NUREG-0800

U.S. NUCLEAR REGULATORY COMMISSION

STANDARD REVIEW PLAN

APPENDIX 7.1-D

GUIDANCE FOR EVALUATION OF THE APPLICATION OF IEEE STD 7-4.3.2

REVIEW RESPONSIBILITIES

Primary - Organization responsible for the review of instrumentation and controls

Secondary - None

1. AREAS OF REVIEW

For nuclear power plants with construction permits issued before January 1, 1971, 10 CFR 50.55a(h) requires that protection systems must be consistent with their licensing basis or may meet the requirements of IEEE Std 603-1991, “IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations,” and the correction sheet dated January 30, 1995. For nuclear power plants with construction permits issued after January 1, 1971, but before May 13, 1999, 10 CFR 50.55a(h) requires that protection systems must meet the requirements stated in either IEEE Std 279-1971, “Criteria for Protection Systems for Nuclear Power Generating Stations,” or IEEE Std 603-1991 and the correction sheet dated January 30, 1995. Applications filed on or after May 13, 1999 for preliminary and final design approvals (10 CFR Part 52, Appendix O), design certification, and construction permits, operating licenses and combined licenses that do not reference a final design approval or design certification, must meet the requirements for safety systems in IEEE Std 603-1991 and the correction sheet dated January 30, 1995.

March 2007

USNRC STANDARD REVIEW PLAN

This Standard Review Plan, NUREG-0800, has been prepared to establish criteria that the U.S. Nuclear Regulatory Commission staff responsible for the review of applications to construct and operate nuclear power plants intends to use in evaluating whether an applicant/licensee meets the NRC's regulations. The Standard Review Plan is not a substitute for the NRC's regulations, and compliance with it is not required. However, an applicant is required to identify differences between the design features, analytical techniques, and procedural measures proposed for its facility and the SRP acceptance criteria and evaluate how the proposed alternatives to the SRP acceptance criteria provide an acceptable method of complying with the NRC regulations.

The standard review plan sections are numbered in accordance with corresponding sections in Regulatory Guide 1.70, "Standard Format and Content of Safety Analysis Reports for Nuclear Power Plants (LWR Edition)." Not all sections of Regulatory Guide 1.70 have a corresponding review plan section. The SRP sections applicable to a combined license application for a new light-water reactor (LWR) are based on Regulatory Guide 1.206, "Combined License Applications for Nuclear Power Plants (LWR Edition)."

These documents are made available to the public as part of the NRC's policy to inform the nuclear industry and the general public of regulatory procedures and policies. Individual sections of NUREG-0800 will be revised periodically, as appropriate, to accommodate comments and to reflect new information and experience. Comments may be submitted electronically by email to NRR_SRP@nrc.gov.

Requests for single copies of SRP sections (which may be reproduced) should be made to the U.S. Nuclear Regulatory Commission, Washington, DC 20555, Attention: Reproduction and Distribution Services Section, or by fax to (301) 415-2289; or by email to DISTRIBUTION@nrc.gov. Electronic copies of this section are available through the NRC's public Web site at http://www.nrc.gov/reading-rm/doc-collections/nuregs/staff/sr0800/, or in the NRC's Agencywide Documents Access and Management System (ADAMS), at http://www.nrc.gov/reading-rm/adams.html, under Accession # ML070660327.

IEEE Std 603-1991 does not directly discuss digital systems, but states that guidance on the application of the criteria in IEEE Std 603-1991 for safety systems using digital programmable computers is provided in IEEE/ANS 7-4.3.2-1982, “American Nuclear Society and IEEE Standard Application Criteria for Programmable Digital Computer Systems in Safety Systems of Nuclear Power Generating Stations.” IEEE/ANS 7-4.3.2-1982 has been revised into IEEE Std 7-4.3.2-2003, “IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations.” Guidance on applying the safety system criteria to computer-based safety systems is provided by IEEE Std 7-4.3.2-2003, as endorsed by Regulatory Guide 1.152, Revision 2, “Criteria for Use of Computers in Safety Systems of Nuclear Power Plants.” IEEE Std 7-4.3.2-2003 specifies computer-specific criteria (incorporating hardware, software, firmware, and interfaces) to supplement the criteria in IEEE Std 603-1998. Although IEEE Std 7-4.3.2-2003 references IEEE Std 603-1998, IEEE Std 603-1991 and the correction sheet dated January 30, 1995 remains the requirement for safety systems in accordance with 10 CFR 50.55a(h).

