U.S. NUCLEAR REGULATORY COMMISSION

July 2011
Revision 3

REGULATORY GUIDE

OFFICE OF NUCLEAR REGULATORY RESEARCH

REGULATORY GUIDE 1.152

(Draft was issued as DG-1249, dated June 2010)

CRITERIA FOR USE OF COMPUTERS IN SAFETY SYSTEMS OF NUCLEAR POWER PLANTS

A. INTRODUCTION

This guide describes a method that the staff of the U.S. Nuclear Regulatory Commission (NRC) considers acceptable to implement Title 10, of the *Code of Federal Regulations,* Part 50, "Domestic Licensing of Production and Utilization Facilities" (10 CFR Part 50) (Ref. 1); 10 CFR 50.55a(h); General Design Criterion (GDC) 21, "Protection System Reliability and Testability," of Appendix A, "General Design Criteria for Nuclear Power Plants," to 10 CFR Part 50; and Criterion III, "Design Control," of Appendix B, "Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants," to 10 CFR Part 50 with regard to the use of computers in safety systems of nuclear power plants. This guide applies to all types of commercial nuclear power plants.

This regulatory guide describes a method that the NRC staff deems acceptable for complying with the Commission's regulations for promoting high functional reliability, design quality, and a secure development and operational environment (SDOE) for the use of digital computers in the safety systems of nuclear power plants. In this context, the term "computer" identifies a system that includes computer hardware, software, firmware, and interfaces.

One of the requirements of GDC 21 is that protection systems (or safety systems) be designed for high functional reliability commensurate with the safety functions to be performed. Criterion III requires, in part, that licensees specify quality standards and provide design control measures for verifying or checking the adequacy of safety system designs.

The regulation at 10 CFR 50.55a(h)(2) requires that protection systems for "plants with construction permits issued after January 1, 1971, but before May 13, 1999, must meet the requirements

---

The NRC issues regulatory guides to describe and make available to the public methods that the NRC staff considers acceptable for use in implementing specific parts of the agency's regulations, techniques that the staff uses in evaluating specific problems or postulated accidents, and data that the staff needs in reviewing applications for permits and licenses. Regulatory guides are not substitutes for regulations, and compliance with them is not required. Methods and solutions that differ from those set forth in regulatory guides will be deemed acceptable if they provide a basis for the findings required for the issuance or continuance of a permit or license by the Commission.

This guide was issued after consideration of comments received from the public.

Regulatory guides are issued in 10 broad divisions: 1, Power Reactors; 2, Research and Test Reactors; 3, Fuels and Materials Facilities; 4, Environmental and Siting; 5, Materials and Plant Protection; 6, Products; 7, Transportation; 8, Occupational Health; 9, Antitrust and Financial Review; and 10, General.

Electronic copies of this guide and other recently issued guides are available through the NRC's public Web site under the Regulatory Guides document collection of the NRC's Electronic Reading Room 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, under Accession No. ML102870022. The regulatory analysis may be found in ADAMS under Accession No. ML101320317. The public comments and the NRC's response to them may be found in ADAMS under Accession No. ML102870028.

stated in either the Institute of Electrical and Electronics Engineers (IEEE) Std. 279, "Criteria for Protection Systems for Nuclear Power Generating Stations," (Ref. 2) or IEEE Std. 603-1991, "Criteria for Safety Systems for Nuclear Power Generating Stations," and the correction sheet dated January 30, 1995 (Ref. 3). For nuclear power plants with construction permits issued before January 1, 1971, protection systems must be consistent with their licensing basis, or may meet the requirements of IEEE Std. 603-1991 and the correction sheet dated January 30, 1995." In 10 CFR 50.55a(h)(3), the NRC states that, for safety systems, "applications filed on or after May 13, 1999, for construction permits and operating licenses under this part, and for design approvals, design certifications, and combined licenses under part 52 of this chapter, must meet the requirements for safety systems in IEEE Std. 603-1991 and the correction sheet dated January 30, 1995."

The NRC issues regulatory guides to describe to the public methods that the staff considers acceptable for use in implementing specific parts of the agency's regulations, to explain techniques that the staff uses in evaluating specific problems or postulated accidents, and to provide guidance to applicants. Regulatory guides are not substitutes for regulations and compliance with them is not required.

