U.S. NUCLEAR REGULATORY COMMISSION

DRAFT REGULATORY GUIDE DG-1374

Proposed Revision 4 to Regulatory Guide 1.152

Issue Date: February 2023
Technical Lead: Khoi Nguyen

CRITERIA FOR PROGRAMMABLE DIGITAL DEVICES IN SAFETY-RELATED SYSTEMS OF NUCLEAR POWER PLANTS

A. INTRODUCTION

Purpose

This regulatory guide (RG) describes an approach that is acceptable to the staff of the U.S. Nuclear Regulatory Commission (NRC) to meet regulatory requirements for promoting high functional reliability, design quality, and a secure development and operational environment (SDOE) for the use of programmable digital devices (PDDs) in the safety-related systems of nuclear power generating stations. This RG endorses, with some exceptions and clarifications, Institute of Electrical and Electronics Engineers (IEEE) Standard (Std) 7-4.3.2-2016, "IEEE Standard Criteria for Programmable Digital Devices in Safety Systems of Nuclear Power Generating Stations" (Ref. 1).

Applicability

This RG applies to nuclear power reactor applicants and licensees subject to Title 10 of the *Code of Federal Regulations* (10 CFR), Part 50, "Domestic Licensing of Production and Utilization Facilities" (Ref. 2), and 10 CFR Part 52, "Licenses, Certifications, and Approvals for Nuclear Power Plants" (Ref. 3).

Applicable Regulations

- 10 CFR Part 50 provides regulations for licensing production and utilization facilities.
    - o 10 CFR 50.55a(h) states that protection systems of nuclear power reactors of all types must meet the requirements specified in 10 CFR 50.55a(h), and each combined license for a utilization facility is subject to the conditions in 10 CFR 50.55a(h). 10 CFR 50.55a(h)(2) mandates compliance with the requirements stated in IEEE Std 279-1968, "Proposed IEEE Criteria for Nuclear Power Plant Protection Systems" (Ref. 4), IEEE Std 279-1971, "Criteria for Protection Systems for Nuclear Power Generating Stations" (Ref. 5), or IEEE Std 603-1991, "IEEE Criteria for Safety Systems for Nuclear Power Generating Stations," and the correction sheet dated January 30, 1995 (Ref. 6), for nuclear power plants with construction permits (CPs) issued between January 1, 1971, and May 13, 1999. For nuclear power plants with CPs issued before January 1, 1971, 10 CFR 50.55a(h)(2) requires compliance with their

This RG is being issued in draft form to involve the public in the development of regulatory guidance in this area. It has not received final staff review or approval and does not represent an NRC final staff position. Public comments are being solicited on this DG and its associated regulatory analysis. Comments should be accompanied by appropriate supporting data. Comments may be submitted through the Federal rulemaking Web site, http://www.regulations.gov, by searching for draft regulatory guide DG-1374. Alternatively, comments may be submitted to the Office of Administration, Mailstop: TWFN 7A-06M, U.S. Nuclear Regulatory Commission, Washington, DC 20555-0001, ATTN: Program Management, Announcements and Editing Staff. Comments must be submitted by the date indicated in the *Federal Register* notice.

Electronic copies of this DG, previous versions of DGs, and other recently issued guides are available through the NRC's public Web site under the Regulatory Guides document collection of the NRC Library at https://nrcweb.nrc.gov/reading-rm/doc-collections/reg-guides/. The DG is also available through the NRC's Agencywide Documents Access and Management System (ADAMS) at http://www.nrc.gov/reading-rm/adams.html, under Accession No. ML22124A313. The regulatory analysis may be found in ADAMS under Accession No. ML22132A293.

plant-specific licensing basis or IEEE Std 603-1991 and the correction sheet dated January 30, 1995. For applicants for CPs, operating licenses, combined licenses, standard design approvals, design certifications, or manufacturing licenses filed after May 13, 1999, 10 CFR 50.55a(h)(3) requires compliance with IEEE Std 603-1991 and the correction sheet dated January 30, 1995. Although 10 CFR 50.55a(h)(2) and (h)(3) and IEEE Std 603-1991 (incorporated by reference) use the term "safety system," consistent with the NRC's definition of safety-related systems in 10 CFR 50.2, "Definitions," this RG uses the term "safety-related system" in lieu of the term "safety system."

