U.S. NUCLEAR REGULATORY COMMISSION

DESIGN-SPECIFIC REVIEW STANDARD FOR mPOWER^{TM} iPWR DESIGN

7.1 INSTRUMENTATION AND CONTROLS - FUNDAMENTAL DESIGN PRINCIPLES

REVIEW RESPONSIBILITIES

Primary - Organization responsible for the review of instrumentation and controls

Secondary - None

The organization responsible for the review of I&C should ensure that the application contains sufficiently detailed functional diagrams and explanations to demonstrate that the hardware and software for I&C architectures incorporate the fundamental design principles, namely independence; redundancy; predictability and repeatability; diversity and defense-in-depth (D3).

The reviewer must read Section 7.0 of this DSRS to understand the I&C review scope, applicable regulatory requirements, DSRS acceptance criteria, and interfaces with other DSRS Chapters.

ADAMS Accession No. ML12313A479

7.1.1 SAFETY SYSTEM DESIGN BASIS

I. AREAS OF REVIEW

The review will evaluate the specific design basis of each I&C safety system and ensure that the information provided for each design basis item is sufficient to enable the detailed design of the I&C system. The review will also verify that the I&C design is consistent with the credit taken in the safety analysis for the I&C system, including design basis, postulated design basis events (DBE) analyses, design descriptions, and operational characteristics of the safety systems.

Review Interfaces

The design basis information may be located in different chapters or sections of the application. The organization responsible for review of I&C safety systems should coordinate with the applicable U.S. NRC technical organizations, as identified in the review procedures section below, in proper identification of the design basis, postulated DBE analysis, system description, system operational characteristics, and the I&C requirements[1] for each safety system.

II. ACCEPTANCE CRITERIA

Requirements

1. 10 CFR 50.55a(h) requires compliance with Institute for IEEE Std. 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," including the correction sheet, dated January 30, 1995, which is referenced in paragraphs 10 CFR 50.55a(h)(2) and (3). This standard includes Section 4, "Safety System Designation." This section requires, in part, that a specific basis be established for the design of each safety system. 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 applicant must demonstrate that the proposed alternative would provide an acceptable level of quality and safety or that compliance with the specified requirements of 10 CFR 50.55a(h) would result in hardship or unusual difficulty without a compensating increase in the level of quality and safety.

2. General Design Criteria (GDC) 10, "Reactor Design," requires the reactor core and associated coolant, control, and protection systems be designed with appropriate margin to assure that specified acceptable fuel design limits are not exceeded during any

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

condition of normal operation, including the effects of anticipated operational occurrences (AOOs).

3. GDC 15, “Reactor coolant system design,” requires that the reactor coolant system and associated auxiliary, control, and protection systems be designed with sufficient margin to assure that the design conditions of the reactor coolant pressure boundary are not exceeded during any condition of normal operation, including AOOs.

4. GDC 16, “Containment Design,” requires reactor containment and associated systems be provided to establish an essentially leak-tight barrier against the uncontrolled release of radioactivity to the environment and to assure that the containment design conditions important to safety are not exceeded for as long as postulated accident conditions require.

5. GDC 19, “Control Room,” requires, in part, that equipment at appropriate locations outside the control room shall be provided (1) with a design capability for prompt hot shutdown of the reactor, including necessary instrumentation and controls to maintain the unit in a safe condition during hot shutdown, and (2) with a potential capability for subsequent cold shutdown of the reactor through the use of suitable procedures.

6. GDC 20, “Protection System Functions,” requires protection system be designed to: (1) initiate automatically the operation of appropriate systems, including the reactivity control systems, to assure that specified acceptable fuel design limits are not exceeded as a result of AOOs, and (2) sense accident conditions and to initiate the operation of systems and components important to safety.

DSRS Acceptance Criteria

There are no specific DSRS acceptance criteria in this section. However, the guidance provided below should be used to review the acceptability of the I&C system design basis documentation.

III. REVIEW PROCEDURES

The reviewer should confirm that the design bases, system design descriptions, system operation characteristics, postulated DBE analyses, and other information set forth in the application for each of the I&C safety systems satisfies the requirements of GDCs 10, 15, 16, 20, and Section 4 of IEEE Std. 603-1991. Many of the system characteristics contained in Section 7.2 of the DSRS are directly associated with the design bases documentation prescribed in IEEE Std. 603-1991, Section 4. These characteristics include, for example, identification of the I&C systems’ safety functions and corresponding protective actions, all monitored variables used to control each protective action, the minimum number and location of sensors required for protective purposes, critical points in time or plant conditions, and the range of transient and steady-state conditions throughout which the safety systems shall perform, including conditions having the potential for functional degradation of safety system performance.

Through a review of design information, including functional block diagrams, descriptions of operation, architectural descriptions, and other design details, the reviewer will confirm that the application contains information sufficient to demonstrate that the requirements contained in

Section 4 of IEEE Std. 603-1991 are satisfied. In addition, the reviewer will confirm that the design basis descriptions have the following characteristics:

1. Completeness - The design basis descriptions should address all system functions necessary to fulfill the system's safety purpose.

2. Consistency - The information provided in the design basis descriptions should be analyzed to confirm its conformance with the plant safety analysis, including the DBE analysis of Chapter 15 of the application, the mechanical and electrical system designs, and other plant system designs.

3. Correctness - The information provided for the design basis items should be technically accurate.

4. Traceability - It should be possible to trace the information in each design basis item to the safety analyses, plant system design documents, regulatory requirements, application commitments, or other plant documents.

5. Unambiguity - The information provided for the design basis items, taken alone and in combination should have one and only one interpretation. The design bases should not contain contradictory statements.

6. Verifiability - The information provided for the design basis items should be stated or provided in such a way as to facilitate the establishment of verification criteria and the performance of analyses and reviews of the various safety systems.

Additional considerations in the review of design basis information

The reviewer will confirm that the application contains a description of all functional requirements for the I&C systems and the operational environment for the I&C systems. The information provided for each design basis item should be sufficient to enable the detailed design of the I&C system to be carried out. As a minimum, each of the design basis aspects identified in IEEE Std. 603-1991, Sections 4.1 through 4.12, should be addressed. The following should be noted about Section 4 of IEEE Std. 603-1991:

1. Section 4.1 of IEEE Std. 603-1991 requires, in part, the identification of the DBEs applicable to each mode of operation along with the initial conditions and allowable limits of plant conditions for each such event. The reviewer should confirm that this information conforms to the analysis provided in Chapter 15 of the application. This includes a review of the DBEs that are examined, the selection of plant variables that are used to initiate protective action, and functional and performance requirements for systems and components. Although DBEs and corresponding safety functions are discussed in Chapter 15 of the application, the reviewer will gain an understanding of the DBEs considered and the initiating events that are analyzed to identify safety functions and protective actions of the execute features.

2. Section 4.2 of IEEE Std. 603-1991 requires, in part, the identification of safety functions and corresponding protective actions of the execute features for each DBE. Additional information to address this requirement is derived from Section 4.4 of IEEE Std. 603-1991, which addresses the identification of variables that are monitored in order to provide protective action.

3. Section 4.3 of IEEE Std. 603-1991 requires, in part, the identification of the permissive conditions for each operating bypass capability that is to be provided. Permissive signals are used to enable, disable, or modify the operation of actuation functions based on plant conditions. The reviewer should confirm that the application contains information sufficient to identify permissive conditions for each operating bypass capability that is provided in the design. The reviewer should consider Section 6.6 of IEEE Std. 603-1991, which provides requirements for operating bypasses applicable to sense and command features, and Section 7.4 of IEEE Std. 603-1991, which provides requirements for operating bypasses applicable to execute features. Additionally, Section 5.8.3 of IEEE 603-1991 requires the indication of bypasses.

