RDB received
5/12/05

TXU
Power

TXU Power
Comanche Peak Steam
Electric Station
P. O. Box 1002 (E01)
Glen Rose, TX 76043
Tel: 254 897 5209
Fax: 254 897 6652
mike.blevins@txu.com

Mike Blevins
Senior Vice President &
Chief Nuclear Officer

2/16/05
70FR7973
(1)

Ref: DG-1130

CPSES-200500996
Log # TXX-05096

May 4, 2005

Rules and Directives Branch, Office of Administration
U. S. Nuclear Regulatory Commission
Washington, DC 20555

SUBJECT: COMANCHE PEAK STEAM ELECTRIC STATION (CPSES) COMMENTS ON DRAFT REGULATORY GUIDE DG-1130, CRITERIA FOR USE OF COMPUTERS IN SAFETY SYSTEMS OF NUCLEAR POWER PLANTS (69 FR 75359)

Gentlemen:

Attached are comments from TXU Generation Company LP (TXU Power) on Draft Regulatory Guide DG-1130, "Criteria For Use of Computers in Safety Systems of Nuclear Power Plants."

Attachment 1 provides both general and specific comments. Attachment 2 is a revised version of the draft regulatory guide to show how the specific comments can be incorporated.

TXU Power appreciates the opportunity to comment on the draft regulatory guide. If there are any questions regarding these comments, please contact Carl B. Corbin at 254-897-0121 or ccorbin1@txu.com.

E-RIDS=ADM-03

SISP Review Complete

Template = ADM-013

Call = S. Aggarwal (SKA)

Sincerely,

TXU Generation Company LP

By: TXU Generation Management Company LLC
Its General Partner

Mike Blevins

By:
Fred W. Madden
Director, Regulatory Affairs

CBC
Attachments

c - B. S. Mallett, Region IV
M. C. Thadani, NRR
Resident Inspectors, CPSES

Comments on Draft Regulatory Guide DG-1130, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants."

General comments:

1. Security applies to hardware and software. This DG focuses mainly on software. Security attributes for hardware need to be addressed (physical access control, modems, connectivity to external networks, data-links, open ports, etc.).

2. Section 2.4.2 "...scanning to ensure against undocumented codes or malicious codes..." – This is likely to 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.

3. Section 2.4.2 "System Software" – This is likely to be proprietary and generally unavailable. It is likely that there is no reliable method to determine this for Operating System Software (i.e., 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 software is modified by the application developer, the security effort should be limited to ensuring that the features within the software do not compromise the security requirements of the system.

4. Section 2.5.2 "Test Phase" –Based on experience, about 99% of this phase for security aspects of the system consists of checking that the designed security features are correctly configured and enabled (i.e., the security design elements have been put in place). The testing of specific security code/features is likely to be unfeasible for many if not most of the security items/functions.

   For instance, setting up the adverse conditions to perform testing might require a "hacker's software toolbox" and expert hacker's knowledge to produce the environment necessary to perform the test.

   Example test requirement: "Verify that the anti-virus software detects and eliminates viruses". Testing for this type of requirement may be undesirable as the testing itself could expose and potentially "infect" or alter the system.

   Requirements should verify that proper anti-virus software has been installed.

5. DG-1130 is based on a life cycle approach. Other approaches, including risk-based approaches are available to address Cyber Security and they should be addressed.

6. NRREG-6847 and NEI-04-04 describe a cyber security assessment methodology which should be used to evaluate the proposed system's cyber security risk/vulnerabilities. The draft regulatory guide should recognize and address this NUREG.

Specific comments:

No.	Location	Comment	Recommendation	
1	B. Discussion 6th paragraph	Clarify the purpose with respect to digital upgrades.	Insert the following at the end of the paragraph: It is to be noted that the requirements specified in sections 2.1 thru 2.9 of this DG are required to be addressed for Plant Safety Related Systems as required by IEEE 7-4.3.2 and IEEE 603. The purpose of this regulatory guide is to provide the staff's position on each attribute due to lack of specificity in the current standards when dealing with newer technologies which have different failure modes and effects, and different configuration control methods than those implemented in present day Nuclear Power Plants.	
2	B. Discussion 7th paragraph 4th sentence	Expand discussion to address both "safety" and "important to safety" digital systems.	Replace sentences with the following: Controls should address access via network connections and via maintenance equipment. Additionally, the design of the plant data communication systems should ensure that the integrity of the safety related digital systems and important to safety digital systems is maintained. These systems should not present an electronic path by which unauthorized personnel can change plant software or display erroneous plant status information to the operators.	