  - 10 CFR Part 50, Appendix A, "General Design Criteria for Nuclear Power Plants," General Design Criterion (GDC) 13, "Instrumentation and control," requires, in part, that operating reactor licensees provide instrumentation to monitor variables and systems over their anticipated ranges for normal operation, anticipated operational occurrences, and accident conditions as appropriate to ensure adequate safety.

  - 10 CFR Part 50, Appendix A, GDC 21, "Protection system reliability and testability," requires, in part, that protection systems be designed for high functional reliability and inservice testability commensurate with the safety functions to be performed. It also requires that protection systems 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.

  - 10 CFR Part 50, Appendix B, "Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants," Criterion III, "Design Control," requires, in part, that licensees specify quality standards and provide design control measures for verifying or checking the adequacy of safety system designs.

- 10 CFR Part 52 governs the issuance of early site permits, standard design certifications, combined licenses, standard design approvals, and manufacturing licenses for nuclear power facilities. Part 52 specifies, among other things, that the contents of some applications must satisfy the requirements of 10 CFR Part 50, Appendix A and Appendix B thereto, and other specified regulations. .

Related Guidance

- Item 18 of the staff requirements memorandum to SECY-93-087, "SECY-93-087—Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Design," dated July 21, 1993 (Ref. 7), provides the Commission's policy for addressing common-cause failures (CCFs) in digital instrumentation and controls (DI&C) systems.

- NUREG-0800, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition," Chapter 7, "Instrumentation and Controls," Branch Technical Position (BTP) 7-19, Revision 8, "Guidance for Evaluation of Defense in Depth and Diversity to Address Common-Cause Failure due to Latent Design Defects in Digital Safety Systems," issued January 2021 (Ref. 8), provides guidance for evaluating an applicant's assessment of the adequacy of defense in depth for a proposed DI&C system. The assessment includes identifying and assessing vulnerabilities to potential CCFs in a proposed DI&C system and evaluating the effects on plant safety of any CCFs that are not prevented or mitigated.

- RG 5.71, “Cyber Security Programs for Nuclear Facilities” (Ref. 9), provides an acceptable approach for complying with the Commission’s regulations on the protection of digital computers, communications systems, and networks from a malicious cyberattack as defined by 10 CFR 73.1, “Purpose and Scope” (Ref. 10).

Purpose of Regulatory Guides

The NRC issues RGs to describe methods that are acceptable to the staff for implementing specific parts of the agency’s regulations, to explain techniques that the staff uses in evaluating specific issues or postulated events, and to describe information that the staff needs in its review of applications for permits and licenses. Regulatory guides are not NRC regulations and compliance with them is not required. Methods and solutions that differ from those set forth in RGs are acceptable if supported by an adequate basis for the issuance or continuance of a permit or license by the Commission.

Paperwork Reduction Act

This RG provides voluntary guidance for implementing the mandatory information collections in 10 CFR Parts 50 and 52 that are subject to the Paperwork Reduction Act of 1995 (44 U.S.C. 3501 et. seq.). These information collections were approved by the Office of Management and Budget (OMB), under control numbers 3150-0011 and 3150-0151. Send comments regarding this information collection to the FOIA, Library, and Information Collections Branch (T6-A10M), U.S. Nuclear Regulatory Commission, Washington, DC 20555-0001, or by e-mail to Infocollects.Resource@nrc.gov, and to the Desk Officer, Office of Information and Regulatory Affairs, NEOB-10202 (3150-0011 and 3150-0151), Office of Management and Budget, Washington, DC, 20503.

Public Protection Notification

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

B. DISCUSSION

Reason for Revision

This revision (Revision 4) of the guide endorses IEEE Std 7-4.3.2-2016 with exceptions and clarifications. Specifically, this revision removes the previous SDOE guidance from this guide and instead endorses, with clarifications, the SDOE criteria within IEEE Std 7-4.3.2-2016. This revision also includes additional guidance for fault detection and self-diagnostics, if used, in DI&C systems. In addition, this revision endorses Annex D of IEEE Std 7-4.3.2-2016 and clarifies the applicability of the control of access guidance for safety-related PDDs.