4. Section 4.4 of IEEE Std. 603-1991 requires, in part, the identification of variables that are monitored in order to provide protective action. Performance requirements, including system response times, system accuracies, ranges, and rates of change of sensed variables to be accommodated until conclusion of the protective action, should be identified in the system designation. The reviewer should confirm that the application includes analyses, including the applicable portion provided in Chapter 15 of the application, demonstrating that system performance requirements are adequate to ensure completion of the protective actions. Additionally, variables that control each protective action by automatic means must be identified and documented using the criteria in Sections 6.1 and 7.1 of IEEE 603-1991. Section 4.4 also requires, in part, the identification of the analytical limit associated with each variable. The reviewer should confirm that an adequate margin exists between the analytical limits and the setpoints. In this context, adequate margin means the proper allowance for instrument uncertainties between 1) the device setpoint and the process analytical limit such that the system initiates protective actions before safety limits are exceeded, and 2) operating limits and setpoints such that there is a low probability for inadvertent actuation of the system. Additional information on setpoint requirements is in Section 6.8 of IEEE 603-1991, and setpoint guidance is contained Section 7.2.7 of this DSRS.

5. Section 4.5 of IEEE Std. 603-1991 describes the minimum criteria for determining whether manual initiation and control of protective actions is allowed. Specifically, the reviewer will confirm that the application describes:

   A. The points in time and plant conditions during which manual control is allowed. Section 4.10 of IEEE Std. 603-1991 requires the identification of critical points in time or the plant conditions for which safety system actuation is credited.
   B. The justification for permitting initiation or control subsequent to initiation solely by manual means.
   C. The range of environmental conditions imposed upon the operator during normal, abnormal, and accident conditions throughout which the manual operations shall be performed.
   D. The variables in Section 4.4 of IEEE Std. 603-1998 that shall be displayed for the operator to use in taking manual action. The reviewer should consider Section 5.8.1 of IEEE Std. 603-1991, which requires the display of manually controlled actions credited for the safety systems to accomplish their safety functions.

   Criteria for manual control of sense and command features are provided in Section 6.2 of IEEE Std. 603-1991, and criteria for manual control of execute features is provided in Section 7.2 of IEEE Std. 603-1991.

6. Section 4.6 of IEEE Std. 603-1991 requires, in part, the identification of the minimum number and location of sensors for those variables identified in Section 4.4 of IEEE Std. 603-1991 that have a spatial dependence. The reviewer should confirm that the application's analysis demonstrates that the number and location of sensors are adequate.

7. Section 4.7 of IEEE Std. 603-1991 requires that the design basis documentation include the range and steady-state transient conditions of both motive and control power and the environment (for example, voltage, frequency, radiation, temperature, humidity, pressure, and vibration) during normal abnormal, and accident circumstances throughout which the safety system shall perform. The reviewer should confirm that the application provides information sufficient to address the range and steady-state transient conditions during normal, abnormal, and accident conditions stated above.

8. Section 4.8 of IEEE Std. 603-1991 requires, in part, identification of the conditions having the potential for functional degradation of safety system performance (including missiles, pipe breaks, fires, loss of ventilation, spurious operation of fire suppression systems, operator error, failure in non safety-related systems, etc.). The application should contain information sufficient to identify conditions having the potential for functional degradation of safety system performance as well as the provisions that are incorporated in the design to maintain each system's capability for performing its safety functions. The reviewer should confirm that the application complies with the independence criteria contained in Section 5.6 of IEEE Std. 603-1991 and the criteria for interactions between sense and command features and other systems contained in Section 6.3 of IEEE Std. 603-1991.

9. Section 4.9 of IEEE Std. 603-1991 requires the identification of the methods used to determine that the reliability of the safety system design is appropriate for each such design, and the identification of the methods used to verify that any qualitative or quantitative reliability goals imposed on the system design have been met. The reviewer will determine the acceptability of system reliability based on the criteria described in IEEE Std. 603-1991 and IEEE Std. 7-4.3.2. The reviewer should also confirm that the application complies with the single failure criterion requirements of Section 5.1 of IEEE Std. 603-1991 and the reliability criteria contained in Section 5.15 of IEEE Std. 603-1991.

10. Section 4.10 of IEEE Std. 603-1991 requires identification of the critical points in time or plant conditions after the onset of a design basis event including: (1) the point in time or plant conditions for which the protective actions of the safety system shall be initiated, (2) the point in time or plant conditions that define the proper completion of the safety function, (3) the point in time or the plant conditions that require automatic control of protective actions, and (4) the point in time or the plant conditions that allow return of a safety system to normal. The reviewer should confirm that the application contains sufficient information to address the critical points in time or plant conditions outlined in Items 1-4. Requirements for automatic and manual initiation and control of protective actions for sense and command features are set forth in Sections 6.1 and 6.2 of IEEE Std. 603-1991, respectively. Requirements for automatic and manual initiation and control of protective actions for execute features are set forth in Sections 7.1 and 7.2 of IEEE Std. 603-1991, respectively.

11. Section 4.11 of IEEE Std. 603-1991 requires documentation of equipment protective provisions that prevent the safety systems from accomplishing their safety functions. The safety-related systems must be designed to accomplish their safety-related functions in accordance with the single failure criterion in Section 5.1 of IEEE Std. 603. The reviewer should also consider the system's capability for test and calibration and the hazard analyses performed on the system as part of this finding. Additional guidance related for test and calibration and hazard analyses is contained in Section 7.2.15 and Appendix A of this DSRS.

12. Section 4.12 of IEEE Std. 603-1991 requires the documentation of any other special design basis that may be imposed on the system design, such as diversity, interlocks, or regulatory agency guidance criteria. These could include other necessary permissive signals that maintain safety-related interlocks, interlocks associated with plant operating modes, or interlocks that provide status and control signals to other systems and alarms.

Remote Shutdown Capability[2]

To the extent that the engineered safety feature (ESF) systems are used to achieve and maintain safe shutdown, the review of these systems in this section is limited to those features that are unique to safe shutdown and not directly related to accident mitigation. The features within the scope below may involve individual component control for safe shutdown versus system-level actuation for accident mitigation, or system-level controls used to achieve and maintain safe shutdown but not used for accident mitigation. System-level controls used for accident mitigation may also need to be reviewed below if the safe shutdown functions of these controls involve features or operating modes that are unique to their safe shutdown functions. This DSRS section also addresses the review of those systems credited for safe shutdown that are not classified as ESF systems.

During safe shutdown, reactivity control systems must maintain a subcritical condition of the core, and residual heat removal systems must operate to maintain adequate cooling of the core. For definitions of plant-specific shutdown conditions, see Chapter 16 in the applicant's safety analysis report (SAR).

1. The design should provide for control in locations removed from the main control room that may be used for manual control and alignment of safe shutdown system equipment needed to achieve and maintain hot and cold shutdown. This control equipment should

[2] Shutdown remote from the control room is not an event analyzed in the accident analysis in Chapter 15 of this DSRS. Specific scenarios have not been specified upon which the adequacy of shutdown capability remote from the control room is evaluated. However, smoke due to a fire in the control room has long been recognized as the type of event that could force the evacuation of the control room and result in a need to shut down remote from the control room. RG 1.189, "Fire Protection for Operating Nuclear Power Plants," establishes the bases for safe shutdown with respect to fire protection. Specifically, fire damage limits as they impact on safe shutdown have been established therein. These limits do not call for consideration of an additional, random, single failure in the evaluation of the capability to safely shut down as a consequence of-fires. The evaluation of conformance to R G 1.189 is addressed in SRP Section 9.5.1. Therefore, the application of the single-failure criterion to remote shutdown is only applicable for other events that could cause the control room to become uninhabitable. These events would not result in consequential damage or unavailability of systems credited for safe shutdown.

be capable of operating independently of (i.e., without interaction with) the equipment in the main control room. This equipment may include the remote shutdown station and other local controls.