3	B. Discussion 8th paragraph Last sentence	Expand discussion to include station administrative procedures.	Replace sentence with sentence below: The security of computer-based systems is established through (1) designing the security features that will meet user 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 users' security program.	
4	C.2. Security 3rd paragraph	Change the focus from quality assurance program to configuration management.	Replace sentence with sentence below: The user should consider establishing a security program that addresses security configuration management as part of its security program. The security program can be incorporated into the existing quality assurance and configuration management programs.	
5	C.2.1 Concepts Phase 3rd paragraph	Expand discussion to address both "safety" and "important to safety" systems. Add a sentence regarding analyzing direct and indirect conductivity.	Replace paragraph with revise paragraph below: Remote access to the safety systems and important to safety systems from outside the technical environment of the plant (e.g., from the administrative or engineering buildings or from outside the plant) that involves a potential security threat to safety functions should not be implemented. Any such direct or indirect connectivity should be analyzed	
6	C.2.2.1 System Features 1st paragraph	Add system configuration as another item to be defined by system users and developers.	Add "; system configuration" after the words "performance requirements" in the first sentence.	
7	C.2.3.1 System Features 1st paragraph	Expand paragraph to address hardware as well as software.	Add "hardware and" before the word "software" in both locations.	
8	C.2.3.1 System Features 3rd paragraph	Clarify access to explicitly include both physical and logical access.	Add "Physical and logical" at the beginning of the sentence.	

9	C.2.3.1 System Features 2nd paragraph and at the end	Add a discussion concerning hardware and split the section into part "a" and "b" for clarity.	Add "a. " before the second paragraph. Add the following new paragraph at the end of the section: b. The safety system hardware design should consider system architecture that includes external connectivity, user interface, maintenance interface, development systems and interfaces, networking architectures (if applicable), built-in communication devices, data-link requirements, data communications requirements, etc.	
10	C.2.4 Implementation Phase	Expand the section to include integrated hardware and software implementation as well as hardware and communication configuration.	Replace paragraph with paragraph below: 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 set-up, software coding and testing, communication configuration and set-up including the incorporation of reused software products.	
11	C.2.4 Implementation Phase	Organize the subsection in a clearer manner.	Start Subsection 2.4.1, System Features, after the first paragraph to include only one paragraph (The developer should ensure that the security design configuration item transformations from the system design specification are correct, accurate, and complete.). Start Subsection 2.4.2, Development Activities, immediately after that.	
12	New section C.2.4.2 Development Activities 1st paragraph 2nd sentence	Scanning is not always meaningful.	Add the words, "where appropriate" after the word "scanning" in the second sentence.	

13	New section C.2.4.2 Development Activities 1st paragraph 3rd sentence	Expand the thought to require that all hidden functions be addressed by a failure modes and affects analysis.	Replace the sentence with the following: The developer should account for any and all hidden functions embedded in the code, it's purpose and impact on the client system. If possible, these functions should be disabled or removed, or as a minimum, they need to be addressed as part of the failure modes and affects analysis of the application code to prevent any unauthorized access.	
14	C.2.5 Test Phase	Need to address System Level Testing for integrated hardware and software and then lead into specifics on software testing. This model is ignoring the hardware configuration aspects of security which are going to be the major reasons for intrusion stemming from modems, open ports, unknown and unanalyzed network connectivity to IT LAN, etc.	Add a thought similar to the paragraph below at the beginning of the section: Need to address System Level Testing for integrated hardware and software and then lead into specifics on software testing. This model is ignoring the hardware configuration aspects of security which are going to be the major reasons for intrusion stemming from modems, open ports, unknown and unanalyzed network connectivity to IT LAN, etc. Revise the current paragraph to read: The objective of testing software security functions is to ensure that the software security requirements and system security requirements allocated to software are validated by execution of integration, system, and acceptance tests where practical and necessary. Testing includes system hardware configuration including all external connectivity, software testing, software integration testing, software qualification testing, system integration testing, and system qualification testing, and system Factory Acceptance Testing.	