Background

The regulation in 10 CFR 50.55a(h)(2) requires that protection systems for nuclear power plants meet the requirements of IEEE Std 279-1968, IEEE Std 279-1971, or IEEE Std 603-1991 and the correction sheet dated January 30, 1995, depending on the licensing basis of the nuclear power plants. The American Nuclear Society Standards Committee and the Nuclear Power Engineering Committee of the IEEE Power Engineering Society developed IEEE Std 7-4.3.2 in 1982 to supplement IEEE Std 603 with criteria for programmable digital computer systems. Since then, IEEE Std 7-4.3.2 has been updated periodically to encompass the evolved digital technologies. With respect to the use of PDDs in safety-related systems, revision 2016 of IEEE 7-4.3.2 states “This standard specifies additional digital system requirements to supplement the criteria and requirements of IEEE Std 603™-2009…” (Ref. 11). The NRC staff has reviewed Revision 2016 of IEEE 7-4.3.2 and finds that it provides acceptable supplemental guidance on how to meet the criteria of IEEE Std 603-1991 incorporated by reference in 10 CFR 50.55a(h). The staff’s endorsement of Revision 2016 of IEEE 7-4.3.2, with exceptions and clarifications, is discussed in Section C of this RG.

The instrumentation and controls (I&C) design should ensure that the safety-related equipment or components can be qualified, procured, installed, commissioned, operated, and maintained to be capable of withstanding, with sufficient reliability and robustness, all conditions specified in the plant design basis or licensing basis. To achieve adequate defense in depth, the I&C architecture and systems design should meet certain fundamental I&C design principles to support the assessment of defense-in-depth adequacy for the overall plant. Fundamental I&C design principles consist of independence, redundancy, diversity and defense in depth, and deterministic behavior (predictability and repeatability). Incorporating these principles in the design facilitates addressing specific hazards within the design (e.g., fault propagation). While diversity is part of the fundamental I&C design principles, it is only considered one means to address CCF. Therefore, the review of diversity focuses more broadly on supporting the defense-in-depth assessment and other measures to address CCF.[1]

Working Group Subcommittee 6.4, “Application of Programmable Digital Devices to Safety Systems of Nuclear Power Generating Stations,” of the IEEE Nuclear Power Engineering Committee prepared IEEE Std 7-4.3.2-2016. This updated standard reflects advances in digital technology and represents a continued effort by IEEE to support the specification, design, and implementation of PDDs in safety-related systems of nuclear power plants. As defined in this standard, the term “programmable digital devices” refers to devices that rely on software instructions or programmable logic to accomplish a function. Examples include a computer, a programmable hardware device, or a device with firmware.

[1] See the NRC Design Review Guide, “Instrumentation and Controls for Non-Light-Water Reactor (NON-LWR) Reviews,” dated October 8, 2020 (Ref. 12), for more information.

The I&C systems that use PDDs adopt advanced technology in both digital devices and the tools for design and development of these devices. These systems are expected to be significantly and functionally different from nondigital systems and may include the use of data communications, self-diagnostics, and integrated functions in a single system or module. Increasing use of PDDs provides potential enhancements to system reliability and performance but may present different hazards than those of safety-related systems that use analog technology. Therefore, the design and development of PDDs in safety-related systems should consider these different hazards. IEEE Std 7-4.3.2-2016 provides criteria for reasonable assurance that the hazards associated with PDDs in safety-related systems are adequately identified and controlled. This standard also provides criteria for the technical and quality characteristics that apply to these PDDs.

Revision 2016 of IEEE Std 7-4.3.2 includes the following eight informative annexes:

1. Annex A, “Mapping of IEEE Std 603-2009 to IEEE Std 7-4.3.2,” maps IEEE Std 7-4.3.2-2016 to the criteria within IEEE Std 603-2009. This annex also identifies which clauses within IEEE Std 7-4.3.2-2016 contain additional requirements beyond those in IEEE Std 603-2009. This annex does not contain any guidance or requirements.

2. Annex B, “Diversity Requirements Determination,” has not received NRC endorsement. BTP 7-19 provides staff guidance for the evaluation of defense in depth and diversity to address CCF due to latent design defects in digital safety systems.