2. Equipment in the remote shutdown stations should be designed in accordance with the same standards as the corresponding equipment in the main control room.

3. Remote shutdown station control transfer devices should be located remote from the main control room and their use should initiate an alarm in the control room.

4. In the event that control functions are transferred from the control room to the remote shutdown station, the design should display parameter indications in the remote shutdown station such that the operators have access to the same parameter indications that they would have relied upon in the control room. Section 7.2.13 of this DSRS provides guidance associated with the typical parameters that should be displayed to monitor the plant status of a prompt hot shutdown of the reactor, maintaining the unit in a safe condition during hot shutdown, and for subsequent cold shutdown.

5. The location should be consistent with the guidance used for the design of remote, alternative, and dedicated shutdown equipment, as appropriate.

6. Access to remote shutdown stations should be under strict administrative controls. (See DSRS Section 7.2.9)

IV. EVALUATION FINDINGS

If the reviewer confirms that the application conforms to the guidance identified above, including the coordination with those having primary review responsibility for the accident analysis, the staff can conclude that the application provides information sufficient to: 1) demonstrate that a documented design basis is established for the design of each I&C safety system of the nuclear power generating station, and 2) the proposed I&C design is conforms to with the safety systems' I&C requirements, including design basis, postulated DBE analyses, design descriptions, and operational characteristics of the safety systems. On such a basis, the reviewer can conclude that the design of I&C systems satisfies the applicable requirements of GDCs 10, 15, 16, 19, 20, and Section 4 of IEEE Std. 603-1991.

V. IMPLEMENTATION

The staff will use this DSRS section in performing safety evaluations of mPower^{TM} -specific DC, or COL, 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 (Agencywide Documents Access and Management System Accession No. 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 evaluation of an mPower™ -specific DC application 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 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 supplement the DSRS section by adding appropriate criteria in order to address new design assumptions. The same approach may be used to meet the requirements of 10 CFR 52.79(a)(41) for COL applications.

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 INDEPENDENCE

I. AREAS OF REVIEW

The review will evaluate the methods described in the application used to demonstrate independence of the I&C systems: (1) between redundant portions of a safety system, (2) between safety systems and the effects of a DBE, and (3) between safety systems and other systems, as required by 10 CFR 50.55a(h). The review addresses the concepts of physical independence, electrical independence, communications independence, and functional independence.

Review Interfaces

Other fundamental design principles, such as redundancy, diversity and defense-in-depth, and predictability and repeatability, inform the review of independence. In addition, the appendices to DSRS Chapter 7 provide additional guidance describing how the reviewer should consider the architectural description, simplicity, and hazard analysis techniques, and how they inform the staff's review of the system's independence.

II. ACCEPTANCE CRITERIA

Requirements

1. 10 CFR 50.55a(h) requires compliance with IEEE Std. 603-1991, including the correction sheet, dated January 30, 1995, which is referenced in paragraphs 10 CFR 50.55a(h)(2) and (3). This standard includes Section 5.6, "Independence." This section requires physical, electrical, and communication independence between redundant portions of safety systems, safety systems and the effects of DBEs, and safety systems and other systems.

2. GDC 13, "Instrumentation and Control," requires in part that instrumentation be provided to monitor variables and systems over their anticipated ranges for normal operations, for AOOs, and for accident conditions as appropriate to assure adequate safety. Appropriate controls should be provided to maintain these variables and systems within prescribed operating ranges.

3. GDC 21, "Protection System Reliability and Testability," 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.

4. 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.

5. 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

The specific DSRS acceptance criteria for independence are as follows:

1. The reviewer 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. Currently, RG 1.75 endorses IEEE Std. 384-1992, "Standard Criteria for Independence of Class 1E Equipment and Circuits," with identified exceptions and clarifications. The applicant should examine the version of RG 1.75 that applies to its application to identify the applicable standards.

   The relevant guidance includes electrical isolation criteria for circuits and electrical equipment that comprise or are associated with safety systems. Note that the evaluation of physical separation of electrical cables and power source independence is part of Chapter 8 of the DSRS and is not documented in this chapter. In addition, the reviewer should evaluate the following when assessing electrical independence:

   A. The reviewer should confirm that the design provides for the use of redundant power sources.

   B. The reviewer should verify that isolation devices are used for interfaces between (1) independent divisions and (2) safety systems and other systems. Isolation devices should be classified as part of the safety system and powered in accordance with 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. Accordingly, the reviewer should verify that each isolation device is powered by a safety related power source.

2. The system should conform to the communication independence guidance in the version of RG 1.152, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants," in place 6 months before the docket date of the application. Currently, RG 1.152 endorses IEEE Std. 7-4.3.2-2003, with identified exceptions and clarifications. The applicant should examine the version of RG 1.152 that applies to its application to identify the applicable standards.

III. REVIEW PROCEDURES

The reviewer will evaluate the I&C system design described in the application to confirm that it meets the independence requirements of GDCs 13, 21, 22, 24, and Section 5.6 of IEEE Std. 603-1991. Through a review of design information, including functional block diagrams, descriptions of operation, architectural descriptions, and other design details, the reviewer will confirm that the proposed design exhibits independence between: (1) redundant portions of a safety system, (2) safety systems and the effects of DBEs, and (3) 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

Physical Independence

Physical independence is attained by physical separation and physical barriers. The reviewer should consider whether the application contains sufficient information to demonstrate the separation of (1) redundant portions of the safety system and (2) safety (protection) and nonsafety-related (control) systems to confirm that all interfaces among redundant portions of the safety system and between safety systems and nonsafety systems have been properly identified and addressed. The reviewer 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. The relevant guidance includes physical separation criteria for circuits and electrical equipment that comprise or are associated with safety systems. Note that the review of physical separation of electrical cables is part of Chapter 8 of the DSRS and is not documented in this chapter.

Electrical Independence

The reviewer should confirm that the I&C systems conform to the electrical independence 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 criteria 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:

1. 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 of the DSRS and is not documented in this chapter.

2. The reviewer should confirm the use of redundant power sources. Note that the evaluation of power source independence is part of Chapter 8 of the DSRS and is not documented in this chapter.

3. The reviewer should 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 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 should also verify that each isolation device is powered by a safety related power source.

Communications Independence

Through a review of design information, including functional block diagrams, descriptions of operation, architectural descriptions, and other design details, the reviewer will confirm that the proposed design exhibits communication independence between: (1) redundant portions of the safety system, and (2) between safety and nonsafety systems. The reviewer should confirm that the design of the data communication meets the requirements of IEEE Std. 603-1991, Section 5.6. The reviewer should also confirm that data communication conforms to the guidance for the separation and isolation of data processing functions of interconnected computers contained in IEEE Std. 7-4.3.2, Clause 5.6, as endorsed by RG 1.152. The reviewer

should consider the following:

1. The application should provide detailed information to demonstrate that the safety function of each safety division is protected from adverse influence from outside the division. For the I&C architecture proposed by the applicant, the reviewer should evaluate the signal path of redundant channels from sensors to final actuation devices to confirm division independence.

2. A safety division should not be dependent upon any information or resource originating or residing outside its own division to accomplish its safety function. Each safety division should receive plant data only from sensors dedicated to that division and that data should not be shared among divisions. Data flows between redundant portions of safety systems should be limited to those credited for coincidence logic voting for actuation and interlocks used for the performance of safety functions.