15	C.2.5.2 Development Activities	Add testing for potential compromise of system integrity.	Add the following paragraph at the end: The developer should perform testing to ensure that the system hardware architecture and external communication devices and configurations are such that they do not provide unauthorized unknown pathways and compromise system integrity. Attention needs to focus on built-in OEM features	
16	C.2.6 Installation and Checkout Phase		Change title to "Site Installation, Checkout and Acceptance Testing Phase."	
17	C.2.6 Installation and Checkout Phase 1st paragraph 2nd sentence	Clarify that the review and test includes physical and logical features.	Add the words "physical and logical" between the words "safety" and "security" in the second sentence.	
18	C.2.6.2 Development Activities	Clarification	Delete the word "comprehensive" in the first sentence and "standards," in the second.	
19	C.2.7 Operation Phase 2nd paragraph	Clarify to note that real time monitoring may not always be possible and to expand the audit scope.	Revise the paragraph to read as noted below: The user should monitor and record access and use of the system to ensure that its digital system security policies are implemented properly. The monitoring should include real-time monitoring where possible and/or periodic audits. The type of monitoring is determined by the risk analyses performed in earlier lifecycle phases. The audit should include the security of any equipment that has direct external digital connectivity such as LAN, modem, data-links, maintenance equipment, user interfaces, etc.	
20	C.2.8.3 Incident Response	Tie plan to station programs.	Add the following sentence at the end of the section: The plan should be incorporated into the existing station programs.	

21	C.2.8.4 Audits and Assessments	Clarify to address modifications explicitly.	Revise the paragraph to read as noted below: The user should perform periodic computer system security self-assessments and audits, which are key components of a good security program. The user should assess proposed safety system changes and their impact on safety system security; evaluate anomalies that are discovered during operation; assess migration requirements; assess modifications made including V&V tasks to ensure that vulnerabilities have not been introduced into the plant environment from modifications.	
22	Regulatory Analysis 3. Technical Approach	Editorial	Insert the section number and title before the paragraph which starts, "Issuing a regulatory guide is ...."	

U.S. NUCLEAR REGULATORY COMMISSION
OFFICE OF NUCLEAR REGULATORY RESEARCH

December 2004
Division 1

DRAFT REGULATORY GUIDE

Contact: Satish K. Aggarwal, (301) 415-6005

DRAFT REGULATORY GUIDE DG-1130

(Proposed Revision 2 of Regulatory Guide 1.152)

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

General Comments:

1. Security applies to hardware and software. This DG focuses mainly on software and as such security attributes for hardware need to be addressed (physical access control, modems, connectivity to external networks, data-links, open ports, etc.)

2. Section 2.4.2"...scanning to ensure against undocumented codes or malicious codes..." – This is likely to 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, 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.

3. Section 2.4.2 "System Software" – This is likely to be proprietary and generally unavailable. It is likely that there is no reliable method to determine this for Operating System Software (i.e. 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 software is modified by the application developer, the security effort should be limited to ensuring that the features within the software do not compromise the security requirements that are required by the system.

4. Section 2.5.2"Test Phase" –Based on experience, about 99% of this phase for security aspects of the system results in checking that designed security features are correctly configured and enabled (i.e. the security design elements have been put in place). The testing of specific security code/features is likely to be unfeasible for many if not most of the security items/functions.

For instance; setting up the adverse conditions to perform testing might require a "hacker's software toolbox" and expert hacker knowledge to produce the environment necessary to perform the test.

Example test requirement: "Verify that the anti-virus software detects and eliminates viruses". Testing for this type of requirement may be undesirable as the testing itself could expose and potentially "infect" or alter the system.

Requirements should verify that proper anti-virus software has been installed.

5. DG-1130 is based on a life cycle approach. Other approaches, including risk-based approaches are available to address Cyber Security and they should be addressed.

6. NRREG-6847 and NEI-04-04 describe a cyber security assessment methodology which should be used to evaluate the proposed system's cyber security risk/vulnerabilities. The draft regulatory guide should recognize and address this NUREG.

A. INTRODUCTION

This regulatory guide describes a method that the staff of the U.S. Nuclear Regulatory Commission (NRC) deems acceptable for complying with the NRC's regulations for promoting high functional reliability and design quality for the use of computers[1] in safety systems of nuclear plants. Specifically, 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 also contains the staff's regulatory position on the "Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations,"[2] which the Nuclear Power Engineering Committee of the Institute of Electrical and Electronics Engineers (IEEE) has promulgated as IEEE Std 7-4.3.2-2003. The NRC staff has collaborated in the development of IEEE Std 7-4.3.2-2003 to ensure that the guidance provided by the consensus standard is consistent with the

[1] For the purposes of this regulatory guide, the term "computer" means a system that includes computer hardware, software, firmware, and interfaces.