3. Annex C, “Dedication of Existing Commercial Computers,” provides useful reference information (i.e., references to certain commercial-grade-dedication related documents) but does not provide specific guidance, and therefore has not received NRC endorsement. This RG endorses Clause 5.17 of IEEE Std 7-4.3.2-2016, which provides guidance for the evaluation and implementation of commercial digital equipment. Further guidance for commercial-grade dedication appears in RG 1.164, “Dedication of Commercial-Grade Items for Use in Nuclear Power Plants” (Ref. 13), which endorses Electric Power Research Institute (EPRI) 3002002982, “Plant Engineering: Guideline for the Acceptance of Commercial-Grade Design and Analysis Computer Programs Used in Nuclear Safety-Related Applications,” issued September 2014 (Ref. 14). In addition, guidance for verifying a DI&C item’s dependability critical characteristics based on an accredited certification during the dedicating process appears in RG 1.250, “Dedication of Commercial-Grade Digital I&C Items for Use in Nuclear Power Plants” (Ref. 15), which endorses Nuclear Energy Institute (NEI) 17-06, “Guidance on Using IEC 61508 SIL Certification to Support the Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Related Applications,” issued December 2021 (Ref. 16). Further, EPRI Topical Report (TR)-106439, “Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications,” issued October 1996 (Ref. 17), contains guidance specific to commercial-grade dedication processes for digital equipment that the staff has found to be acceptable, with clarifications, as documented in the NRC safety evaluation report, “Safety Evaluation by the Office of Nuclear Reactor Regulation Electric Power Research Institute Topical Report, TR 106439, Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications,” dated July 17, 1997 (Ref. 18).

4. Annex D, “Identification and Control of Hazards,” provides guidance for identifying and controlling hazards. Section C of this RG discusses the NRC’s endorsement of Annex D.

5. Annex E, “Communication Independence,” has not received NRC endorsement. This RG endorses, with clarifications, the communication independence criteria within the normative parts of the standard, as discussed in Section C of this RG.

6. Annex F, “Computer Reliability,” has been deleted.

7. Annex G, “Glossary,” defines certain terms used in the standard. This annex does not contain any guidance or requirements.

8. Annex H, “Bibliography,” contains the references used in the standard. This annex does not contain any guidance or requirements.

Consideration of International Standards

The International Atomic Energy Agency (IAEA) works with member states and other partners to promote the safe, secure, and peaceful use of nuclear technologies. The IAEA develops Safety Requirements and Safety Guides for protecting people and the environment from the harmful effects of ionizing radiation. This system of safety fundamentals, safety requirements, safety guides, and other relevant reports, reflects an international perspective on what constitutes a high level of safety. To inform its development of this RG, the NRC considered IAEA Safety Requirements and Safety Guides pursuant to the Commission’s International Policy Statement (Ref. 19) and Management Directive and Handbook 6.6, “Regulatory Guides” (Ref. 20). No relevant international standards related to promoting high functional reliability, design quality, and a SDOE for the use of PDDs in the safety-related systems of nuclear power generating stations were identified.

Documents Discussed in Staff Regulatory Guidance

This RG endorses, in part, the use of one or more codes or standards developed by external organizations, and other third-party guidance documents. These codes, standards and third-party guidance documents may contain references to other codes, standards or third-party guidance documents (“secondary references”). If a secondary reference has itself been incorporated by reference into NRC regulations as a requirement, then licensees and applicants must comply with that standard as set forth in the regulation. If the secondary reference has been endorsed in a RG as an acceptable approach for meeting an NRC requirement, then the standard constitutes a method acceptable to the NRC staff for meeting that regulatory requirement as described in the specific RG. If the secondary reference has neither been incorporated by reference into NRC regulations nor endorsed in a RG, then the secondary reference is neither a legally-binding requirement nor a “generic” NRC approved acceptable approach for meeting an NRC requirement. However, licensees and applicants may consider and use the information in the secondary reference, if appropriately justified, consistent with current regulatory practice, and consistent with applicable NRC requirements.

C. STAFF REGULATORY GUIDANCE

1. This RG endorses, in part, the methods described in IEEE Std 7-4.3.2-2016 as adequate bases for complying with the requirements of regulations with respect to high functional reliability and design requirements for PDDs used in the safety-related systems of nuclear power plants. The staff takes some exceptions to the guidance in IEEE Std 7-4.3.2-2016 and provides clarifications and points of emphasis as identified below.

a. Exceptions

(1) Revision 2016 of IEEE Std 7-4.3.2 presents an approach that the staff considers acceptable in meeting the requirements of NRC regulations with respect to high functional reliability and design requirements for PDDs used in the safety-related systems of nuclear power plants, subject to the following specific exceptions.