3. For designs that implement sharing of data between trip processing units and voting unit processors, or among voting unit processors, the reviewer should confirm that the proposed design includes provisions to cope with a trip processing unit or voting unit processor experiencing a lock-up condition (also known as hang or freeze), whether the processor controls a reactor trip or engineered safeguards system function. Such design provisions should include the following:

   A. Any voting unit processor or trip processing unit experiencing a lock-up condition will produce an alarm in the main control room and send a trip signal to all voting unit processors or trip processor units for that channel/division.

   B. If any two or more voting unit processors or trip processing units experience a simultaneous lock-up condition, an alarm will be displayed in the main control room and a reactor trip will result.

   C. The means used for ensuring that a trip signal is produced from either a trip processing unit or voting unit processor that experiences a lock-up condition should be completely independent among safety divisions, should be hardware-based, and completely independent of software.

   These design provisions apply to microprocessor-based technology as well as other forms of complex logic such as programmable logic devices (e.g. Field Programmable Gate Arrays (FPGAs)).

4. Communication processing faults in one safety division should not adversely affect performance of the safety function in other divisions.

5. Functions that are not necessary for safety should be executed outside the safety system.

6. The application should identify communications methods, including communications protocols, memory allocation methods, and message formatting methodology. The following should be evaluated.

   A. The protocol selected for the data communication is adequate to support performance of all safety function of the supported systems.

B. Vital communication should be point-to-point by means of a dedicated medium. Vital communications include communications that are needed to support a safety function. Failure of vital communications could inhibit the performance of the safety function. The most common implementation of vital communications is the distribution of channel trip information to other divisions for the purpose of voting.

C. Vital communications, such as the sharing of channel trip decisions for the purpose of voting, should include provisions for ensuring that received messages are correct and are correctly understood. Such communications should employ error-detecting or error-correcting coding along with means for dealing with corrupt, invalid, untimely or otherwise questionable data. Error-correcting methods, if used, should be shown to reconstruct the original message exactly or designate the message as unrecoverable. None of this activity should affect the operation of the safety-function processor.

D. The communication process itself should be carried out by a communications processor separate from the processor that executes the safety function. The communication and function processors should operate asynchronously, sharing information only by means of dual-ported memory that is dedicated exclusively to this exchange of information. Access to the shared memory should be controlled in such a manner that the function processor has priority access to the shared memory to complete the safety function in a deterministic manner (consistent with section 7.1.4 of this DSRS).

E. The safety function processor should not perform communication handshaking, as well as using acknowledgment signals and should not accept interrupts from outside its own safety division.

F. The cycle time for the safety function processor should be determined in consideration of the longest possible completion time for each access to the shared memory. Guidance for reviewing cycle time is provided in Subsection 7.1.4, “Determinism,” of this DSRS.

G. Incoming message data should be stored in fixed predetermined locations in the shared memory and in the memory associated with the function processor.

H. Only desired data in predefined address, fixed format, fixed length, and structure should be accepted and processed by the receiving system. Unrecognized messages and data should be identified and discarded by the receiving system.

I. The effects of data communication equipment malfunction or failure that generates erroneous signals should be examined. Corrupted messages, missing messages and duplicate messages should be detected and repaired.

7. All safety functions should be performed without interruption by any other signals, regardless of whether these signals are valid or erroneous.

8. Communication faults should not adversely affect the performance of required safety functions. The potential hazards to and from the data communication equipment should

be reviewed. Provisions for communications should be analyzed for hazards and performance deficits posed by unneeded functionality and complication.

9. Priority modules should be safety-related. A command initiating a safety function should have the highest priority and should override lower priority commands. All requirements that apply to safety software should also apply to priority module software. The priority module software should be stored in the nonvolatile memories to prevent online alteration.

Functional Independence

Functional independence provides additional assurance regarding the isolation of a safety system from other safety systems. Functional independence seeks to prevent safety function failures by ensuring that physically and electrically independent portions of safety systems (with the exception of coincidence voting) do not depend on information from other independent portions of the safety system. The concept of functional diversity (using different parameters, different technologies, different logic or algorithms, or different actuation means to provide several ways of detecting and responding to a significant event) helps accomplish functional independence, but does not totally address it.

Consideration of functional independence in the I&C system design helps demonstrate that successful completion of the system's safety functions is not dependent upon any behavior, including failures and normal operation of another system, or upon any signals, data, or information derived from the other system. Functional independence could also be used as a means of achieving isolation between redundant systems.

Through a review of design information, including functional block diagrams, descriptions of operation, architectural descriptions, and other design details, the reviewer should verify that the following criteria related to functional independence are appropriately considered in the design of I&C systems:

1. Functional independence is supported by the architectural design and treatment of data that are shared between functions.

2. In computer systems, one-way, broadcast data communication should be used where computer based systems of a higher safety classification provide data to systems of lower safety classification. Hardware characteristics that enforce the one-direction communication feature (e.g., the use of a link that is connected only to a transmitter in the higher classified system and only to a receiver in the lower classified system) should be considered as the preferred means of ensuring one-directional communication.

IV. EVALUATION FINDINGS

If the reviewer confirms that the application conforms to the guidance identified above, the staff can conclude that the application provides information sufficient to demonstrate that the proposed I&C systems 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. On such a basis, the reviewer can conclude that the design of I&C systems satisfies the guidance contained in RG 1.75, RG 1.152, and RG 1.53, and independence requirements of GDCs 13, 21, 22, 24, and Section 5.6 of IEEE Std. 603-1991.

V. IMPLEMENTATION

This section is identical throughout this mPower™ DSRS Section 7.1. The reviewer must read Section 7.1.1 Safety System Design Basis subsection "V. Implementation".

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 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 application should provide information that describes what level of redundancy is used 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. In addition to the redundancy, the application should also describe the means employed in the I&C design for guarding against common cause failures.

Review Interfaces

Other fundamental design principles, such as independence, D3, and determinism, inform the review of redundancy. In addition, the appendices to DSRS Chapter 7 provide additional guidance describing how the reviewer should consider the architectural description, simplicity, and hazard analysis techniques, and how they inform the staff's review of the system's redundancy.

II. ACCEPTANCE CRITERIA

Requirements

1. 10 CFR 50.55a(h) requires compliance with IEEE Std. 603-1991, including the correction sheet, dated January 30, 1995, which is referenced in paragraphs 10 CFR 50.55a(h)(2) and (3). This standard includes Section 5.1, "Single-Failure Criterion." This section states, in part, that the safety system must perform all safety functions required for a DBE in the presence of (1) any single detectable failure within the safety systems concurrent with all identifiable, but non-detectable failures, (2) all failures caused by the single failure, and (3) all failures and spurious system actions that cause or are caused by the DBE requiring the safety functions.

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

The specific DSRS acceptance criteria for redundancy are as follows:

The system should conform to the physical and electrical independence guidance contained in the version of RG 1.53 in place 6 months before the docket date of the application. Currently, RG 1.53 endorses IEEE Std. 379-2000, "Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems," with identified exceptions and clarifications. The applicant should examine the version of RG 1.53 that applies to its application to identify the applicable standards.

III. REVIEW PROCEDURES

Through a review of design information, including functional block diagrams, descriptions of operation, architectural descriptions, and other design details, the reviewer should confirm that the application provides information sufficient to demonstrate that the guidance on the single failure criterion in RG 1.53 is satisfied. IEEE Std. 379 provides a detailed discussion of how the safety I&C systems address the single failure criterion that the reviewer will consider in the review.