[2] IEEE publications may be purchased from the IEEE Service Center, 445 Hoes Lane, Piscataway, NJ 08854.

NRC's regulations. 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."

Regulatory guides are issued to describe to the public methods that the NRC 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 regulatory guides is not required. Regulatory guides are issued in draft form to solicit public comment and involve the public in developing the agency's regulatory positions. Draft regulatory guides have not received complete staff review; therefore, they do not represent official NRC staff positions.

This draft 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

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 non-safety 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 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 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 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. Annex C to this standard provides useful information on providing confidence that an existing commercial computer is of sufficiently high quality and reliability to be used in a safety system.

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 draft regulatory guide to include Regulatory Positions 2.1 – 2.9, which provide specific guidance concerning computer-based (cyber) safety system security. It is to be noted that the requirements specified in sections 2.1 thru 2.9 of this DG are required to be addressed for Plant Safety Related Systems as required by IEEE 7-4.3.2 and IEEE 603. The purpose of this regulatory guide is to provide the staff's position on each attribute due to lack of specificity in the current standards when dealing with newer technologies which have different failure modes and effects, and different configuration control methods than those implemented in present day Nuclear Power Plants.

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 system software and data should be provided to prevent changes by unauthorized personnel. Controls should address access via network connections and via maintenance equipment. Additionally, the design of the plant data communication systems should ensure that the integrity of the safety related digital systems and important to safety digital systems is maintained. These systems should not present an electronic path by which unauthorized personnel can change plant software or display erroneous plant status information to the operators. Annex E to IEEE Std 7-4.3.2-2003 provides useful information for establishing communication independence of plant equipment and systems.

Computer-based systems must be secure from electronic vulnerabilities, as well as from physical vulnerabilities, which have been well addressed. 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 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 user 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 users' security program.

Regulatory Positions 2.1 – 2.9 (presented in Section C of this draft regulatory guide) provide specific guidance concerning safety system security. The effectiveness of the security functions implemented in the software safety system should be confirmed during verification and validation (V&V) and in the configuration management of the safety system software in each lifecycle phase.

In addition to the aspects discussed in Section C of this draft regulatory guide, 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. Guidance is provided in Branch Technical Position HICB-14, "Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems."
(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 users to obtain further information regarding specific areas of the standard.

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, with the exception that the use of barriers, as proposed in Clause 5.6(a) of IEEE Std 7-4.3.2, is not acceptable to the NRC, as a means of ensuring independence between safety functions and nonsafety functions on the same computer. However, Clause 5.6(b) of IEEE Std 7-4.3.2 requires that, in the absence of using barriers, all software on a safety-related computer must be developed in accordance with IEEE Std 7-4.3.2-2003 and IEEE Std 603. This approach is acceptable to the NRC for meeting its existing regulatory requirements for addressing independence between safety software and nonsafety software residing on the same computer.

2. Security

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

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

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

The user should consider establishing a security program that addresses security configuration management as part of its security program. The security program can be incorporated into the existing quality assurance and configuration management programs.

The Quality Assurance organization should conduct periodic audits to determine the effectiveness of the digital safety system security program.

Regulatory positions 2.1 – 2.9 describe digital safety system security activities and recommendations for the individual phases of the waterfall lifecycle.

2.1 Concepts Phase

In the concepts phase, the user and developer should delineate safety system security features that should be implemented to meet the desired system security capabilities. During this activity, the system architecture is selected and the desired safety system security functional capabilities are allocated to hardware, software, and user interface components.

The user and developer should perform security risk analyses to identify potential security vulnerabilities in the relevant phases of the system and software 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 systems and important to safety systems from outside the technical environment of the plant (e.g., from the administrative or engineering buildings or from outside the plant) that involves a potential security threat to safety functions should not be implemented. Any such direct or indirect connectivity should be analyzed.

2.2 Requirements Phase

2.2.1 *System Features*

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

The security requirements are 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 software and hardware system requirements, which include security requirements.