1.1 As discussed in Section B of this RG, the NRC staff has not endorsed Annexes B, C, and E. However, the staff believes that these annexes contain useful information.

1.2 Revision 2016 of IEEE Std 7-4.3.2 includes examples to supplement the guidance. However, the NRC's endorsement of IEEE Std 7-4.3.2-2016 does not constitute a determination that the examples are applicable for all licensees and applicants. A licensee or applicant should ensure that a given example is applicable to its plant-specific circumstances before implementing the guidance as described in that example.

b. Clarifications

(1) System Integrity

1.1 Safety-related instrumentation and control systems should be designed to operate in a predictable and repeatable manner. The term "predictable"[1] generally refers to the ability to determine the output of a system at any time through known relationships among the controlled system states and required responses to those states, such that a given set of input signals will always produce the same output signals. The term "repeatable"[1] generally refers to the output of a system being consistently achieved given the same input and system properties, including internal and external conditions. PDDs used in safety-related systems should have adequate system integrity such that the safety-related system can operate in a predictable and repeatable manner. Clause 5.5 of IEEE Std 7-4.3.2-2016 provides criteria for achieving system integrity in PDDs for use in safety-related systems. Clause 5.5.1 of IEEE Std 7-4.3.2-2016 refers to Annex D for guidance related to identifying and addressing potential hazards of the system. The NRC staff finds that Annex D of IEEE Std 7-4.3.2-2016 is an acceptable method to identify and control hazards of DI&C devices used in safety-related systems subject to the following clarifications:

1.1.1 The scope of Annex D is limited to DI&C devices.

1.1.2 Annex D provides fault tree analysis and failure modes and effects analysis as the examples of hazards analysis techniques. However, the NRC staff's endorsement of Annex D does not constitute an endorsement of these techniques, and these techniques are not the only techniques for hazards analysis.

1.1.3 Annex D discusses Annex C in the background section. However, as discussed in Section C1a(1)1.1 of this guide, the NRC staff has not endorsed Annex C of IEEE Std 7-4.3.2-2016 because it simply provides useful reference information, rather than specific guidance.

1.2 Clause 5.5.3 of IEEE Std 7-4.3.2-2016 provides criteria that the NRC staff finds acceptable for the use of self-diagnostics for the timely detection of failures. In addition, the criteria for fault detection and self-diagnostics in Clause 5.5.3 should be supplemented with the following:

1.2.1 Typical self-diagnostic methods may include, but are not limited to, monitoring memory and memory reference integrity, using watchdog timer (WDT) or processors, monitoring communication channels, monitoring central processing unit statuses, and checking data integrity. A WDT used to detect lock-up conditions should be independent of the microprocessor it is monitoring such that the WDT is not subject to the same failure condition as the microprocessor. Upon detection of a lock-up condition or other failure, the WDT should place the output of the system into a predetermined fail-safe state based on the safety-related system application. This WDT function should be completed independently of the microprocessor it is monitoring. One approach the NRC staff finds acceptable for implementing a WDT is to use a hardware-based device to perform the WDT counter, reset, time-out, and fail-safe functions.

1.2.2 If self-diagnostic features are integrated into the safety-related DI&C systems, the following criteria should be applied:

(a) The design of self-diagnostic features maintains channel independence and system integrity and meets the single-failure criterion.

(b) The safety classification of the hardware and software used to perform self-diagnostics is equivalent to that of the tested system unless physical, electrical, and communication independence are maintained such that no failure of the test function can inhibit the performance of the safety function.

(c) Failures detected by self-diagnostics are consistent with the failure detectability assumptions of the single-failure analysis and the failure modes and effects analysis.

(d) Self-diagnostic features do not add complexity to the safety-related system. Interfaces between software that performs protection functions and software for other functions such as self-diagnostics should be designed to minimize the complexity of the software logic and data structures.

(e) Self-diagnostic functions are verified during periodic functional tests.

1.2.3 Self-diagnostics could be credited, on an application-specific basis, to either reduce or eliminate the channel operability tests, provided criteria 1.2.2(a), 1.2.2(b), 1.2.2(c), 1.2.2(d), and 1.2.2(e) and the following are met:

(a) Self-diagnostic features do not adversely impact the reliability of the DI&C safety-related system and its ability to perform safety functions.

(b) Self-diagnostics achieve the same acceptance criteria applied to the manual periodic channel operability test.