In addition to satisfying the single-failure criterion, suitably implemented redundancy enables system testing without loss of function. Similarly, redundancy enables component bypass or removal from service without loss of function. Additional redundancy may be warranted when protection and control systems share common components.

The reviewer should consider the following when assessing redundancy:

1. The application should provide a single-failure analysis in accordance with IEEE Std. 603-1991, Section 5.1, 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 that: (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, (3) the design of a safety system is such that no single failure of a component will result in spurious actuations and (4) necessary action is taken to eliminate, prevent, or control failure modes.

3. The reviewer will confirm that the application provides information sufficient to demonstrate that all SSCs needed for safe shutdown have sufficient redundancy to satisfy 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 will 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 to address these issues.

4. The reviewer will confirm that the removal from service of any single safety system component does not result in a loss of the required minimum redundancy unless the reliable operation of the system can be otherwise demonstrated. The application should provide information to demonstrate how redundancy of channels implements the single-failure criteria as required by GDC 24. Channel redundancy should support safe removal of a channel from service (or channel bypass) for testing as prescribed by the technical specification.

The reviewer should also consider the following IEEE Std. 603-1991 requirements in the review of redundancy:

1. Section 5.7, which provides requirements for test and calibration of safety system equipment.

2. Section 6.3, which provides requirements for interactions between sense and command features and other systems.

3. Section 6.5, which provides requirements for test and calibration of sense and command feature sensors during reactor operations.

4. Section 6.7, which provides maintenance bypass requirements for sense and command features.

5. Section 7.5, which provides maintenance bypass requirements for execute features.

IV. EVALUATION FINDINGS

If the reviewer confirms that the application conforms to the guidance identified above, the staff can conclude that the application provides information sufficient to demonstrate that the design 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. On such a basis, the reviewer can conclude that the design of I&C systems satisfies the guidance contained in RG 1.53 and the redundancy requirements contained in GDCs 21, 24, and Section 5.1 of IEEE Std. 603-1991.

V. IMPLEMENTATION

This section is identical throughout this mPower™ DSRS Section 7.1. The reviewer must read Section 7.1.1 Safety System Design Basis subsection “V. Implementation”.

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 PREDICTABILITY AND REPEATABILITY

The review will evaluate the methods described in the application to demonstrate that the I&C system output is predictable and repeatable. Predictable and repeatable system behavior refers to the case in which input signals and system characteristics result in output signals through known relationships among the system states and responses to those states. Such a system will produce the same outputs for a given set of input signals (and the sequence of inputs) within well-defined response time limits to allow timely completion of credited actions. I&C safety systems should be designed to operate in such a predictable and repeatable manner, which is also called "deterministic" behavior.

I. AREAS OF REVIEW

For digital systems, the reviewer will evaluate the predictability and repeatability of the output of digital I&C and data communications systems. The objective of this review is to (1) verify that system timing derived from the analysis of DBEs has been allocated to the I&C system architecture as appropriate and has been satisfied in the I&C system design, (2) confirm that the I&C system design and communication protocols provide features to assure system (or logic) performance in terms of response to inputs and time to produce a response, and (3) confirm that hazards that could challenge predicted behavior have been adequately identified and accounted for in the design.

Review Interfaces

Other fundamental design principles, such as independence, D3, and redundancy, inform the review of I&C system output predictability and repeatability. In addition, the appendices to DSRS Chapter 7 provide additional guidance describing how the reviewer should consider the architectural description, simplicity, and hazard analysis techniques, and how they inform the staff's review of the I&C system output predictability and repeatability.

II. ACCEPTANCE CRITERIA

Requirements

1. 10 CFR 50.55a(h) requires compliance with IEEE Std. 603-1991, including the correction sheet, dated January 30, 1995, which is referenced in paragraphs 10 CFR 50.55a(h)(2) and (3). IEEE Std. 603-1991 provides requirements related to safety system performance and the timing of safety system response. The standard requires, in part, that safety systems have a documented design basis as follows:

   A. Section 4.4 specifies limits, ranges, and rates of change of variables that should be included in the documented design basis.

   B. Section 4.10 indicates that the applicant should identify critical points in time after the onset of a DBE that should be specified in the design basis.

   In addition, Section 5.5, "System Integrity," of IEEE Std. 603-1991 requires safety systems be designed to accomplish their safety-related functions under the range of conditions enumerated in the design basis. After initiation by either automatic or manual means, the sequence of protective actions (from receipt of a signal from the sense and command features to the actuated equipment that perform the safety function) shall go

to completion in conformance with IEEE Std. 603, Section 5.2, “Completion of Protective Action.”

2. GDC 13, "Instrumentation and Control," requires in part that instrumentation be provided to monitor variables and systems over their anticipated ranges for normal operations, for AOOs, and for accident conditions as appropriate to assure adequate safety. Digital instrumentation must respond quickly enough so that the behavior of variables can be ascertained by operators.

3. GDC 21, “Protection System Reliability and Testability,” requires, in part, that the protection system be designed for high functional reliability and in-service testability commensurate with the safety functions to be performed.”

4. 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 AOOs.

DSRS Acceptance Criteria

There are no specific DSRS acceptance criteria in this section. However, the guidance provided below should be used to review the acceptability of the I&C system output predictability and repeatability.

III. REVIEW PROCEDURES

Through a review of design information, including functional block diagrams, descriptions of operation, architectural descriptions, and other design details, the reviewer will confirm that the application conforms to the performance and timing requirements for safety systems contained in IEEE Std. 603-1991.

The timing of specific system responses credited in the safety analysis may affect the system architecture because it may not be possible to obtain sufficient computational performance for a specific function or group of functions from a single processor or the locations where functions are performed may be widely separated. Timing of credited actions may also increase complexity, either by fragmenting the system into multiple processors or by code tuning, which makes the software product (or logic) harder to understand, verify, and maintain.

The reviewer will confirm that the application provides a detailed timing analysis discussing how the I&C system and supporting communication systems address the concept of predictability and repeatability. Appendix B of this chapter provides guidance on the relationship between the I&C system architecture and predictability and repeatability. The reviewer should also consider the following IEEE Std. 603-1991 sections in the review of predictability and repeatability:

1. Section 4.4, regarding limits, ranges, and rates of change of variables should be included in the documented design basis.

2. Section 4.10, regarding critical points in time should be specified for after the onset of a DBE.

3. Section 5.5, regarding the capability of safety systems to accomplish their safety-related functions under the range of conditions enumerated in the design basis.

4. Section 5.2, regarding the sequence of protective actions (from receipt of a signal from the sense and command features to the actuated equipment that perform the safety function) that will go to completion after initiation by either automatic or manual means.

The reviewer should confirm that the application provides sufficient information (in the form of architectural descriptions, functional block diagrams, descriptions of operation, etc.) to demonstrate that the proposed system's real-time performance is repeatable, predictable, and known at all times.

The review will include the following when assessing predictability and repeatability:

1. Verify that the digital I&C system timing analysis identifies limiting response times, digital computer timing requirements, architecture, and design commitments.

2. The digital I&C system timing analysis should address all system components from signal collection to completion of protective action (e.g., sensor, transmitter, analog-to-digital converter, multiplexer, data communication equipment, de-multiplexer, computers, memory devices, controls, displays, logic processing, output processing, and voting).

3. Verify that the timing of specific system responses credited in the safety analysis have been allocated to the digital computer portion of the system, as appropriate, and have been satisfied in the digital system architectural design. Hardware and software design specifications should reflect these functional timing requirements.

4. Verify the digital I&C system timing analysis demonstrates that the protection safety functions are achieved within the times assumed in the safety analysis.

5. Verify that design practices that do not implement rigorous real-time and predictable and repeatable performance in digital I&C systems are documented. For those practices identified, verify (1) the methods used for controlling the associated risk have been documented, (2) such practices do not affect safety functions, and (3) the design does not impede any protective action.

