U.S. NUCLEAR REGULATORY COMMISSION

Revision 2
January 2006

REGULATORY GUIDE

OFFICE OF NUCLEAR REGULATORY RESEARCH

REGULATORY GUIDE 1.152

(*Draft was issued as DG-1130, dated December 2004*)

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

A. INTRODUCTION

General Design Criterion (GDC) 21, "Protection System Reliability and Testability," of Appendix A, "General Design Criteria for Nuclear Power Plants," to Title 10, Part 50, "Domestic Licensing of Production and Utilization Facilities," of the *Code of Federal Regulations* (10 CFR Part 50), requires, among other things, that protection systems (or safety systems) must be designed for high functional reliability commensurate with the safety functions to be performed. Criterion III, "Design Control," of Appendix B, "Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants," to 10 CFR Part 50, requires, among other things, that quality standards must be specified and design control measures must be provided for verifying or checking the adequacy of design.

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

The Advisory Committee on Reactor Safeguards has been consulted concerning this guide and has concurred in the stated regulatory positions.

This regulatory guide contains information collections that are covered by the requirements of 10 CFR Part 50, which 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.

B. DISCUSSION

IEEE Std 7-4.3.2-2003, "Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations," was prepared by Working Group SC 6.4, "Application of Programmable Digital Computers to Safety Systems," of the Institute of Electrical and Electronics Engineers (IEEE) Nuclear Power Engineering Committee. 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 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."

Instrumentation and control (I&C) 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 regarding the possibility that a design error in the software in redundant channels of a safety system could lead to common-cause 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 (QA) programs that incorporate software QA and verification and validation (V&V). 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 I&C 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 within the acceptable time.

The justification for equipment diversity, or for the diversity of related system software such as a realtime 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 incorporating common failure modes. Claims for diversity based only on different manufacturers are insufficient without consideration of the above.

With respect to software diversity, experience (as documented in the final report, entitled "Digital Instrumentation and Control Systems in Nuclear Power Plants — Safety and Reliability Issues," which the National Research Council published in 1997) indicates that independence of failure modes may not be achieved in cases where multiple versions of software are developed from the same software requirements. Other considerations, such as functional and signal diversity, that lead to different software requirements form a stronger basis for diversity.

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 that "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, "Criteria for Protection Systems For Nuclear Generating Stations" or IEEE Std. 603-1991, "Criteria for Safety Systems for Nuclear Power Generating Stations." IEEE Std. 279-1971, paragraph 4.7.1, "Classification of Equipment," requires that any equipment that is used for both protective and control functions shall be classified as part of the protection system. IEEE Std. 603-1991, paragraph 5.6.3.1, "Interconnected Equipment," also requires that equipment that is used for both safety and nonsafety functions shall be classified as part of the safety systems. The term "equipment" includes both software and hardware of the digital systems. For this reason, any software providing nonsafety functions that resides on the computer providing a safety function must be classified as a part of the safety system. If a licensee desires that a nonsafety function be performed by a safety computer, the software to perform that function must be classified as safety-related, with all the attendant regulatory requirements for safety software, including communications isolation from other nonsafety software.

IEEE Std 7-4.3.2-2003 does not provide guidance regarding security measures for computer-based system equipment and software systems. Consequently, the NRC has modified this regulatory guide to include Regulatory Positions 2.1 – 2.9, which provide specific guidance concerning computer-based (cyber) safety system security.

Clause 5.9 of IEEE Std 7-4.3.2-2003, "Control of Access," refers to the applicable requirements in IEEE Std 603-1998 and 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." For digital computer-based systems, controls of both physical and electronic access to safety system and data should be provided to prevent unauthorized changes. Controls should address access via network connections and via 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.

Computer-based systems (hardware and software) must be secure from electronic vulnerabilities. The consideration of hardware should include physical access control, modems, connectivity to external networks, data links, open ports, etc. Security of computer-based system software relates to the ability to prevent unauthorized, undesirable, and unsafe intrusions throughout the life cycle of the safety system. Computer-based systems are secure from electronic vulnerabilities if unauthorized and inappropriate access and use of those systems is prevented. The security of computer-based systems is established through (1) designing the security features that will meet licensee's security requirements in the systems, (2) developing the systems without undocumented codes (e.g., back door coding, viruses, worms, Trojan horses, and bomb codes), and (3) installing and maintaining those systems in accordance with the station administrative procedures and the licensee's security program.

IEEE Std 7-4.3.2-2003 includes seven informative annexes. As discussed below, the NRC has not endorsed Annexes B – F:

(a) Annex A, "Mapping of IEEE Std 603-1998 to IEEE Std 7-4.3.2-2003," does not provide any guidance or requirements.