(c) Provisions are in place to confirm the execution of the self-diagnostics during plant operation. The capability to periodically test and calibrate the automatic test equipment should also be provided.

(d) Administrative control and operation procedures are maintained to periodically verify the performance of self-diagnostics (e.g., periodic checks of event logs, manual verification of setpoints, rebooting of startup self-diagnostics).

1.3 Clause 5.5.4 of IEEE Std 7-4.3.2-2016 provides guidance on the use of priority functions. This clause addresses how command signals received from safety-related I&C PDDs and PDDs that are non-safety-related (NSR) for actuating a safety-related component should be prioritized. This clause does not specify whether the priority function is implemented within the PDD performing the safety-related function or in a separate PDD. If the priority function is used, the licensee or applicant should analyze the implementation to identify the potential introduction of additional hazards due to the increase in interconnectivity between safety-related PDDs and NSR PDDs.

(2) Independence

2.1 A propagational failure is one hazard that safety-related systems that use digital communication may be more susceptible to due to the increased potential for errors to be introduced during communications processing and transmission. Sufficient independence should be incorporated into the instrumentation and control design to prevent (1) the propagation of faults from systems that are NSR to safety-related systems or (2) the propagation of faults between redundant portions of a safety-related system and (3) the effects of design-basis events on the safety-related system. Furthermore, sufficient independence should be incorporated to ensure the effectiveness of the redundancy provided in the instrumentation and control design for maximizing the reliability of systems that support safety functions. Clause 5.6 of IEEE Std 7-4.3.2-2016 provides criteria that the NRC staff finds acceptable for maintaining independence between PDDs belonging to redundant safety divisions and between safety-related PDDs and NSR PDDs. In addition, the criteria for communication independence in Clause 5.6.4.2 should be supplemented with the following:

2.1.1 Provisions for interdivisional communication should be included to prevent the ability to send software instructions to a safety function processor that could adversely impact the processor’s functionality unless all safety functions associated with that processor are either bypassed or not in service. The progress of a safety function processor through its instruction sequence should not be affected by any message from outside its division. For example, a received message should not be able to direct the processor to execute a subroutine or branch to a new instruction sequence.

2.1.2 Data communication capacity (i.e., bandwidth) should be sufficient to prevent data congestion.

2.1.3 “Point-to-point” data communication means that the message is passed directly from the sending node to the receiving node without the involvement of equipment outside the division of the sending or receiving node.

2.2 In addition to the independence criteria in Clause 5.6, Clauses 5.8.1 and 5.8.2 provide criteria that apply to multidivisional control and display stations for control of safety-related equipment. The term "control," used in the context of multidivisional control and display workstations, includes all functions that can affect the safety-related equipment, including, but not limited to, bypass, lockout, blocks, and inhibit functions. In addition, the criteria for the interface between information displays and safety-related systems in Clause 5.8.2 should be supplemented with the following:

2.2.1 The control processor and its associated communication processor should only process the commands that pass the error checking.

(3) Control of Access

3.1 Clauses 5.9 and 5.6 of IEEE Std 7-4.3.2-2016 provide criteria that the NRC staff finds acceptable for the protection of safety-related systems from non-malicious acts, such as undesirable behavior of connected systems and unintended access to safety-related systems. Licensees and applicants should provide a vulnerability assessment for the SDOE in accordance with the guidance of Clause 5.9 of IEEE Std 7-4.3.2-2016. Based on the results of the vulnerability assessment, the licensee and applicant should identify measures, design features, or both to address identified vulnerabilities.

3.2 Clause 5.9.3 provides criteria for the interaction between cyber security features (e.g., intrusion detection software, virus protection software, access control software) and safety functions. Licensees and applicants should avoid implementation of cyber security features directly in the safety-related systems. In any case, implementation of cyber security features shall not adversely impact the performance, effectiveness, reliability, or operation of safety functions.

3.3 With regard to providing safeguards to safety-related PDDs before installation, Clause 5.9.4 of IEEE Std 7-4.3.2-2016 should be supplemented with the following additional consideration:

3.3.1 Receipt, storage, staging, and testing of safety-related PDDs before installation should occur in a secure environment.

