Relaxation for the Post Accident SRV Position Indication System, 2006

95. NRC Inspection Manual, Inspection Procedure 52001, Digital Retrofits Receiving Prior Approval, March 2, 1998

96. NRC Inspection Manual, Inspection Procedure 93807, Systems Based Instrumentation and Control Inspection, 5/94

97. NUREG/CR-5560, Aging of Nuclear Plant Resistance Temperature Detectors, June 1990

98. NUREG/CR-6082, Data Communications, August 1993

99. NUREG/CR-6083, Reviewing Real Time Performance of Nuclear Reactor Safety Systems, August 1993

100. NUREG/CR-6090, The PLC and Its Application in Nuclear Reactor Protection Systems, 1993

101. NUREG/CR-6101, Software Reliability and Safety in Nuclear Reactor Protection Systems, 1993

102. NUREG/CR-6303, Method for Performing Diversity and Defense in Depth Analyses of Reactor Protection Systems, 1994

103. NUREG/CR-6421, A Proposed Acceptance Process for Commercial Off the Shelf (COTS) Software in Reactor Applications, 1996

104. NUREG/CR-6463, Review Guidelines on Software Languages for Use in Nuclear Power Plant Safety Systems, 1996

105. NUREG-0493, A Defense in Depth and Diversity Assessment of the RESAR 414 Integrated Protection System, 1979

106. NUREG-0694, TMI Related Requirements for New Operating Reactor Licenses, 1980

107. NUREG-0718, Licensing Requirements for Pending Applications for Construction Permits and Manufacturing License, 1981

108. NUREG-0737, Clarification of TMI Action Plan Requirements, 1982

109. NUREG-0737 Supplement 1, Clarification of TMI Action Plan Requirements - Requirements for Emergency Response Capability, 1983

110. NUREG-0809, Review of Resistance Temperature Detector Time Response Characteristics, August 1981

111. RG 1.100, Revision 3, Seismic Qualification of Electric Equipment for Nuclear Power Plants, 2009

112. RG 1.105, Revision 3, Setpoints for Safety-related Instrumentation, 1999

113. RG 1.118, Revision 3, Periodic Testing of Electric Power and Protection Systems, 1995

114. RG 1.151, Revision 1, Instrument Sensing Lines, 2010

115. RG 1.152, Revision 3, Criteria for Digital Computers in Safety Systems of Nuclear Power Plants, 2011

116. RG 1.153, Revision 1, Criteria for Safety Systems, 1996

117. RG 1.168, Revision 1, Verification, Validation, Reviews and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants, 2004

118. RG 1.169, Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants, 1997

119. RG 1.170, Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants, 1997

120. RG 1.171, Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants, 1997

121. RG 1.172, Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants, 1997

122. RG 1.173, Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants, 1997

123. RG 1.174, Revision 2, An Approach for Use Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Licensing Basis, 2011

124. RG 1.177, Revision 1, An Approach for Plant-Specific, Risk-Informed Decision Making: Technical Specifications, 2011

125. RG 1.180, Revision 1, Guidelines for Evaluating Electromagnetic and Radio Frequency Interference in Safety-related Instrumentation and Control Systems, 2003

126. RG 1.189, Revision 2, Fire Protection for Operating Nuclear Power Plants, 2009

127. RG 1.200, Revision 2, An Approach for Determining the Technical Adequacy of Probabilistic Risk Assessment Results for Risk-Informed Activities, 2009

128. RG 1.204, Guidelines for Lightning Protection of Nuclear Power Plants, 2005

129. RG 1.206, Combined License Applications for Nuclear Power Plants (LWR Edition), 2007

130. RG 1.209, Guidelines for Environmental Qualification of Safety-Related Computer-Based Instrumentation and Control Systems in Nuclear Power Plants, 2007

131. RG 1.22, Periodic Testing of Protection System Actuation Functions, 1972

132. RG 1.28, Revision 4, Quality Assurance Program Requirements (Design and Construction), 2010

133. RG 1.47, Revision 1, Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems, 2010

134. RG 1.53, Revision 2, Application of the Single Failure Criterion to Nuclear Power Plant Protection Systems, 2003

135. RG 1.62, Revision 1, Manual Initiation of Protection Action, 2010

136. RG 1.68, Revision 3, Initial Test Programs for Water-Cooled Nuclear Power Plants, August 2007

137. RG 1.70, Revision 3, Standard Format and Content of Safety Analysis Reports for Nuclear Power Plants, 1978, reviewed 2009

138. RG 1.75, Revision 3, Criteria for Independence of Electrical Safety Systems, 2005

139. RG 1.89, Revision 1, Environmental Qualification of Certain Electric Equipment Important to Safety for Nuclear Power Plants, 1984

140. RG 1.97, Revision 4, Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants, 2006

141. RIS 2006-17, NRC Staff Position on the Requirements of 10 CFR 50.36, A Technical Specifications,' Regarding Limiting Safety System Settings During Periodic Testing and Calibration of Instrument Channels, August 24, 2006

142. SE by NRR, August 11, 2000, Acceptance for Referencing of Topical Report CENPD 396 P, Revision 1, Common Qualified Platform

143. SE by NRR, December 11, 2001, Review of Triconex Corporation Topical Report 7286 545, Qualification Summary Report and 7286 545, Amendment 1 to Qualification Summary Report, Revision 1

144. SE by NRR, February 8, 2001, WCAP 15413, "Westinghouse 7300a ASIC Based Replacement Module Licensing Summary Report," Project No. 700

145. SE by NRR, January 13, 1993, Boiling Water Reactors, Regulatory Guide 1.97, Post Accident Neutron Flux Monitoring Instrumentation

146. SE by NRR, January 21, 1992, Pressurized Water Reactors Accumulator Pressure and Volume Instrumentation Relaxation of Regulatory Guide 1.97 Environmental Qualification Requirements

147. SE by NRR, July 17, 1997, EPRI Topical Report TR 106439

148. SE by NRR, July 30, 1998, Electric Power Research Institute Topical Report TR 107330, Generic Requirements Specification for Qualifying a Commercially Available PLC for Safety-related Applications in Nuclear Power Plants

149. SE by NRR, May 5, 2000, Siemens Power Corporation, Topical Report EMF 2110(NP), "Teleperm XS: A Digital Reactor Protection System"

150. SE by NRR, November 22, 1993, Pressurized Water Reactors Containment Sump Water Temperature Instrumentation, Regulatory Guide 1.97

151. SE by NRR, October 24, 2003, Palo Verde Nuclear Generating Station, Units 1, 2 and 3, "Issuance of Amendments on the Core Protection Calculator System Upgrade"

152. SE by NRR, September 25, 2006, Final Safety Evaluation for Boiling Water Reactor Owners' Group (BWROG) Topical Report (TR) NEDO 33160, Regulatory Relaxation for the Post Accident SRV [Safety Relief Valve] Position Indication System

153. SECY 91-292, Digital Computer Systems for Advanced Light Water Reactors, September 1991

154. SECY 93-087, Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light Water Reactor (ALWR) Designs, April 2, 1993

155. SRM SECY 93-087, Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light Water Reactor (ALWR) Designs, July 21, 1993

156. TR-106439, Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications, October 1996

157. TR-106453-3925, Temperature Sensor Evaluation, June 1996

158. TR-107330, Generic Requirements Specification for Qualifying a Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants, 1998