6. Verify that data communications system timing is predictable and repeatable. Consider data rates, data bandwidths, and data precision for normal and off-normal operation, including the impact of environmental extremes. The application should make note of any delay that could impair the communication system's predictability and repeatability and provide a basis to conclude that such delays are neither part of any safety function 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.

7. The cycle time for the safety function processor should be determined in consideration of the longest possible completion time for each access to the shared memory assuming worst-case conditions for the transfer of access from the communications processor to the function processor. Failure of the system to meet the limiting cycle time should be detected and alarmed. To ensure predictable behavior, every datum in a message

packet should be included in every transmit cycle, whether it has changed since the previous transmission or not.

8. Verify that the processing cycle is defined, predictable, and repeatable within a specified sample time. In addition, the timing analysis should demonstrate that all safety functions are accomplished in each cycle or within a specific number of cycles. A discussion of why it is acceptable should be included in the application.

9. I&C safety systems that exhibit predictable and repeatable behavior, in general, should not be designed with the capability for unscheduled event-based disruptions or operator-based system functions that would inhibit or prevent the system from accomplishing its safety function. For software-based designs, predictable behavior also includes that the cycle time is repeatable with all safety functions accomplished in each cycle or within a specific number of cycles that is invariant.

10. Confirm that the I&C architecture design does not diminish the design's conformance with the other fundamental design principles.

IV. EVALUATION FINDINGS

If the reviewer confirms that the application conforms to the guidance identified above, the staff can conclude that the application provides information sufficient to demonstrate that the design of the I&C and data communication systems adequately address the fundamental design principle of predictability and repeatability at both the system and component levels as demonstrated in the applicant's timing analysis. On such a basis, the reviewer can conclude that the design of I&C systems satisfies the reliability, predictability, and repeatability requirements of GDCs 21, 29 and Sections 4.4, 4.10, 5.2, and 5.5 of IEEE Std. 603-1991.

V. IMPLEMENTATION

This section is identical throughout this mPower^{TM} DSRS Section 7.1. The reviewer must read Section 7.1.1 Safety System Design Basis subsection "V. Implementation".

VI. REFERENCES

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

7.1.5 DIVERSITY AND DEFENSE-IN-DEPTH

I. AREAS OF REVIEW

The objective of this review is to verify that (1) the I&C safety systems have a level of D3 such that there are two or more redundant systems or components which will be able to perform the safety functions credited in the safety analysis, (2) the different systems or components will have different attributes so as to reduce the likelihood of common cause failure (CCF), and (3) the displays and manual controls for critical safety functions initiated by operator action are diverse from digital systems used in the automatic portion of the protection systems. The 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. Conformance with these objectives is sufficient to demonstrate conformance to the applicable requirements of 10 CFR 50.55a(h). To the extent the application addresses the requirements of 10 CFR 50.62 with respect to equipment used to address anticipated transient without SCRAM (ATWS) events, such considerations will be evaluated as part of this DSRS section.

Review Interfaces

1. Other fundamental design principles, such as independence, determinism, and redundancy, inform the review of D3. In addition, the appendices to DSRS Chapter 7 provide additional guidance describing how the reviewer should consider the architectural description, simplicity, and hazard analysis techniques, and how they inform the staff's review of the system's D3.

2. DSRS Chapter 18 defines a methodology, applicable to new reactors, for evaluating manual operator actions as a diverse means of coping with AOOs and postulated accidents (PAs) that are concurrent with a software CCF of the digital I&C protection system. Appendix 18-A of DSRS Chapter 18 offers additional guidance.

3. The review of D3 should be coordinated with the organization responsible for the review of Chapter 15 of the application. The reviewer should confirm with the organization responsible for the review of reactor systems that the analytical basis detailed in the D3 assessment is acceptable and consistent with the Chapter 15 analysis, and that the design of the mechanical systems used for ATWS mitigation is acceptable.

II. ACCEPTANCE CRITERIA

Requirements

1. 10 CFR 50.55a(h) requires compliance with IEEE Std. 603-1991, including the correction sheet, dated January 30, 1995, which is referenced in paragraphs 10 CFR 50.55a(h)(2) and (3). This standard includes Section 5.1, "Single Failure Criteria." This section states, in part, that the safety system must perform all safety functions required for a DBE in the presence of (1) any single detectable failure within the safety systems concurrent with all identifiable but non-detectable failures, (2) all failures caused by the single failure, and (3) all failures and spurious system actions that cause or are caused by the DBE requiring the safety functions.

2. GDC 13, "Instrumentation and Control," requires, in part, that instrumentation be provided to monitor variables and systems over their anticipated ranges for normal

operations, for AOOs, and for accident conditions as appropriate to assure adequate safety.

3. GDC 22, “Protective System Independence,” requires in part that design techniques, such as functional diversity or diversity in component design and principles of operation, shall be used to the extent practical to prevent loss of the protection function.

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.

5. 10 CFR 50.62 requires, in part, automatic initiation of ATWS mitigation systems and equipment that is diverse and independent from the reactor trip system.

6. 10 CFR 50.34(f)(2)(xiv), “Containment Isolation Systems,” requires, in part, that all non-essential systems are isolated automatically by the containment isolation system.

DSRS Acceptance Criteria

The specific DSRS acceptance criteria for D3 are as follows:

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

2. Staff’s Requirement Memorandum (SRM) to SECY-93-087 describes the NRC position on defense-in-depth in Item 18.II.Q.

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

4. The system should conform to the guidance in the version of RG 1.53, in place 6 months before the docket date of the application. Currently, RG 1.53 endorses IEEE Std. 379-2000, “Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems,” with identified exceptions and clarifications. The applicant should examine the version of RG 1.53 that applies to its application to identify the applicable standards. Clause 5.5 of IEEE Std. 379 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.

5. 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. The applicant should examine the version of RG 1.62 that applies to its application to identify the applicable standards.

6. IEEE Std. 7-4.3.2 provides guidance on performing an engineering evaluation of software CCF for digital-based systems, 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.

III. REVIEW PROCEDURES

The reviewer will confirm that the application has addressed vulnerabilities to CCF in accordance with the NRC position on D3 originating from the 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."

D3 can assure that a safety task will be accomplished when necessary to mitigate plant AOOs and PAs, while also providing a defense against CCFs. Defense-in-depth is the principle of providing multiple barriers to any credible failure 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.

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. 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.

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 SRM, dated July 21, 1993, to SECY-93-087, and particularly Item 18.II.Q, forms the foundation of this position.

In the review of D3 assessments, the reviewer will focus on the following four points:

1. D3 Assessment

   The reviewer will confirm that a D3 assessment has been completed for the proposed I&C system and that the assessment demonstrates that vulnerabilities to common cause failures have been adequately addressed. The focus of the D3 assessment should be on the protection systems; however, other systems may be included in the D3 assessment to the extent that they are credited as providing diverse functions to protect against CCF in the protection systems.