3.4 This RG is not intended to address the control-of-access features to prevent malicious cyberattacks. For protection for safety-related systems from malicious cyberattacks, the requirements of 10 CFR 73.54, "Protection of digital computer and communication systems and networks," address cybersecurity of digital assets, which include those systems used to perform safety-related functions and functions that are important to safety, security, and emergency preparedness. The NRC published 10 CFR 73.54 to require licensees to establish, implement, and maintain cybersecurity plans and programs to protect critical digital assets, including digital safety systems, from malicious cyberattacks. RG 5.71 provides an acceptable approach to meet the requirements of 10 CFR 73.54. For licensees that choose to provide, as part of their license submittal, descriptions of cybersecurity design features intended to address the guidance of RG 5.71, the extent of the staff's review of these features is limited to ensuring that these features do not adversely affect or degrade the safety-related system's reliability or its capability to perform its safety functions. Licensees and applicants should also consider the cybersecurity guidance in RG 5.71 in preparing a design certification under 10 CFR Part 52. Within such consideration, measures should be included to ensure that safety-related I&C systems do not present an electronic path that could enable unauthorized access to the plant's safety-related system (e.g., the use of a hardware-based unidirectional device is one approach the NRC staff would consider acceptable for implementing such measures).

(4) Common-Cause Failure

4.1 CCFs have been identified as a type of hazard to which PDDs in safety-related digital systems could be more susceptible, due to the integration capabilities provided by the technology and its inherent complexity compared to analog technologies. PDDs in safety-related systems can be vulnerable to a CCF due to defects in the devices' hardware or to latent defects in the software or software-based logic. A CCF of PDDs within a DI&C system can either (1) result in loss of capability to perform a safety function concurrent with an anticipated operational occurrence, a postulated accident, or normal operations, or (2) initiate the operation of a function without a valid demand or cause an erroneous (i.e., spurious) system action. The latter is typically referred to as "spurious operation" or "spurious actuation."

4.2 Clause 5.16 of IEEE Std 7-4.3.2-2016 provides criteria that the NRC staff finds acceptable for addressing potential CCFs in PDDs of safety-related systems. In addition, the NRC staff uses the guidance in BTP 7-19 to evaluate the applicants' defense in depth and diversity assessment as a means to address CCFs due to latent design defects in digital safety-related systems.

(5) Use of Commercial Digital Equipment

5.1 Clause 5.17 of IEEE Std 7-4.3.2-2016 provides criteria that the NRC staff finds acceptable for addressing the use of commercial digital equipment in safety-related systems of nuclear power generations. Clause 5.17 references Annex C for additional information about commercial grade item acceptance and dedication. However, as discussed in Section C1a(1)1.1 of this guide, the NRC staff has not endorsed Annex C of IEEE Std 7-4.3.2-2016.

D. IMPLEMENTATION

The NRC staff may use this regulatory guide as a reference in its regulatory processes, such as licensing, inspection, or enforcement. However, the NRC staff does not intend to use the guidance in this regulatory guide to support NRC staff actions in a manner that would constitute backfitting as that term is defined in 10 CFR 50.109, “Backfitting,” and as described in NRC Management Directive 8.4, “Management of Backfitting, Forward Fitting, Issue Finality, and Information Requests,” (Ref. 21), nor does the NRC staff intend to use the guidance to affect the issue finality of an approval under 10 CFR Part 52, “Licenses, Certifications, and Approvals for Nuclear Power Plants.” The staff also does not intend to use the guidance to support NRC staff actions in a manner that constitutes forward fitting as that term is defined and described in Management Directive 8.4. If a licensee believes that the NRC is using this regulatory guide in a manner inconsistent with the discussion in this Implementation section, then the licensee may file a backfitting or forward fitting appeal with the NRC in accordance with the process in Management Directive 8.4.

REFERENCES[2]

1. Institute of Electrical and Electronics Engineers (IEEE) Standard (Std) 7-4.3.2-2016, "IEEE Standard Criteria for Programmable Digital Devices in Safety Systems of Nuclear Power Generating Stations," Piscataway, NJ, August 25, 2016.[3]

2. *U.S. Code of Federal Regulations* (CFR), "Domestic Licensing of Production and Utilization Facilities," Part 50, Chapter 1, Title 10, "Energy."