This regulatory guide contains information collection requirements covered by 10 CFR Part 50 that the Office of Management and Budget (OMB) approved under OMB control number 3150-0011. The NRC may neither conduct nor sponsor, and a person is not required to respond to, an information collection request or requirement unless the requesting document displays a currently valid OMB control number. This regulatory guide is a rule as designated in the Congressional Review Act (5 U.S.C. 801–808). However, the NRC has determined this regulatory guide is not a major rule as designated by the Congressional Review Act and has verified this determination with the OMB.

B. DISCUSSION

The regulation at 10 CFR 50.55a(h) requires that protection systems for nuclear power plants meet the requirements of IEEE Std. 603-1991 and the correction sheet dated January 30, 1995. With respect to the use of computers in safety systems, IEEE Std. 7-4.3.2 2003, "Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations," (Ref. 4) specifies computer-specific requirements to supplement the criteria and requirements of IEEE Std. 603-1998, "Standard Criteria for Safety Systems for Nuclear Power Generating Stations" (Ref. 5).

Working Group SC 6.4, "Application of Programmable Digital Computers to Safety Systems," of the IEEE Nuclear Power Engineering Committee prepared IEEE Std. 7-4.3.2-2003. This standard evolved from IEEE Std. 7-4.3.2-1993 and reflects advances in digital technology. It also represents a continued effort by IEEE to support the specification, design, and implementation of computers in safety systems of nuclear power plants. In addition, IEEE Std. 7-4.3.2-2003 contains computer-specific requirements to supplement the criteria and requirements of IEEE Std. 603-1998.

Instrumentation and control system designs that use computers in safety systems make extensive use of advanced technology (i.e., equipment and design practices). These designs are expected to be significantly and functionally different from current designs and may include the use of microprocessors, digital systems and displays, fiber optics, multiplexing, and different isolation techniques to achieve sufficient independence and redundancy.

With the introduction of digital systems into plant safety system designs, concerns have emerged about the possibility that a design error in the software in redundant safety system channels could lead to a common-cause failure or common-mode failure of the safety system function. Conditions may exist

under which some form of diversity may be necessary to provide additional assurance beyond that provided by the design and quality assurance programs that incorporate software quality assurance and verification and validation. The design techniques of functional diversity, design diversity, diversity in operation, and diversity within the four echelons of defense in depth (provided by the reactor protection, engineered safety features actuation, control, and monitoring instrumentation and control systems) can be applied as defense against common-cause failures. Manual operator actuations of safety and nonsafety systems are acceptable, provided that the necessary diverse controls and indications are available to perform the required function under the associated event conditions and can be completed within the acceptable time.

The justification for equipment diversity or for the diversity of related system software, such as a real-time operating system, must extend to equipment components to ensure that actual diversity exists. For example, different manufacturers might use the same processor or license the same operating system, thereby introducing the possibility of common failure modes. Claims of diversity based only on the use of different manufacturers are insufficient without consideration of the above.

With respect to software diversity, experience indicates that the independence of failure modes may not be achieved in cases in which multiple versions of software are developed from the same software requirements. The National Research Council documented this experience in a final report entitled, "Digital Instrumentation and Control Systems in Nuclear Power Plants - Safety and Reliability Issues," issued 1997 (Ref. 6). Other considerations, such as functional and signal diversity, that lead to different software requirements form a stronger basis for diversity. Other NRC staff positions and guidance govern diversity and defense-in-depth issues.

Some safety system designs may use computers that were not specifically designed for nuclear power plant applications. Clause 5.4.2 of IEEE Std. 7-4.3.2-2003 provides general guidance for commercial-grade dedication.