2. Analysis of DBEs as Part of D3

The application should contain information sufficient to demonstrate that the D3 assessment analyzes each postulated common-mode failure for each event that is evaluated in the accident analysis section of the application using best-estimate methods. The application should include the following information:

A. vulnerabilities to CCF in the I&C system

B. plant response (calculated using realistic assumptions) demonstrating that any radiation release for each postulated CCF of the events evaluated in Chapter 15 does not exceed 10 percent of the applicable siting dose guideline values in 10 CFR 52.47(a)(2)(iv) or violate the integrity of the primary coolant pressure boundary (the application should (1) demonstrate that sufficient diversity exists to achieve these goals, or (2) identify the vulnerabilities discovered and the corrective actions taken)

C. an evaluation of all elements or signal sources common to two or more system echelons, including 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

D. a demonstration that adequate diversity is provided within the design for each of these events (adequate diversity applies to consideration of the software-based development tools used to develop software for computer-based processors or software-developed logic for digital logic devices)

E. justification should be provided if vulnerabilities, are not addressed by design modification, refined analyses, or provision of alternate trip, initiation, or mitigation capability)

3. Diverse System Characteristics

If a postulated CCF could disable a safety function, then a diverse means, with a documented basis that the diverse means is unlikely to be subject to the same common-mode failure, should be capable of performing either the same function or a different function that will accomplish the same protection action. The diverse or different function may be performed by a nonsafety system if the system is of sufficient quality to perform the necessary function under the associated event conditions. When a diverse means is needed to be available to replace an automated system used to accomplish a credited safety function as a result of the D3 assessment identifying a potential CCF, the reviewer should confirm that the credited safety function (or a different function that will execute the same desired safety protection) can be accomplished via either an automated system or manual operator actions performed from the main control room. The preferred diverse means is normally an automated system. In this context, the diverse means should be:

A. At the system or division level (depending on the design);

B. Initiated from the control room;

C. Capable of responding with sufficient time available for the operators to determine the need for protective actions even with indicators that may be malfunctioning due to the CCF if credited in the D3 coping analysis;

D. Appropriate for the event;

E. Supported by sufficient instrumentation that indicates:

i. the protective function is needed,
ii. the safety-related automated system did not perform the protective function, and
iii. whether the automated diverse means or manual action is successful in performing the safety function.

The diverse means could be safety-related and part of a safety division, and would then be subject to meet divisional independence and automatic and/or manual control requirements as defined in IEEE Std. 603-1991. The independence requirements of a diverse protection system for a safety protection system (i.e., physical, electrical, and communication separation) are defined in IEEE Std. 603-1991. The diverse means could also be nonsafety-related in which case the IEEE Std. 603-1991 requirements to separate safety-related equipment from not safety-related equipment would still apply and would require independence of the two systems. In either case, the diverse means should be independent of the safety system such that a CCF of the safety system would not affect the diverse system. See Figure 1.

Use of Automation as a Diverse Means

If automation is used in the diverse means, the reviewer should confirm that the functions are provided by equipment that is not affected by the postulated CCF and are sufficient to maintain plant conditions within recommended acceptance criteria for the particular AOO or PA. The automated diverse means may be a nonsafety-related system, provided that the system is of sufficient quality to perform the necessary function(s) under the associated event conditions. The reviewer should confirm that the automated diverse means is similar in quality to systems required by the ATWS rule (10 CFR 50.62), as described in the enclosure to GL 85-06.

Use of Manual Action as a Diverse Means

The method for actuating the protective safety functions could be via manual operator actions that meet human factors engineering (HFE) acceptability criteria. If manual operator actions are used as the diverse means or as part of the diverse means to accomplish a safety function, the reviewer should confirm that a suitable HFE analysis was performed by the applicant to demonstrate that plant conditions can be maintained within recommended acceptance criteria for the particular AOO or PA. The acceptability of such actions is to be reviewed by the NRC staff in accordance with DSRS Chapter 18, which provides review criteria for crediting manual operator actions in D3 Analyses.

The following should be considered when reviewing manual actions:

A. If the D3 assessment indicates that a safety-related manual initiation could 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 that are diverse from one another would be needed).

B. If the safety-related system or division level manual initiation required by IEEE Std. 603-1991 is sufficiently diverse, the diverse (second) manual means would not be necessary (see Figure 1).

C. If credit is taken for a manual actuation method that meets both the IEEE Std. 603-1991, Sections 6.2 and 7.2 requirements and a need for a diverse manual means, then the applicant should demonstrate that such criteria are satisfied and that sufficient diversity exists.

D. The difference between Time Available and Time Required for operator action is a measure of the safety margin. As this difference decreases, uncertainty in the estimate of the difference between these times should be appropriately considered on a case-by-case basis. This uncertainty could reduce the level of assurance in, and potentially invalidate a conclusion that operators can perform the action reliably within the time available. For complex situations and for actions with limited margin, such as less than 30 minutes between time available and time required, a more focused staff review will be performed.

E. If the diverse means is nonsafety-related, the reviewer should confirm that the manual diverse means is similar in quality to systems required by the ATWS rule (10 CFR 50.62), as described in the enclosure to GL 85-06. In addition, the reviewer should confirm that IEEE Std. 603-1991, Section 5.6, "Independence," is considered for the independence of the safety systems and the diverse means.