3. CFR, "Licenses, Certifications, and Approvals for Nuclear Power Plants," Part 52, Chapter 1, Title 10, "Energy."

4. IEEE Std 279-1968, "Proposed IEEE Criteria for Nuclear Power Plant Protection Systems," Piscataway, NJ.

5. IEEE Std 279-1971, "Criteria for Protection Systems for Nuclear Power Generating Stations," Piscataway, NJ.

6. IEEE Std 603-1991, "IEEE Criteria for Safety Systems for Nuclear Power Generating Stations," and the correction sheet dated January 30, 1995, Piscataway, NJ

7. U.S. Nuclear Regulatory Commission (NRC), Staff Requirements Memorandum to SECY-93-087, "SECY-93-087—Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Design," Washington, DC, July 21, 1993. (ADAMS Accession No. ML003708056)

8. NRC, NUREG-0800, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition," Chapter 7, "Instrumentation and Controls," Branch Technical Position 7-19, Revision 8, "Guidance for Evaluation of Defense in Depth and Diversity to Address Common-Cause Failure Due to Latent Design Defects in Digital Safety Systems," Washington, DC, January 2021.

9. NRC, Regulatory Guide 5.71, "Cyber Security Programs for Nuclear Facilities," Washington, DC.

10. CFR, "Physical Protection of Plants and Materials," Part 73, Chapter 1, Titles 10, "Energy."

11. IEEE Std 603-2009, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," Piscataway, NJ.

[2] Publicly available NRC published documents are available electronically through the NRC Library on the NRC's public Web site at http://www.nrc.gov/reading-rm/doc-collections/ and through the NRC's Agencywide Documents Access and Management System (ADAMS) at http://www.nrc.gov/reading-rm/adams.html. The documents can also be viewed online or printed for a fee in the NRC's Public Document Room (PDR) at 11555 Rockville Pike, Rockville, MD. For problems with ADAMS, contact the PDR staff at 301-415-4737 or (800) 397-4209; fax (301) 415-3548; or e-mail pdr.resource@nrc.gov.

[3] Copies of Institute of Electrical and Electronics Engineers (IEEE) documents may be purchased from the Institute of Electrical and Electronics Engineers Service Center, 445 Hoes Lane, PO Box 1331, Piscataway, NJ 08855, or through the IEEE's public Web site at http://www.ieee.org/publications_standards/index.html.

12. NRC, “Design Review Guide (DRG): Instrumentation and Controls for Non-Light-Water Reactor (Non-LWR) Reviews,” Washington, DC, February 26, 2021. (ADAMS Accession No. ML21011A140)

13. NRC, Regulatory Guide 1.164, “Dedication of Commercial-Grade Items for Use in Nuclear Power Plants,” Washington, DC.

14. Electric Power Research Institute (EPRI) 3002002982, “Plant Engineering: Guideline for the Acceptance of Commercial-Grade Design and Analysis Computer Programs Used in Nuclear Safety-Related Applications,” Palo Alto, CA, September 2014.[4]

15. NRC, Regulatory Guide 1.250, “Dedication of Commercial-Grade Digital I&C Items for Use in Nuclear Power Plants,” Washington, DC.

16. Nuclear Energy Institute, NEI 17-06, “Guidance on Using IEC 61508 SIL Certification to Support the Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Related Applications,” Revision 1, Washington, DC, December 2021 (ADAMS Accession No. ML21337A380).[5]

17. EPRI Topical Report (TR) 106439, “Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications,” Palo Alto, CA, October 1996.

18. NRC, “Safety Evaluation by the Office of Nuclear Reactor Regulation Electric Power Research Institute Topical Report, TR 106439, Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications,” Washington, DC, July 17, 1997. (ADAMS Accession No. ML12205A284)

19. NRC, “International Policy Statement,” Washington, DC, May 12, 2014. (ADAMS Accession No. ML14132A317)

20. NRC, Management Directive (MD) 6.6, “Regulatory Guides,” Washington, DC, May 2, 2016.

21. NRC, MD 8.4, “Management of Backfitting, Forward Fitting, Issue Finality, and Information Requests,” Washington, DC, September 20, 2019.

[4] Copies of Electric Power Research Institute (EPRI) standards and reports may be purchased from EPRI, 3420 Hillview Ave., Palo Alto, CA 94304; telephone (800) 313-3774; fax (925) 609-1310.

[5] Publications from the Nuclear Energy Institute (NEI) are available at their Web site: http://www.nei.org/or by contacting the headquarters at Nuclear Energy Institute, 1776 I Street NW, Washington DC 20006-3708, Phone: 202-739-800, Fax 202-785-4019.