If a referenced industry code or standard has been separately incorporated into NRC’s regulations, licensees and applicants must comply with that code or standard as set forth in the regulations. If the referenced code or standard has been endorsed by the NRC staff in a regulatory guide, that code or standard constitutes an acceptable method of meeting the related regulatory requirement as described in the regulatory guide. By contrast, if a referenced code or standard has neither been incorporated into the NRC’s regulations nor been endorsed by a regulatory guide, licensees and applicants may consider and use the information in the referenced code or standard, if appropriately justified, consistent with current regulatory practice.

IEEE Std 603-1998, was evolved from IEEE Std 603-1991. The 1998 version of IEEE Std 603, was revised to clarify the application of the standard to computer-based safety systems and to advanced nuclear power generating station designs. IEEE 603-1998 provides criteria for the treatment of electromagnetic and radio frequency interferences (EMI/RFI) and includes common-cause failure of digital computers in the single failure criterion. However, IEEE Std 603-1998 has neither been incorporated into the regulations nor endorsed by a regulatory guide. Therefore, the use of criteria from IEEE Std 603-1998 by licensees and applicants may be acceptable, if appropriately justified, consistent with current regulatory practice.

Annex A of IEEE Std 7-4.3.2-2003, “Mapping of IEEE Std 603-1998 to IEEE Std 7-4.3.2-2003,” provides more information about the relationship of IEEE Std 7-4.3.2-2003 to IEEE Std 603-1998.

Standard Review Plan (SRP) Appendix 7.1-C contains guidance on the application of the requirements of IEEE Std 603-1991.

SRP Appendix 7.1-B contains guidance on the application of the requirements of IEEE Std 279-1971.

2. SCOPE

The scope of IEEE Std 7-4.3.2-2003 and Regulatory Guide 1.152, Revision 2 includes all safety instrumentation and control (I&C) systems that are computer-based. IEEE Std 7-4.3.2-2003 serves to amplify criteria in IEEE Std 603-1991 to address the use of computers as part of safety systems in nuclear power generating stations, systems covered by Sections 7.2 through

7.6 of the plant safety analysis report (SAR). Although NRC did not endorse the annexes of IEEE Std 7-4.3.2-2003 in Regulatory Guide 1.152, Revision 2, subsections in this SRP appendix address guidance from some the annexes. The criteria contained in IEEE Std 7-4.3.2-2003, in conjunction with requirements in IEEE Std 603-1991, establish minimum functional and design criteria for computers used as components of a safety system. Although intended for digital safety systems, the criteria of IEEE Std 7-4.3.2-2003 can be applied to any digital I&C system. For non-safety digital I&C systems covered by SAR Sections 7.7 and 7.8, which are systems that have a high degree of importance-to-safety based on risk, graded application of the criteria of IEEE Std 7-4.3.2-2003 could be considered by the reviewer. Data communication systems covered by SAR Section 7.9 are support systems to I&C systems. Hence, the criteria and guidance for the communication systems are the same as those for the principal I&C systems they support.

The coordination review needed for each I&C system is discussed in SRP Section 7.0.

3. DEFINITIONS, ABBREVIATIONS, AND REFERENCES

This SRP appendix does not provide any additional definitions or abbreviations to those that appear in IEEE Std 7-4.3.2-2003.

In addition to the references listed in IEEE Std 7-4.3.2-2003, NRC staff should be familiar with national and international standards, regulatory guides, SRP branch technical positions (BTPs) and other guidance relevant to the topics under review that are identified in the discussion of the review topics below.

4. SAFETY SYSTEM DESIGN BASIS (IEEE Std 7-4.3.2-2003 Clause 4)

Clause 4 of IEEE Std 603-1991 requires that the specific bases established for the design of each safety system are reviewed to determine whether they are consistent with the requirements of Clause 4 of IEEE Std 603-1991. Section 4 of SRP Appendix 7.1-C provides review guidance.

5. SAFETY SYSTEM CRITERIA (IEEE Std 7-4.3.2-2003 Clause 5)

Clause 5 of IEEE Std 603-1991 requires that safety systems shall, with precision and reliability, maintain plant parameters within acceptable limits established for each design basis event. The following subsections address the criteria in the order they are listed in IEEE Std 7-4.3.2-2003. For some criteria there are no additional criteria beyond what is stated in IEEE Std 603-1991 and the appropriate subsection of SRP Appendix 7.1-C is referenced.