Clause 5.6(a) of IEEE Std. 7-4.3.2-2003 states: "Barrier requirements shall be identified to provide adequate confidence that the nonsafety functions cannot interfere with the performance of the safety functions of the software or firmware. The barriers shall be designed in accordance with the requirements of this standard. The nonsafety software is not required to meet these requirements." However, 10 CFR 50.55a(h) requires that nuclear power plants conform either to IEEE Std. 279-1971 or IEEE Std. 603-1991. Clause 4.7.1, "Classification of Equipment," of IEEE Std. 279-1971 requires that any equipment that is used for both protective and control functions be classified as part of the protection system. Clause 5.6.3.1, "Interconnected Equipment," of IEEE Std. 603-1991 also requires that equipment that is used for both safety and nonsafety functions be classified as part of the safety systems. The term "equipment" includes both the software and hardware components of the digital systems. For this reason, any software providing nonsafety functions that resides on a computer providing a safety function must be classified as a part of the safety system. If a licensee wants a safety-related computer system to perform a nonsafety function, it must classify the software that performs the nonsafety function as safety-related software with all the attendant regulatory requirements for safety software, including communications independence from other nonsafety software.

Clause 5.9, "Control of Access," of IEEE Std. 7-4.3.2-2003 refers to the requirements in Clause 5.9 of IEEE Std. 603-1998, which states, "The design shall permit the administrative control of access to safety system equipment. These administrative controls shall be supported by provisions within the safety systems, by provision in the generating station design, or by a combination thereof." IEEE Std. 7-4.3.2-2003 does not provide any additional guidance for computer-based system equipment and software systems to address the IEEE Std. 603-1998 access control requirements of Clause 5.9 or the independence requirements of Clause 5.6.3. Consequently, the NRC modified Regulatory Guide 1.152,

Revision 2, to include regulatory positions that provide specific guidance concerning the protection of the design and development phases of computer-based safety systems, which is intended to address the criteria within these clauses.[1] This guide is not intended to address the ability of those protective features to thwart malicious cyber attacks. The requirements of 10 CFR 73.54, "Protection of Digital Computer and Communication Systems and Networks" (Ref. 7), address cyber security of digital assets, which include those systems used to perform safety and important to safety, security, and emergency preparedness functions. In addition, the staff has determined that only Regulatory Positions 2.1 - 2.5 apply to licensing reviews and has removed Regulatory Positions 2.6 - 2.9 from this document.

The NRC published 10 CFR 73.54 to require licensees to develop cyber-security plans and programs to protect critical digital assets, including digital safety systems, from malicious cyber attacks. Regulatory Guide 5.71, "Cyber Security Programs for Nuclear Facilities" (Ref. 8), provides guidance to meet the requirements of 10 CFR 73.54. The programmatic cyber security provisions of this new regulation and its associated guidance address Regulatory Positions 2.6 - 2.9 in Revision 2 of Regulatory Guide 1.152, which the NRC has removed from this revision of the guide. For licensees that choose to provide, as part of their license submittal, descriptions of cyber-security design features intended to address the guidance of Regulatory Guide 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 system's reliability or its capability to perform its safety function.

To avoid confusion between the coverage of the provisions of this regulatory guide and 10 CFR 73.54, the licensee should note the following:

- Secure Development Environment is defined as the condition of having appropriate physical, logical and programmatic controls during the system development phases (i.e., concepts, requirements, design, implementation, testing) to ensure that unwanted, unneeded and undocumented functionality (e.g., superfluous code) is not introduced into digital safety systems.

- Secure Operational Environment is defined as the condition of having appropriate physical, logical and administrative controls within a facility to ensure that the reliable operation of digital safety systems are not degraded by undesirable behavior of connected systems and events initiated by inadvertent access to the system.

- The establishment of a Secure Development and Operational Environment (SDOE) for digital safety systems, in the context of Regulatory Guide 1.152, refers to: (1) measures and controls taken to establish a secure environment for development of the digital safety system against undocumented, unneeded and unwanted modifications and (2) protective actions taken against a predictable set of undesirable acts (e.g., inadvertent operator actions or the undesirable behavior of connected systems) that could challenge the integrity, reliability, or functionality of a digital safety system during operations. These SDOE actions may include adoption of protective design features into the digital safety system design to preclude inadvertent access to the system and/or protection against undesirable behavior from connected systems when operational.

[1] The design requirements of 10 CFR Part 50, including the need for redundancy, diversity, and defense in depth, are based on the need to ensure reliable system functionality in the face of a wide range of failure modes up to and including the "design-basis accidents" described in each site's updated final safety analysis report and in the combined operating license and design certification applicants' final safety analysis reports. The regulations at 10 CFR Part 50 do not require licensees to include cyber-security-related features (hardware or software or both) in safety-related system designs (i.e., features intended to provide protection against malicious cyber attacks).