Requirements specifying the use of pre-developed software (e.g., reuse software and commercial off-the-shelf software) should minimize the vulnerability of the safety system (e.g., by minimizing the number of pre-developed software functions used by the safety system to the extent necessary or using existing security functions of the pre-developed software).

2.2.2 *Development Activities*

The developer should delineate its security policies to ensure the developed 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 and undocumented functions or applications.

2.3 Design Phase

2.3.1 *System Features*

The safety system (hardware & software) security requirements identified in the system requirements specification should be translated into specific design configuration items in the hardware and software design description

a. The safety system software security design configuration items should address control over (1) access to the software functions, (2) use of safety system services, (3) data communication with other systems, and (4) the list of personnel who may access and use the system

Design configuration items incorporating pre-developed software into the safety system should be specified such that vulnerability of the safety system security is minimized.

Physical and logical access control should be based on the results of risk analyses. The results of the analyses may require more complex access control, such as a comination of knowledge (e.g., password, property (e.g., key, smart-card) and personal features (e.g., fingerprints), rather than just a password.

b. The safety system hardware design should consider system architecture that includes external connectivity, user interface, maintenance interface, development systems and interfaces, networking architectures (if applicable), built-in communication devices, data-link requirements, data communications requirements, etc.

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 set-up, software coding and testing, communication configuration and set-up including the incorporation of reused software 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 ensure against tampering with the developed software. The developer's standards and procedures should include testing, including scanning where appropriate, to ensure against undocumented codes or malicious codes 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 any and all hidden functions embedded in the code, it's purpose and impact on the client system. If possible, these functions should be disabled or removed, or as a minimum, they need to be addressed as part of the failure modes and affects analysis of the application code to prevent any unauthorized access. If provisions cannot be implemented for pre-developed software, the use of such software should be justified considering potential security threats.

The user and developer should review the possibility for deliberate modification of software to cause erroneous behavior of the software triggered by certain time or data constraints (e.g., viruses, worms, and Trojan horses).

2.5 Test Phase

Need to address System Level Testing for integrated hardware and software and then lead into specifics on software testing. This model is ignoring the hardware configuration aspects of security which are going to be the major reasons for intrusion stemming from modems, open ports, unknown and unanalyzed network connectivity to IT LAN, etc.

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

2.5.1 *System Features*

The security requirements and configuration items are part of the overall system requirements and design configuration items. Therefore, testing security design configuration items is just one element of the overall system testing. The user and developer should test each system security feature to verify that the implemented system does not increase the risk of security vulnerabilities.

2.5.2 *Development Activities*

The developer should perform testing and scanning to ensure the developed products (i.e., 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 and undocumented functions or applications. Additionally, the developer should audit the configuration management processes to ensure that the software is developed in accordance with the appropriate configuration management procedures and standards.

The developer should perform testing to ensure that the system hardware architecture and external communication devices and configurations are such that they do not provide unauthorized unknown pathways and compromise system integrity. Attention needs to focus on built-in Original Equipment Manufacturer (OEM) features.

2.6 Site Installation, Checkout and Acceptance Testing Phase

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

2.6.1 *System Features*

The user should ensure that the system features enable the user 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 user or licensee should have a digital system security program. The security policies, 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 user to perform a security assessment, which includes a risk assessment, to identify the potential security vulnerabilities caused by installation 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 end user in its intended operational environment.

The user should monitor and record access and use of the system to ensure that its digital system security policies are implemented properly. The monitoring should include real-time monitoring where possible and/or periodic audits. The type of monitoring is determined by the risk analyses performed in earlier lifecycle phases. The audit should include the security of any equipment that has direct external digital connectivity such as LAN, modem, data-links, maintenance equipment, user interfaces, etc.

The user 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 user and the system. The user 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 user 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 software to a new operational environment)
- Retirement (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 user 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 software, the user should verify that the migrated software meets 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*

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 user 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.

The user should establish a security configuration management program as part of its security program. The security configuration program may be incorporated into the existing configuration management program.

2.8.3 *Incident Response*

The user 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. The plan should be incorporated into the existing station programs.

2.8.4 *Audits and Assessments*

The user should perform periodic computer system security self-assessments and audits, which are key components of a good security program. The user should assess proposed safety system changes and their impact on safety system security; evaluate anomalies that are discovered during operation; assess migration requirements; 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 user should assess the effect of replacing or removing the existing safety system security functions from the operating environment. The user should include in the scope of this assessment the effect on safety and non-safety system interfaces of removing the system security functions. The user 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 user interactions, or retirement of the safety system interfacing functions).