5.1. Single-Failure Criterion (IEEE Std 7-4.3.2-2003 Clause 5.1)

The requirements are in IEEE Std 603-1991. Subsection 5.1 of SRP Appendix 7.1-C provides additional guidance. Clause 5.1 in IEEE Std 603-1991 defines the single-failure criterion. Guidance for the application of this criterion is provided in IEEE Std 379-2000, “IEEE Standard Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems,” which is endorsed by Regulatory Guide 1.53, Revision 2, “Application of the Single-Failure Criterion to Safety.” The approach stated in Clause 5.5 of IEEE Std 379-2000 is also appropriate for potential common-cause failures associated with computer hardware and software that have been developed under the criteria of IEEE Std 603-1991 and IEEE STD 7-4.3.2-2003.

SRP Appendix 7.1-C discusses certain concerns of digital computer-based systems; for example, a design using shared databases and process equipment has the potential to propagate a common-cause failure of redundant equipment and software programming errors can defeat the redundancy achieved by the hardware architectural structure. Because of these concerns, the NRC staff has placed significant emphasis on defense-in-depth against common-cause failures within and between functions. SRP BTP 7-19 provides guidance for evaluating diversity and defense-in-depth features. SRP BTP 7-19 has the following objectives: (1) To verify that adequate diversity has been provided in the design of the digital system to meet the criteria established by NRC requirements, (2) To verify that adequate defense-in-depth has been provided to meet NRC criteria, and (3) To verify that the displays and manual controls for critical safety functions initiated by operator actions are diverse from the computer systems used in the automatic actuation of plant safety systems.

5.2. Completion of Protective Action (IEEE Std 7-4.3.2-2003 Clause 5.2)

The reviewer should refer to Subsection 5.2 of SRP Appendix 7.1-C for guidance on the implementation of the requirements of IEEE Std 603-1991.

5.3. Quality (IEEE Std 7-4.3.2-2003 Clause 5.3)

The applicant/licensee should confirm that quality assurance provisions of Appendix B to 10 CFR Part 50 are applied to the safety system. The evaluation of the adequacy of the quality assurance program is addressed in the review of Chapter 17 of the SAR.

For digital computer-based systems, the applicant/licensee should address the quality criteria described in Clause 5.3 of IEEE Std 7-4.3.2-2003. Hardware quality is addressed in IEEE Std 603-1991. Software quality is addressed in IEEE/EIA Std 12207.0-1996 and supporting standards. In addition to the requirements of IEEE Std 603-1991, the following activities necessitate additional criteria that are applicable to the quality criterion. The criteria are provided in the following clauses of IEEE Std 7-4.3.2-2003:

5.3.1	Software development
5.3.2	Software tools
5.3.3, 5.3.4	Verification and validation, Independent verification and validation requirements
5.3.5	Software configuration management
5.3.6	Software project risk management

EPRI Topical Report TR-106439, “Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications,” as accepted by the NRC safety evaluation dated July 17, 1997, and EPRI TR-107330, “Generic Requirements Specification for Qualifying a Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants, as accepted by the NRC safety evaluation dated July 30, 1998 provide guidance for the evaluation of existing commercial computers and software to comply with the criteria of

Clause 5.3.2 of IEEE Std 7-4.3.2-2003. The guidance of SRP BTP 7-14 may be applied to the evaluation of vendor processes described in EPRI Topical Report TR-106439.

The Software tools clause was revised to address expanded use of software tools and methods to confirm suitability. IEC 60880-2-2002, "Software for Computers Important to Safety for Nuclear Power Plants - Part 2, Software Aspects of Defense Against Common Cause Failures, Use of Software Tools and of Pre-developed Software," specifically addresses the use of software tools. If, however, it can not be demonstrated that defects not detected by software tools or introduced by software tool will be detected by verification and validation (V&V) activities, the software tool should be designed as safety related software itself, with all the attendant regulatory requirements for safety software.

IEEE Std 7-4.3.2 Clause 5.3.2 recommends that Software tools used to support software development processes and V&V processes should be controlled under configuration management; and that one or both of the following methods should be used to confirm the software tools are suitable for use:

a) A test tool validation program should be developed to provide confidence that the necessary features of the software tool function as required.

b) The software tool should be used in a manner such that defects not detected by the software tool will be detected by V&V activities.