- "Cyber security" refers to those measures and controls, implemented to comply with 10 CFR 73.54, to protect critical digital assets against the malicious acts of an adversary up to and including the design basis threat, as defined by 10 CFR 73.1, "Purpose and Scope. "

- This regulatory guide is not intended to be used in lieu of the guidance provided in Regulatory Guide 5.71 to comply with the cyber security requirements of 10 CFR 73.54. The guidance in this regulatory guide provides a method that licensees can use to comply with the requirements of both 10 CFR 50 and GDCs. The guidance in regulatory guide 5.71 provides a method that licensees can use to comply with the requirements of 10 CFR 73.54. Under the NRC regulations, licensees are required to comply with both regulations.

The NRC's intention is that the combination of this regulatory guide and the programmatic provisions under 10 CFR 73.54 should seamlessly address the secure design, development, and operation of digital safety systems. Notwithstanding the guidance in this regulatory guide, additional cyber-security restrictions may be imposed based on each nuclear facility's cyber-security program.

For digital safety systems, establishment of a secure development environment includes the protection of digital computer-based systems throughout the development life cycle of the system to prevent unauthorized, unintended, and unsafe modifications. During development, operation, and maintenance measures should be taken to protect safety systems from inadvertent actions that may result in unintended consequences to the system. Establishment of a secure development environment includes the protection of both physical and logical access to the safety system and its data such that controls should be provided to prevent unauthorized changes. Controls should address access through both network connections and maintenance equipment. Additionally, the design of the plant data communication systems should ensure that the systems do not present an electronic path by which a person can make unauthorized changes to plant safety systems or display erroneous plant status information to the operators.

The regulatory guide provides guidance for designing digital systems (hardware and software) such that they are free from vulnerabilities that could affect the reliability of the system. In the context of this regulatory guide, vulnerabilities are considered to be (1) deficiencies in the design that may allow inadvertent, unintended, or unauthorized access or modifications to the safety system that may degrade its reliability, integrity or functionality during operations or (2) an inability of the system to sustain the safety function in the presence of undesired behavior of connected systems. The considerations for hardware access control should include physical access control, configuration of modems, connectivity to external networks, data links, and open ports. The licensee can provide an SDOE for digital safety systems by (1) designing features that will meet the licensee's secure operational environment requirements for the systems, (2) ensuring that the system is developed without undocumented codes (e.g., backdoor coding), unwanted functions or applications, and any other coding that could adversely affect the reliable operation of the digital system, and (3) maintaining a secure operational environment for digital safety systems in accordance with the station administrative procedures and the licensee's other programs to protect against unwanted and unauthorized access or changes to these systems.

IEEE Std. 7-4.3.2-2003 includes the following seven informative annexes:

1. Annex A, "Mapping of IEEE Std. 603-1998 to IEEE Std. 7-4.3.2-2003," provides a mapping of the criteria of IEEE Std. 603-1998 to any elaborations found in IEEE Std. 7-4.3.2-2003. This particular annex does not contain any new guidance or requirements.

2. Annex B, "Diversity Requirements Determination," has not received NRC endorsement because it provides inadequate guidance. Additional guidance appears in NUREG-0800, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition" (Ref. 9), Chapter 7, "Instrumentation and Controls," Branch Technical Position 7-19, "Guidance for Evaluation of Diversity and Defense-in-Depth in Digital Computer-Based Instrumentation and Control Systems."

3. Annex C, "Dedication of Existing Commercial Computers," has not received NRC endorsement because it provides inadequate guidance. Electric Power Research Institute Topical Report (TR)-106439, "Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications," issued October 1996 (Ref. 10) contains adequate guidance, which the NRC has endorsed.

4. Annex D, "Identification and Resolution of Hazards," provides general information on the use of qualitative or quantitative fault tree analysis (FTA) and failure modes and effects analysis (FMEA) techniques throughout the system development life cycle. The staff agrees that FTA and FMEA are well-known techniques for analyzing potential hazards; however, the NRC has not endorsed this annex because it provides inadequate guidance concerning the use of FTA and FMEA techniques. While this Annex is not endorsed, the hazard identification guidance in Annex D may provide useful information on the assessment of the susceptibility of digital safety systems to inadvertent access or undesired behavior of connected systems.