(b) Annex B, "Diversity Requirements Determination," is not endorsed by the NRC because it provides inadequate guidance. Branch Technical Position (BTP) HICB-19, "Guidance for Evaluation of Defense-in-Depth and Diversity in Digital Computer-Based Instrumentation and Control Systems," in NUREG-0800, "Standard Review Plan," Section 7, "Instrumentation and Controls," provides additional guidance.

(c) Annex C, "Dedication of Existing Commercial Computers," is not endorsed by the NRC because it provides inadequate guidance. Adequate guidance is available in EPRI TR-106439, "Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications," which the NRC has endorsed.

(d) Annex D, "Identification and Resolution of Hazards," provides general information regarding 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, this annex is not endorsed because it provides inadequate guidance concerning the use of FTA and FMEA.

(e) Annex E, "Communication Independence," is not endorsed by the NRC because it provides insufficient guidance. Additional guidance is provided in 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," in NUREG-0800.

(f) 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 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 the computer systems.

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

Regulatory Positions 2.1 – 2.9 provide specific guidance concerning safety system security.

C. REGULATORY POSITION

1. Functional and Design Requirements

Conformance with the requirements of IEEE Std 7-4.3.2-2003, "Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations," 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 safety systems of nuclear power plants.

2. Security

This regulatory position uses the waterfall lifecycle phases only as a framework for describing specific digital safety system security guidance. The digital safety system development process should address potential security vulnerabilities in each phase of the digital safety system lifecycle.
The framework waterfall lifecycle consists of the following phases:

- Concepts
- Requirements
- Design
- Implementation
- Test
- Installation, Checkout, and Acceptance Testing
- Operation
- Maintenance
- Retirement

The lifecycle phase-specific security requirements should be commensurate with the risk and magnitude of the harm resulting from unauthorized and inappropriate access, use, disclosure, disruption, or destruction of the digital safety system.

Regulatory positions 2.1 – 2.9 describe digital safety system security guidance for the individual phases of the lifecycle.

2.1 Concepts Phase

In the concepts phase, the licensee and developer should identify safety system security capabilities that should be implemented.

The licensee and developer should perform security assessment to identify potential security vulnerabilities in the relevant phases of the system life cycle. The results of the analysis should be used to establish security requirements for the system (hardware and software).

Remote access to the safety system should not be implemented. Computer-based safety systems may transfer data to other systems through one-way communication pathways.

2.2 Requirements Phase

2.2.1 *System Features*

The licensees and developers should define the security functional performance requirements and system configuration; interfaces external to the system; and the requirements for qualification, human factors engineering, data definitions, documentation for the software and hardware, installation and acceptance, operation and execution, and maintenance.

The security requirements should be part of the overall system requirements. Therefore, the V&V process of the overall system should ensure the correctness, completeness, accuracy, testability, and consistency of the system security requirements.

Requirements specifying the use of pre-developed software and systems (e.g., reuse software and commercial off-the-shelf systems) should address the vulnerability 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*

The development process should ensure the system does not contain undocumented code (e.g., back door coding), malicious code (e.g., intrusions, viruses, worms, Trojan horses, or bomb codes), and other unwanted and undocumented functions or applications.

2.3 Design Phase

2.3.1 *System Features*

The safety system security requirements identified in the system requirements specification should be translated into specific design configuration items in the system design description. The safety system security design configuration items 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 incorporating pre-developed software into the safety system should address security vulnerabilities of the safety system.

Physical and logical access control should be based on the results of cyber-security qualitative risk analyses. Cyber-security risk is the combination of the consequence to the nuclear power plant and the susceptibility of a digital system to internal and external cyber-attack. The results of the analyses may require more complex access control, such as a combination of knowledge (e.g., password), property (e.g., key, smart-card) or personal features (e.g., fingerprints), rather than just a password.

2.3.2 *Development Activities*

The developer should delineate the standards and procedures that will conform with the applicable security policies to ensure the system design products (hardware and software) do not contain undocumented code (e.g., back door coding), malicious code (e.g., intrusions, viruses, worms, Trojan horses, or bomb codes), and other unwanted or undocumented functions or applications.

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 set-up [including the incorporation of reused software and commercial off-the-shelf (COTS) products].

2.4.1 *System Features*

The developer should ensure that the security design configuration item transformations from the system design specification are correct, accurate, and complete.