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 draft regulatory guide. No backfitting is intended or approved in connection with the issuance of this guide.

The NRC has issued this draft guide to encourage public participation in its development. Except when 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 the active guide will reflect public comments and will be used in evaluating (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 that have a clear nexus with this guidance.

REGULATORY ANALYSIS

Background

With the introduction of computers in safety systems, concerns have arisen over the possibility that the use of computer software could result in a common-mode failure. Because of these concerns, the NRC staff has placed significant emphasis on defense-in-depth against propagation of common-mode failures within and between functions. The two principal factors for defense against common-mode failures are quality and diversity. Each postulated common-mode failure should be analyzed using best-estimate methods to address vulnerabilities to common-mode failures. Design qualification and quality assurance programs are intended to provide protection against design deficiencies and manufacturing errors. The guidelines in IEEE Std 603-1998 and IEEE Std 7-4.3.2-2003 should be applied to the development of digital computer systems for purposes of developing high-quality hardware and software.

1. Problem

IEEE Std 7-4.3.2-1993 was endorsed by Revision 1 of Regulatory Guide 1.152 in January 1996. The development processes for computer systems continue to evolve. The revision of this standard (IEEE Std 7-4.3.2-2003) represents a continued effort by IEEE to support the specification, design, and implementation of computers in safety systems. The regulatory guide should, therefore, be revised to reflect the current state of the technology.

2. Objective

The objective of the regulatory action is to update NRC guidance for the use of computers in safety systems and to provide guidance on safety system security.

3. Technical Approach

Issuing a regulatory guide is consistent with the NRC policy of evaluating the latest versions of national consensus standards in terms of their suitability for endorsement by regulatory guides. This regulatory guide endorses the guidance of IEEE Std 7-4.3.2-2003 with a minor exception. As such, this guide provides a standardized approach so that the nuclear industry and the NRC staff may have a common understanding of the criteria for the use of computers in safety systems.

IEEE Std 7-4.3.2-2003 includes the following significant changes:

.(a) The "Software Quality Metrics" clause was added. The industry practice s moving toward the use of software quality metrics to assure, monitor, and improve software quality, in addition to the verification and validation (V&V) that has traditionally been applied.

.(b) The "Qualification of Existing Comme rcial Computers" clause was expanded to provide additional guidance that addresses the move toward the use of more commercial hardware and software in safety systems.
.(c) The "Software Tools" clause was revi sed to address expanded use of software tools and methods.
.(d) The "Verification and Validation" clause was revised to reference IEEE Std 10121998.
.(e) The "Software Configuration M anagement" clause was expanded to provide additional guidance by identifying the key requirements for configuration management for safety system software using the guidance in IEEE Std 828-1998 and IEEE Std 1042-1987.
.(f) A "Software Project Ri sk Management" clause was added to provide additional guidance consistent with IEEE Std 1540-2001 on risk management, and IEEE Std 12207.0-1996 on software lifecycle processes.
.(g) A "Fault Detection and Self-Diagnosti cs" clause was added to discuss features that are unique to software and computer systems.
.(h) The "Identification" clause was ex panded to include software-specific requirements by extending the IEEE Std 603-1998 identification requirements to software.
.(i) Annex C, "Dedication of Existing Commercial Computers," was updated to more completely address issues associated with commercial off-the-shelf software (COTS).
.(j) Annex D, "Identificati on and Resolution of Hazards," was revised to represent current practices and processes for hazards analysis.

In addition, the staff has provided guidance specific to computer-based (cyber) safety system security.

4. Conclusion

The NRC should revise Regulatory Guide 1.152, since this action should enhance the licensing process. The staff has concluded that the proposed action will reduce unnecessary burden on both the NRC and its licensees, and it will result in an improved process for the use of computers in safety systems. Furthermore, the staff sees no adverse effects associated with revising Regulatory Guide 1.152. Use of this revision by the licensees of currently operating nuclear power plants is entirely optional and voluntary.

BACKFIT ANALYSIS

As described in 10 CFR 50.109(c), this draft revision of Regulatory Guide 1.152 does not require a backfit analysis because the use of this revision by the licensees of currently operating nuclear power plants is entirely voluntary.