In addition to the criteria of IEEE Std 603-1991 and IEEE Std 7-4.3.2-2003, SRP BTP 7-14 directs the reviewer to specific features of software development that should be reviewed. SRP BTP 7-14 has three objectives:

- To confirm that plans exist that will provide a high-quality software life cycle process, and that these plans commit to documentation of life cycle activities that permit the NRC staff to evaluate the quality of the design features upon which the safety determination is based.

- To verify that implementation of the software life cycle process meets the criteria expected for high-quality software.

- To assess the adequacy of the design outputs.

All software development life cycles share certain characteristics. The activities that will be performed can be grouped into a number of categories (termed activity groups in SRP BTP 7-14); the activity groups are common to all life cycles. Life cycle activities produce process documents and design outputs which can be reviewed and assessed. The documents to be provided for each life cycle activity group are shown in Figure 7-A-1 of SRP BTP 7-14. The information to be reviewed is subdivided into three topic areas: software life cycle process planning; software life cycle process implementation; and software life cycle development process outputs. The applicant/licensee need not develop a separate document for each of the topics identified below; however, project documentation should encompass all of the topics. The information documents in the three areas are as follows:

(i) Software Life Cycle Process Planning
Software management plan (including software engineering measures)
Software development plan

Software quality assurance plan
Integration plan
Test plan
Installation plan
Maintenance plan
Training plan
Operations plan
Software safety plan
Software verification and validation plan
Software configuration management plan.

(ii) Software Life Cycle Process Implementation
Safety analyses
Verification and validation analysis and test reports
Configuration management reports.

One or more sets of these reports should be available for each of the following activity groups:
Software metrics data
Requirements
Design
Implementation
Integration
Validation and test procedures
Installation
Operations
Maintenance.

(iii) Software Life Cycle Development Process Outputs
Software requirements specifications
Hardware and software architecture descriptions
Software design specifications
Software metrics data
Code listings
Build documents
Test results
Installation configuration tables
Operations manuals
Maintenance manuals
Training manuals.

5.3.1 **Software Development** (IEEE Std 7-4.3.2-2003 Sub-Clause 5.3.1)

Computer system development activities should include the development of computer hardware and software. The integration of the computer hardware and software and the integration of the computer with the safety system should be addressed in the development process.

The computer system development process typically consists of the following computer lifecycle phases:

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

The activities during the lifecycle phases are summarized as:

- Creating the conceptual design of the system, translation of the concepts into specific system requirements
- Using the requirements to develop a detailed system design
- Implementing the design into hardware and software functions
- Testing the functions to assure the requirements have been correctly implemented
- Installing the system and performing site acceptance testing
- Operating and maintaining the system
- Retiring the system.

SRP BTP 7-14 describes the characteristics of a software development process that the NRC staff evaluates when assessing the quality criteria of the entire Clause 5.3 of IEEE Std 7-4.3.2-2003. Software characteristics can be divided into two sets: functional characteristics and software development process characteristics. The first set includes those characteristics that directly relate to the actions that the safety system software should take, while the second includes those characteristics of the software development process that contribute to assurance that the software will perform the required actions. Both sets are important in safety system software. The sets, and the definitions of the characteristics, are listed below.

Functional Characteristics:

- Accuracy — The degree of freedom from error of sensor and operator input, the degree of exactness exhibited by an approximation or measurement, and the degree of freedom from error of actuator output.

- Functionality — The operations which must be carried out by the software. Functions generally transform input information into output information in order to affect the reactor operation. Inputs may be obtained from sensors, operators, other equipment, or other software. Outputs may be directed to actuators, operators, other equipment, or other software.

- Reliability — The degree to which a software system or component operates without failure. This definition does not consider the consequences of failure, only the existence of failure.

- Robustness — The ability of a software system or component to function correctly in the presence of invalid inputs or stressful environmental conditions. This includes the ability to function correctly despite some violation of the assumptions in its specification.

- Safety — Those properties and characteristics of the software system that directly affect or interact with system safety considerations. The other characteristics discussed in SRP BTP 7-14 are important contributors to the overall safety of the software-controlled safety system, but are primarily concerned with the internal operation of the software. The safety characteristic, however, is primarily concerned with the effect of the software on system hazards and the measures taken to control those hazards.

- Security — The ability to prevent unauthorized, undesired, and unsafe intrusions. Regulatory Guide 1.152, Revision 2 provides specific guidance concerning computer-based (cyber) safety system security which is discussed in Subsection 9 of this appendix.