2.4.2 *Development Activities*

The developer should implement security procedures and standards to minimize and mitigate tampering with the developed system. The developer's standards and procedures should include testing with scanning as appropriate, to address undocumented codes or malicious functions that might (1) allow unauthorized access or use of the system or (2) cause systems to behave beyond the system requirements. The developer should account for hidden functions and vulnerable features embedded in the code, and their purpose and impact on the safety system. If possible, these functions should be disabled, removed, or (as a minimum) addressed (e.g., as part of the failure modes and affects analysis of the application code) to prevent any unauthorized access.

Scanning is dependent on the platform and code being used, and may not be available for the specified code and compiler. This may be a difficult task with little assurance that the results will be comprehensive and successful in uncovering hidden problems given the size and complexity of most modern computer systems. Pure application code scanning may be partially successful, but many operating systems, machine code, and callable library function aspects of the system may not be able to be successfully scanned and are just as likely to be where avenues for exploitation exist.

COTS systems are likely to be proprietary and generally unavailable for review. It is likely that there is no reliable method to determine security vulnerabilities for Operating systems (for example, Microsoft and other operating system suppliers do not provide access to the source code for operating systems and callable code libraries). In such cases, unless such systems are modified by the application developer, the security effort should be limited to ensuring that the features within the system do not compromise the security requirements of the system, and the security functions should not be compromised by the other system functions.

2.5 Test Phase

The objective of testing security functions is to ensure that the system security requirements are validated by execution of integration, system, and acceptance tests where practical and necessary. Testing includes system hardware configuration (including all external connectivity), software integration testing, software qualification testing, system integration testing, system qualification testing, and system factory acceptance testing.

2.5.1 *System Features*

The security requirements and configuration items are part of validation of the overall system requirements and design configuration items. Therefore, security design configuration items are just one element of the overall system validation. Each system security feature should be validated to verify that the implemented system does not increase the risk of security vulnerabilities and does not reduce the reliability of safety functions.

2.5.2 *Development Activities*

The developer should configure and enable the designed security features correctly. 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 OEM features.

2.6 Installation, Checkout, and Acceptance Testing

In installation and checkout, the safety system is installed and tested in the target environment. The system licensee should perform an acceptance review and test the safety system security features. The objective of installation and checkout security testing is to verify and validate the correctness of the safety physical and logical system security features in the target environment.

2.6.1 *System Features*

The licensee should ensure that the system features enable the licensee to perform post-installation testing of the system to verify and validate that the security requirements have been incorporated into the system appropriately.

2.6.2 *Development Activities*

A licensee should have a digital system security program. The security policies, standards, and procedures should ensure that installation of the digital system will not compromise the security of the digital system, other systems, or the plant. This may require the licensee to perform a security assessment, which includes a risk assessment, to identify the potential security vulnerabilities caused by installation of the digital system. The risk assessment should include an evaluation of new security constraints in the system; an assessment of the proposed system changes and their impact on system security; and an evaluation of operating procedures for correctness and usability. The results of this assessment should provide a technical basis for establishing certain security levels for the systems and the plant.

2.7 Operation Phase

The operation lifecycle process involves the use of the safety system by the licensee in its intended operational environment. During the operations phase, the licensee should ensure that the system security is intact by techniques such as periodic testing and monitoring, review of system logs, and real-time monitoring where possible.

The licensee should evaluate the impact of safety system changes in the operating environment on safety system security; assess the effect on safety system security of any proposed changes; evaluate operating procedures for compliance with the intended use; and analyze security risks affecting the licensee and the system. The licensee should evaluate new security constraints in the system; assess proposed system changes and their impact on system security; and evaluate operating procedures for correctness and usability.

2.8 Maintenance Phase

The maintenance phase is activated when the licensee changes the system or associated documentation. These changes may be categorized as follows:

- Modifications (i.e., corrective, adaptive, or perfective changes)
- Migration (i.e., the movement of system to a new operational environment)
- Replacement (i.e., the withdrawal of active support by the operation and maintenance organization, partial or total replacement by a new system, or installation of an upgraded system)

System modifications may be derived from requirements specified to correct errors (corrective), to adapt to a changed operating environment (adaptive), or to respond to additional licensee requests or enhancements (perfective).

2.8.1 *Maintenance Activities*

Modifications of the safety system should be treated as development processes and should be verified and validated as described above. Security functions should be assessed as described in the above regulatory positions, and should be revised (as appropriate) to reflect requirements derived from the maintenance process.

When migrating systems, the licensee should verify that the migrated systems meet the safety system security requirements. The maintenance process should continue to conform to existing safety system security requirements unless those requirements are to be changed as part of the maintenance activity.

2.8.2 *Quality Assurance*

The licensee should address security in its quality assurance program. The security quality assurance section can be incorporated into the existing quality assurance program. The cyber-security features should be maintained under a configuration management program.