5. Annex E, "Communication Independence," has not received NRC endorsement because it provides insufficient guidance. NUREG-0800, Appendix 7.0-A, "Review Process for Digital Instrumentation and Control Systems," Appendix 7.1-C, "Guidance for Evaluation of Conformance to IEEE Std. 603," and Section 7.9, "Data Communication Systems," provide additional guidance.

6. Annex F, "Computer Reliability," describes an approach for measuring the reliability of digital computers used in safety systems. The NRC does not endorse the concept of quantitative reliability goals as a sole means of meeting its regulations for the reliability of digital computers used in safety systems. The NRC's acceptance of the reliability of computer systems is based on deterministic criteria for both hardware and software. Quantitative reliability determination, using a combination of analysis, testing, and operating experience, can provide an added level of confidence in the reliable performance of computer systems.

7. Annex G, "Bibliography," provides the references used in the standard. The bibliography provides sufficient detail to enable licensees to obtain further information on specific areas of the standard.

As discussed below, the NRC has not endorsed Annexes B - F. Regulatory Positions 2.1 - 2.5 provide specific guidance concerning the establishment of an SDOE for the protection of digital safety systems against undesirable actions and events that may affect the reliable operation of the system.

C. REGULATORY POSITION

1. Functional and Design Requirements

Conformance with the requirements of IEEE Std. 7-4.3.2-2003 is a method that the NRC staff has deemed acceptable for satisfying the NRC's regulations with respect to high functional reliability and design requirements for computers used in the safety systems of nuclear power plants. As addressed in Section B above, the NRC does not endorse Annexes B-F of IEEE Std. 7-4.3.2-2003.

2. Secure Development and Operational Environment for the Protection of Digital Safety Systems

This regulatory position uses the life cycle phases of the waterfall model only as a framework for describing specific guidance for the protection of digital safety systems and the establishment of an SDOE for those systems. The digital safety system development process should identify and mitigate potential weakness or vulnerabilities in each phase of the digital safety system life cycle that may degrade the SDOE or degrade the reliability of the system. The framework for the waterfall life cycle model consists of the following phases:

(1) concepts,
(2) requirements,
(3) design,
(4) implementation,
(5) test,
(6) installation, checkout, and acceptance testing,
(7) operation,
(8) maintenance, and
(9) retirement.

The NRC will evaluate the secure development environment controls applied to safety system development through the test phase and any secure operational environment design features intended to ensure reliable system operation included in a submittal as part of its review of a license amendment request, design certification, or combined license application. Cyber-security and other security controls applied to the latter phases of the life cycle that occur at a licensee's site (i.e., site installation, operation, maintenance, and retirement) are not part of the 10 CFR Part 50 licensing process and fall under the purview of other licensee programs. When vendors develop digital safety systems, licensees should include provisions in their procurement specification to ensure that the vendor takes appropriate measures to establish a secure development environment and includes any features in the system design required by the licensee to support a secure operational environment for the digital safety system.

Regulatory Positions 2.1 - 2.5 describe digital safety system guidance for the establishment of a secure environment during the design and development phases of the life cycle and are applicable to the review of license amendment requests, design certification, and combined operating license applications. The guidance is specifically intended to ensure reliable operation of digital safety systems.

2.1 Concepts Phase

In the concepts phase, the licensee should identify digital safety system design features required to establish a secure operational environment for the system. A licensee should describe these design features as part of its application.

The licensee should assess the digital safety system's potential susceptibility to inadvertent access and undesirable behavior from connected systems over the course of the system's life cycle that could degrade its reliable operation. This assessment should identify the potential challenges to maintaining a secure operational environment for the digital safety system and a secure development environment for development life cycle phases. The results of the analysis should be used to establish design feature requirements (for both hardware and software) to establish a secure operational environment and protective measures to maintain it.

The licensee should not allow remote access to the safety system. For the purposes of this guidance, remote access is defined as the ability to access a computer, node, or network resource that performs a safety function or that can affect the safety function from a computer or node that is located in an area with less physical security than the safety system (e.g., outside the protected area).