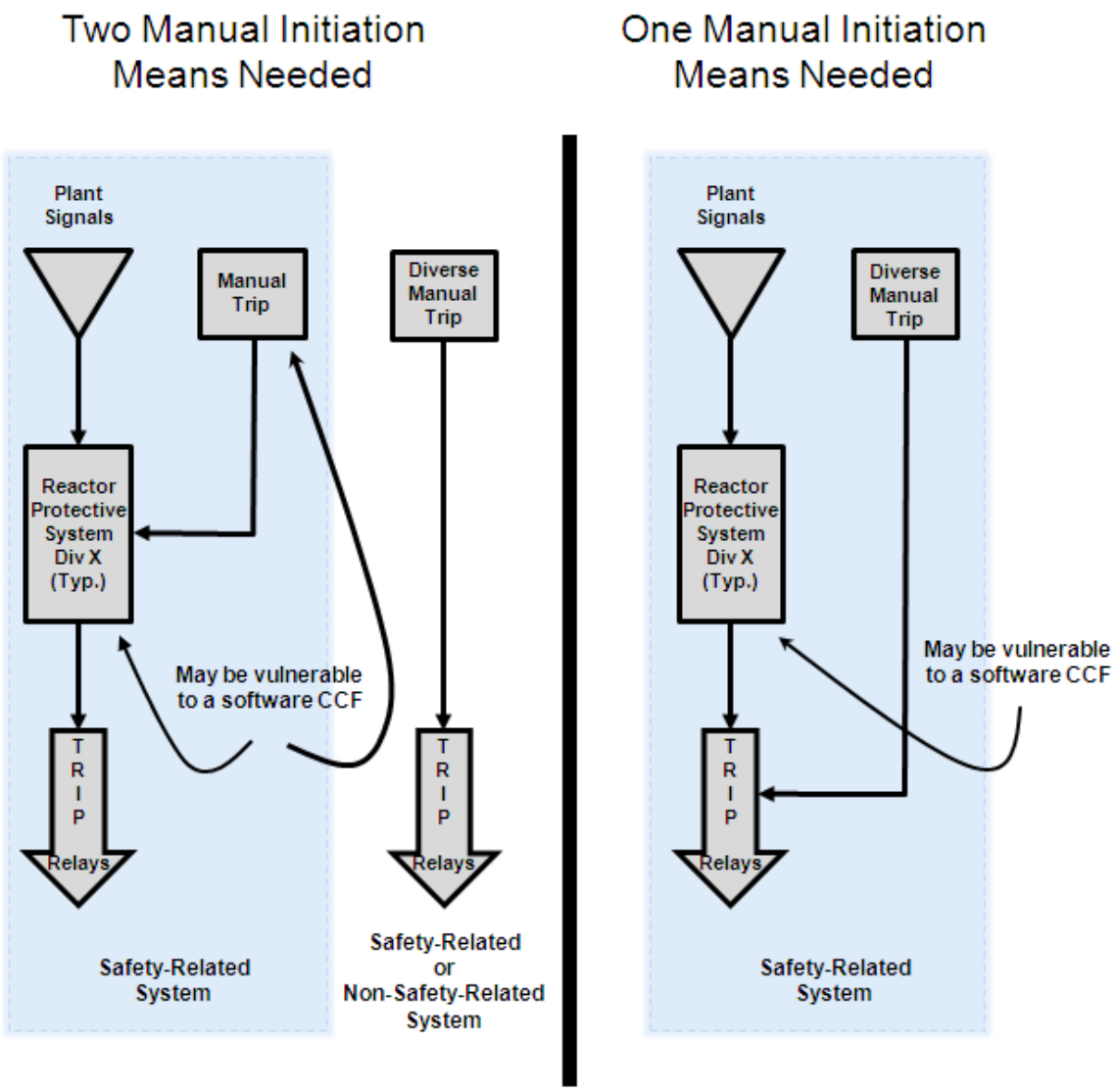

Figure 1. Two Manual Initiation methods versus One Initiation Method

4. Displays and Controls

A set of displays and controls located in the main control room should be provided for manual, system-level actuation of critical safety functions and monitoring of parameters that support the safety functions. The displays and controls should be independent and diverse from the safety computer system identified in Items 1 and 3 above.

Failure of monitoring or display systems should not influence the functioning of the reactor trip system (RTS) or ESF. If a plant monitoring system failure can induce 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.

5. Additional Considerations for D3 Review

A. Prioritization between safety-related and diverse nonsafety-related 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. A command initiating a safety function should have the highest priority and should override lower priority commands. For example, a reactor trip would be considered the safe state and should not be overridden even if generated by a spurious actuation caused by a CCF of the automated protection system. However, in the case of the spurious actuation of ESF actuation system (AS) equipment, the design should afford the reactor operator the ability to manually control components in the priority scheme. Many options are available for how the system accomplishes these actions (i.e., through hardwiring or direct network control or through a priority module, etc.).

   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, should have lower priority and may be overridden by higher priority commands. An example is a postulated CCF that causes the ESFAS to erroneously turn off components credited to perform a safety function. The reviewer should note whether the priority scheme would allow the reactor operator to place such components in the safe state necessary to support the safety function and how the system accomplishes the operator action.

   iv. The analysis of the proposed priority ranking should explain conflicts due to timing and sequencing of signals. 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.

B. While the D3 assessment should consider failure of the protection system to actuate a safety function when plant conditions warrant 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 should address 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 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 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 the adequacy of such strategies.

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

iv. The design of a diverse automated or diverse manual actuation system should address how to minimize the potential for a spurious actuation of the protective system caused by the diverse means.

C. In reviewing the D3 assessment using the above acceptance criteria, the reviewer should evaluate whether the analysis of the D3 design features conforms to the guidance of NUREG/CR-6303. In general, several types of diversity should exist, some of which should exhibit the attributes listed in NUREG/CR-6303. The reviewer should be aware of the following when reviewing the D3 assessment:

i. The justification for equipment diversity, or for the diversity of related system logic such as a real-time operating system, should extend to the equipment's components to assure that actual diversity exists. For example, different manufacturers might use the same processor or license the same operating system, thereby incorporating the potential for common failure causes in otherwise different equipment. Claims for diversity on the basis of the difference in manufacturer name are insufficient without consideration of the above.

ii. With respect to computer software and software-based logic diversity, experience indicates that independence may not be achieved in cases in which, for example, multiple versions of software are developed using the same set of software, system, and logic development tools. Other considerations, such as technology, functional and signal diversity that lead to different software, system, and logic requirements form a stronger basis for diversity.

In addition, the evaluation of failure modes as a result of CCF should include the possibility of partial actuation and failure to actuate with false indications, as well as a total failure to actuate, in accordance with NUREG/CR-6303.

D. Many system design and testing attributes, procedures, and practices can contribute to significantly reducing the probability of CCF. However, there are two design attributes, either of which is sufficient to eliminate consideration of software based or software logic based CCF:

i. Diversity – If sufficient diversity exists in the protection system, then the potential for CCF within the channels can be considered to be appropriately addressed without further action.

ii. Testability – If a system is sufficiently simple such that every possible combination of inputs and every possible sequence of device states are tested and all outputs are verified for every case (100% tested), then CCF within the system can be considered to be appropriately addressed without further action. If a portion or component of a system can be fully tested, then it can be considered not to have a potential for software-based CCF. Fully tested or 100% testing means that every possible combination of inputs and every possible sequence of device states are tested, and all outputs are verified for every case. Further, in assessing the system states, the guidance provided in IEEE Std. 7-4.3.2, Clause 5.4.1, "Computer system [equipment qualification] testing," should be addressed. This approach is applicable to microprocessor-based technology as well as other forms of complex logic such as programmable logic devices (e.g. Field Programmable Gate Arrays (FPGAs)).

6. Conformance with 10 CFR 50.62

As defined in 10 CFR 50.62, an ATWS event is an AOO followed by failure of the reactor trip portion of the protection system. Diverse actuation system (DAS) and ATWS mitigation functions may be combined into a single system, or the ATWS mitigation functions may be performed by a completely separate system. For ATWS mitigation systems in pressurized water reactors, 10 CFR 50.62 requires diversity from the sensor output to the final actuation device. The ATWS mitigation systems should include the capability for initiation from the control room and should be testable at power (up to, but not necessarily including, the final actuation device). The ATWS mitigation logic and DAS should be designed such that, once initiated, the mitigation function will go to completion. Logic and actuation device power for the ATWS mitigation system should be from an instrument power supply independent from the power supplies for the existing RTS.

The reviewer should verify that the DAS functions are independent and diverse from the RTS and ESFAS, and that the ATWS mitigation systems are diverse from the RTS. However, interconnections between the RTS and ESFAS (for interlocks providing for reactor trip if certain ESFs are initiated, ESF initiation when a reactor trip occurs, or operating bypass functions) are permitted. RTS and ESFAS may be combined into a single controller or central processing unit. However, the preferred method is to perform the RTS and ESFAS functions in distinct and separate modules, systems, or platforms. Whether distinct or combined, the following criteria are addressed:

A. D3 is adequately addressed to protect against CCF.

B. The interconnections between the RTS and ESFAS (for interlocks providing for reactor trip if certain ESFs are initiated, ESF initiation when a reactor trip occurs, or operating bypass functions) can be demonstrated not to impair the functions required by the ATWS rule (10 CFR 50.62).

C. The fundamental principle of simplicity has been adequately addressed.

7. Conformance with 10 CFR 50.34(f)(2)(xiv)

Signal diversity should be provided for the containment isolation function. The containment isolation functions of the ESFAS should be reviewed to confirm that the ESFAS automatically closes each isolation device on each nonessential penetration. For plants with digital-computer-based ESFAS, signal diversity should be confirmed in the review of the applicant's D3 analysis.

IV. EVALUATION FINDINGS

If the reviewer confirms that the application conforms to the guidance identified above, the staff can conclude that the application provides information sufficient to demonstrate that the proposed I&C systems are designed with sufficient diversity to cope with a DBE concurrent with a CCF that disables the safety function. On such a basis, the reviewer can conclude that the design of I&C systems satisfies the guidelines in the SRM to SECY-93-087 and NUREG/CR-6303 with regard to D3, and the D3 requirements contained in GDCs 13, 22, 24, 10 CFR 50.62, 10 CFR 50.34(f)(2)(xiv), and Section 5.1 of IEEE Std. 603-1991.

V. IMPLEMENTATION

This section is identical throughout this mPower^{TM} DSRS Section 7.1. The reviewer must read Section 7.1.1 Safety System Design Basis subsection “V. Implementation”.

VI. REFERENCES

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