The licensee's quality assurance group (such as information/network security expert) should conduct periodic audits to determine the effectiveness of the digital safety system security procedures.

If the safety system security functions were not previously verified and validated using a level of effort commensurate with the safety system security functional requirements, and appropriate documentation is not available or adequate, the licensee should determine whether the missing or incomplete documentation should be generated. In making this determination of whether to generate missing documentation, the minimum safety system security functional requirements should be taken into consideration.

2.8.3 *Incident Response*

The licensee should develop an incident response and recovery plan for responding to digital system security incidents(e.g., intrusions, viruses, worms, Trojan horses, or bomb codes). The plan should be developed to address various loss scenarios and undesirable operations of plant digital systems, including possible interruptions in service due to the loss of system resources, data, facility, staff, and/or infrastructure. The plan should define contingencies for ensuring minimal disruption to critical services in these instances.

2.8.4 *Audits and Assessments*

The licensee should perform periodic computer system security self-assessments and audits, which are key components of a good security program. The licensee should assess proposed safety system changes and their impact on safety system security; evaluate anomalies that are discovered during operation; assess migration requirements; and assess modifications made including V&V tasks to ensure that vulnerabilities have not been introduced into the plant environment from modifications.

2.9 Retirement Phase

In the retirement lifecycle phase, the licensee should assess the effect of replacing or removing the existing safety system security functions from the operating environment. The licensee should include in the scope of this assessment the effect on safety and nonsafety system interfaces of removing the system security functions. The licensee should document the methods by which a change in the safety system security functions will be mitigated (e.g., replacement of the security functions, isolation from other safety systems and licensee interactions, or retirement of the safety system interfacing functions). The security procedures should include cleansing the hardware and data. Upon removal from service, the licensee should consider data cleansing, disk destruction, or complete overwrite.

3. Referenced Standards

Clause 2 of IEEE Std 7-4.3.2-2003 references several industry codes and standards. If a referenced standard has been separately incorporated into the NRC's regulations, licensees and applicants must comply with the standard as set forth in the regulations. If the referenced standard has been endorsed by the NRC staff in a regulatory guide, the standard constitutes an acceptable method of meeting a regulatory requirement as described in the regulatory guide. If a referenced standard has been neither incorporated into the NRC's regulations nor endorsed 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 to applicants and licensees regarding the NRC staff's plans for using this guide. No backfitting is intended or approved in connection with the issuance of this guide.

Except in cases in which an applicant or licensee proposes or has previously established an acceptable alternative method for complying with specified portions of the NRC's regulations, the methods to be described in this guide will be used in evaluation of (1) submittals in connection with applications for construction permits, design certifications, operating licenses, and combined licenses for use of computers in safety systems, and (2) submittals from operating reactor licensees who voluntarily propose to initiate safety system modifications if there is a clear nexus between the proposed modifications and this guidance with respect to the requirements for use of computers in safety systems of nuclear power plants.

REGULATORY ANALYSIS

The NRC staff did not prepare a separate regulatory analysis for this regulatory guide. However, the regulatory analysis for Draft Regulatory Guide DG-1130, "Criteria for use of Computers in Safety Systems of Nuclear Power Plants," dated December 2004, provides the regulatory basis for this regulatory guide. The NRC issued DG-1130 in December 2004 to solicit public comment concerning the draft of this Revision 2 of Regulatory Guide 1.152.

A copy of the regulatory analysis for DG-1130 is available for inspection and copying for a fee at the NRC's Public Document Room (PDR), which is located at 11555 Rockville Pike, Rockville, Maryland; the PDR's mailing address is USNRC PDR, Washington, DC 20555-0001. The PDR can also be reached by telephone at (301) 415-4737 or (800) 397-4205, by fax at (301) 415-3548, and by email to PDR@nrc.gov. Copies are also available at current rates from the U.S. Government Printing Office at P.O. Box 37082, Washington, DC 20402-9328 or by telephone at (202) 512-1800. In addition, copies are available at current rates from the National Technical Information Service at 5285 Port Royal Road, Springfield, VA 22161, on the Internet at http://www.ntis.gov, or by telephone at (703) 487-4650. In addition, the regulatory analysis is available electronically as a part of Draft Regulatory Guide DG-1130 through the NRC's Agencywide Documents Access and Management System (ADAMS) at http://www.nrc.gov/reading-rm/adams.html, under Accession No. ML043170314. Note, however, that the NRC has temporarily suspended public access to ADAMS so that the agency can complete security reviews of publicly available documents and remove potentially sensitive information. Please check the NRC's Web site for updates concerning the resumption of public access to ADAMS.