Other NRC staff positions and guidance govern unidirectional and bidirectional data communications between safety and nonsafety digital systems.

2.2 Requirements Phase

2.2.1 System Features

The licensee should define the functional performance requirements and system configuration for a secure operational environment; interfaces external to the system; and requirements for qualification, human factors engineering, data definitions, documentation for the software and hardware, installation and acceptance, operation and execution, and maintenance.

The design feature requirements intended to maintain a secure operating environment and ensure reliable system operation should be part of the overall system requirements. Therefore, the verification process of the requirements phase should ensure the correctness, completeness, accuracy, testability, and consistency of the system's SDOE feature.

Requirements specifying the use of pre-developed software and systems (e.g., reused software and commercial off-the-shelf (COTS) systems) should address the reliability of the safety system (e.g., by using pre-developed software functions that have been tested and are supported by operating experience).

2.2.2 Development Activities

During the requirements phase, the licensee should prevent the introduction of unnecessary or extraneous requirements that may result in inclusion of unwanted or unnecessary code.

2.3 Design Phase

2.3.1 System Features

The safety system design features for a secure operational environment identified in the system requirements specification should be translated into specific design configuration items in the system design description.

Licensees should be aware that digital safety systems will be considered Critical Digital Assets and must adhere to the requirements of 10 CFR 73.54. Regulatory Guide 5.71 describes an acceptable defensive architecture to comply with 10 CFR 73.54. The architecture described in the guidance would have licensees place all digital safety systems in the highest level of their defensive architecture and only

permit one-way communication (if any communication is desired) from the digital safety system to other systems in lower levels of the defensive architecture. Licensees should be aware that Section B.1.4 of Appendix B to Regulatory Guide 5.71 notes that one-way communications should be enforced using hardware mechanisms. A licensee's adherence to the provisions of 10 CFR 73.54 will be evaluated per regulatory programs specific to that regulation.

The safety system design configuration items for a secure operational environment intended to ensure reliable system operation should address control over (1) physical and logical access to the system functions, (2) use of safety system services, and (3) data communication with other systems. Design configuration items that incorporate pre-developed software into the safety system should address how this software will not challenge the secure operational environment for the safety system.

Physical and logical access control features should be based on the results of the assessment performed in the concepts phase of the life cycle. The results of this assessment may identify the need for more complex access control measures, such as a combination of knowledge (e.g., password), property (e.g., key and smart card), or personal features (e.g., fingerprints), rather than just a password.

2.3.2 Development Activities

During the design phase, measures should be taken to prevent the introduction of unnecessary design features or functions that may result in the inclusion of unwanted or unnecessary code.

2.4 Implementation Phase

In the system (integrated hardware and software) implementation phase, the system design is transformed into code, database structures, and related machine executable representations.

The implementation activity addresses hardware configuration and setup, software coding and testing, and communication configuration and setup (including the incorporation of reused software and COTS products).

2.4.1 System Features

The developer should ensure that the transformation from the system design specification to the design configuration items of the secure operational environment is correct, accurate, and complete.

2.4.2 Development Activities

The developer should implement secure development environment procedures and standards to minimize and mitigate any inadvertent or inappropriate alterations of the developed system. The developer's standards and procedures should include testing, (such as scanning), as appropriate, to address undocumented codes or functions that might (1) allow unauthorized access or use of the system or (2) cause systems to behave outside of the system requirements or in an unreliable manner.

The developer should account for hidden functions and vulnerable features embedded in the code, their purpose and their impact on the integrity and reliability of the safety system. These functions should be removed or (as a minimum) addressed (e.g., as part of the failure modes and effects analysis of the application code) to prevent any unauthorized access or degradation of the reliability of the safety system.

COTS systems are likely to be proprietary and generally unavailable for review. In addition, a reliable method may not exist for determining the complete set of system behaviors inherent in a given

operating system (e.g., operating system suppliers often do not provide access to the source code for operating systems and callable code libraries). In such cases, unless the application developer can modify these systems, the developer should ensure that the features within the operating system do not compromise the required design features of the secure operational environment so as to degrade the reliability of the digital safety system.

2.5 Test Phase

The objective of testing the design features of the secure operational environment is to ensure that the design requirements intended to ensure system reliability are validated by the execution of integration, system, and acceptance tests where practical and necessary.

Testing includes system hardware configuration (including all connectivity to other systems, including external systems), software integration testing, software qualification testing, system integration testing, system qualification testing, and system factory acceptance testing.

2.5.1 System Features

The secure operational environment design requirements and configuration items intended to ensure reliable system operation should be part of the validation effort for the overall system requirements and design configuration items. Therefore, design configuration items for the secure operational environment are just one element of the overall system validation. Each system design feature of the secure operational environment should be validated to verify that the implemented feature achieves its intended function to protect against inadvertent access or the effects of undesirable behavior of connected systems and does not degrade the safety system's reliability.

2.5.2 Development Activities

The developer should correctly configure and enable the design features of the secure operational environment. The developer should also test the system hardware architecture, external communication devices, and configurations for unauthorized pathways and system integrity. Attention should be focused on built-in original equipment manufacturer features.

3. Referenced Standards

Clause 2 of IEEE Std. 7-4.3.2-2003 references several industry codes and standards. If the NRC has incorporated a referenced standard into its regulations, licensees and applicants must comply with the standard as set forth in those regulations. If the NRC staff has endorsed the referenced standard in a regulatory guide, the standard constitutes an acceptable method for use in meeting a regulatory requirement as described in the regulatory guide. If the NRC has neither incorporated a referenced standard into its regulations nor endorsed the standard in a regulatory guide, licensees and applicants may consider and use the information in the referenced standard, if appropriately justified, consistent with regulatory practice.

D. IMPLEMENTATION

The purpose of this section is to provide information on how applicants and licensees[2] may use this guide and information regarding the NRC's plans for using this regulatory guide. In addition, it describes how the NRC staff complies with the Backfit Rule (10 CFR 50.109) and any applicable finality provisions in 10 CFR Part 52.

Use by Applicants and Licensees

Applicants and licensees may voluntarily[3] use the guidance in this document to demonstrate compliance with the underlying NRC regulations. Methods or solutions that differ from those described in this regulatory guide may be deemed acceptable if they provide sufficient basis and information for the NRC staff to verify that the proposed alternative demonstrates compliance with the appropriate NRC regulations. Current licensees may continue to use guidance the NRC found acceptable for complying with the identified regulations as long as their current licensing basis remains unchanged.

Licensees may use the information in this regulatory guide for actions which do not require NRC review and approval such as changes to a facility design under 10 CFR 50.59. Licensees may use the information in this regulatory guide or applicable parts to resolve regulatory or inspection issues.

Use by NRC Staff

The staff may discuss with licensees, various actions consistent with staff positions in this regulatory guide, as one acceptable means of meeting the underlying NRC regulatory requirement. Such discussions would not ordinarily be considered backfitting even if prior versions of this regulatory guide are part of the licensing basis of the facility. However, unless this regulatory guide is part of the licensing basis for a facility, the staff may not represent to the licensee that the licensee's failure to comply with the positions in this regulatory guide constitutes a violation.

If an existing licensee voluntarily seeks a license amendment or change and (1) the NRC staff's consideration of the request involves a regulatory issue directly relevant to this new or revised regulatory guide and (2) the specific subject matter of this regulatory guide is an essential consideration in the staff's determination of the acceptability of the licensee's request, then the staff may request that the licensee either follow the guidance in this regulatory guide or provide an equivalent alternative process that demonstrates compliance with the underlying NRC regulatory requirements. This is not considered backfitting as defined in 10 CFR 50.109(a)(1) or a violation of any of the issue finality provisions in 10 CFR Part 52.

The NRC staff does not intend or approve any imposition or backfitting of the guidance in this regulatory guide. The NRC staff does not expect any existing licensee to use or commit to using the guidance in this regulatory guide, unless the licensee makes a change to its licensing basis. The NRC staff does not expect or plan to request licensees to voluntarily adopt this regulatory guide to resolve a generic regulatory issue. The NRC staff does not expect or plan to initiate NRC regulatory action which would require the use of this regulatory guide. Examples of such unplanned NRC regulatory actions

---

[2] In this section, "licensees" refers to licensees of nuclear power plants under 10 CFR Parts 50 and 52; and the term "applicants," refers to applicants for licenses and permits for (or relating to) nuclear power plants under 10 CFR Parts 50 and 52, and applicants for standard design approvals and standard design certifications under 10 CFR Part 52.

[3] In this section, "voluntary" and "voluntarily" means that the licensee is seeking the action of its own accord, without the force of a legally binding requirement or an NRC representation of further licensing or enforcement action.

include issuance of an order requiring the use of the regulatory guide, requests for information under 10 CFR 50.54(f) as to whether a licensee intends to commit to use of this regulatory guide, generic communication, or promulgation of a rule requiring the use of this regulatory guide without further backfit consideration.

Additionally, an existing applicant may be required to adhere to new rules, orders, or guidance if 10 CFR 50.109(a)(3) applies.

Conclusion

This regulatory guide is not being imposed upon current licensees and may be voluntarily used by existing licensees. In addition, this regulatory guide is issued in conformance with all applicable internal NRC policies and procedures governing backfitting. Accordingly, the NRC staff issuance of this regulatory guide is not considered backfitting, as defined in 10 CFR 50.109(a)(1), nor is it deemed to be in conflict with any of the issue finality provisions in 10 CFR Part 52.

If a licensee believes that the NRC is either using this regulatory guide or requesting or requiring the licensee to implement the methods or processes in this regulatory guide in a manner inconsistent with the discussion in this Implementation section, then the licensee may file a backfit appeal with the NRC in accordance with the guidance in NUREG-1409 and NRC Management Directive 8.4.

REFERENCES[4]

1. 10 CFR Part 50, "Domestic Licensing of Production and Utilization Facilities," U.S. Nuclear Regulatory Commission, Washington, DC.

2. IEEE Std. 279-1971, "Criteria for Protection Systems for Nuclear Power Generating Stations," Institute of Electrical and Electronics Engineers, Piscataway, NJ.[5]

3. IEEE Std. 603 1991, "Criteria for Safety Systems for Nuclear Power Generating Stations," and the correction sheet dated January 30, 1995, Institute of Electrical and Electronics Engineers, Piscataway, NJ.

4. IEEE Std. 7-4.3.2-2003, "Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations," Institute of Electrical and Electronics Engineers, Piscataway, NJ

5. IEEE Std. 603-1998, "Standard Criteria for Safety Systems for Nuclear Power Generating Stations," Institute of Electrical and Electronics Engineers, Piscataway, NJ.

6. "Digital Instrumentation and Control Systems in Nuclear Power Plants—Safety and Reliability Issues," National Research Council, Washington, DC, 1997.[6]

7. 10 CFR Part 73, "Physical Protection of Plants and Materials," U.S. Nuclear Regulatory Commission, Washington, DC.

8. Regulatory Guide 5.71, "Cyber Security Programs for Nuclear Facilities," U.S. Nuclear Regulatory Commission, Washington, DC.

9. NUREG-0800, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition," U.S. Nuclear Regulatory Commission, Washington, DC.

10. TR-106439, "Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications," Electric Power Research Institute, Palo Alto, CA, October 1996.[7]

---

[4] All publicly available NRC documents are available electronically through the Electronic Reading Room on the NRC's public Web site at http://www.nrc.gov/reading rm/doc collections/cfr/. The documents can also be viewed on-line for free or printed for a fee in the NRC's Public Document Room (PDR) at 11555 Rockville Pike, Rockville, MD; the mailing address is USNRC PDR, Washington, DC 20555; telephone (301) 415-4737 or (800) 397-4209; fax (301) 415 3548; and e mail pdr.resource@nrc.gov.

[5] 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.

[6] Publications of the National Research Council may be purchased through the National Academies Press at their Web site www.NAP.edu, or by contacting the NAP bookstore at 500 Fifth St. N.W., Washington DC 20001, Phone (202) 334-2451.

[7] Copies of Electric Power Research Institute (EPRI) documents may be obtained by contacting the Electric Power Research Institute, 3420 Hillview Avenue, Palo Alto, CA 94304, Telephone: 650-855-2000 or on-line at http://my.epri.com/portal/server.pt.