5.3.1.1 Software Quality Metrics (IEEE Std 7-4.3.2-2003 Sub-Clause 5.3.1.1)

Industry practice is moving towards the use of software quality metrics to assure/monitor/ improve software quality in addition to the V&V that has traditionally been applied. SRP BTP 7-14 has identified one of the characteristics to be considered during the implementation of the software lifecycle activities as “Measurement” - a set of indicators used to determine the success or failure of the activities and tasks defined in the planning document.

The use of software quality metrics should be considered throughout the software life cycle to assess whether software quality requirements are being met. When software quality metrics are used, the following life cycle phase characteristics should be considered:

- Correctness/Completeness (Requirements phase)
- Compliance with requirements (Design phase)
- Compliance with design (Implementation phase)
- Functional compliance with requirements (Test and Integration phase)
- On-site functional compliance with requirements (Installation and checkout phase)
- Performance history (Operation and Maintenance phase).

The basis for the metrics selected to evaluate software quality characteristics should be included in the software development documentation. IEEE Std 1061-1998, “IEEE Standard for a Software Quality Metrics Methodology,” discusses software quality metrics methodology and methods by which various metrics systems can be evaluated

Reviewers should be careful when reviewing the results of any software metric to evaluate what that metric actually measures, and what conclusion can be reached based on these measurements. The metric may, for example, be useful to the software vendor to show diminishing returns on continued testing, but unless the quality and thoroughness of the testing program is evaluated, it may not be sufficient to demonstrate that the software is of high quality. Quality becomes more visible through a well conceived and effectively implemented software metrics program. A metrics methodology using a diversity of software measures and that appropriately aggregates the measurement data could provide quantitative data giving staff insight into the rigor of the safety software development process and resulting quality of the life cycle outputs.

5.3.2 Software Tools (IEEE Std 7-4.3.2-2003 Sub-Clause 5.3.2)

Software tools used to support software development processes and V&V processes should be controlled under configuration management. One or both of the following methods should be used to confirm the software tools are suitable for use:

- A test tool validation program should be developed to provide confidence that the necessary features of the software tool function as required.

- The software tool should be used in a manner such that defects not detected by the software tool will be detected by V&V activities. If, however, it can not be proven that defects not detected by software tools or introduced by software tool will be detected by V&V activities, the software tool should be designed as Appendix B quality software itself, with all the attendant regulatory requirements for software developed under an Appendix B program.

Tool operating experience may be used to provide additional confidence in the suitability of a tool, particularly when evaluating the potential for undetected defects.

SRP BTP 7-14 states that the resource characteristics that the software development plan should exhibit include methods/tools and standards. Methods/tools requires a description of the software development methods, techniques and tools to be used. The approach to be followed for reusing software should be described. The plan should identify suitable facilities, tools and aids to facilitate the production, management and publication of appropriate and consistent documentation and for the development of the software. It should describe the software development environment, including software design aids, compilers, loaders, and subroutine libraries. The plan should require that tools be qualified with a degree of rigor and level of detail appropriate to the safety significance of the software which is to be developed using the tools. Methods, techniques and tools that produce results that cannot be verified to an acceptable degree or that are not compatible with safety requirements should be prohibited, unless analysis shows that the alternative would be less safe.

Reviewers should thoroughly evaluate tool usage. Tools used for software development may reduce or eliminate the ability for the vendor to evaluate the output of those tools, and therefore rely on the tool, or on subsequent testing to show the software will perform as intended. Testing alone can only show that those items tested for operate as intended, and can not be relied upon to show that no unintended functions exist, or that the software will function in conditions other that those specifically tested. The use of software tools should be evaluated in the overall context of the quality control and V&V process, and there should be a method of evaluating the output of the tool.

5.3.3 Verification and Validation (IEEE Std 7-4.3.2-2003 Sub-Clause 5.3.3)

V&V is an extension of the program management and systems engineering team activities. V&V is used to identify objective data and conclusions (i.e., proactive feedback) about digital system quality, performance, and development process compliance throughout the system life cycle. Feedback consists of anomaly reports, performance improvements, and quality improvements regarding the expected operating conditions across the full spectrum of the system and its interfaces.

V&V processes provide an objective assessment of software products and processes throughout the software life cycle. This assessment demonstrates whether the system requirements and software requirements (i.e., those allotted to software via software specifications) are correct, complete, accurate, consistent, and testable. At the concepts stage of the software and hardware life cycle, the system functional requirements should be communicated between the plant systems engineers, the control room operators, the maintenance staff, and the software and hardware designers and vendors. This interaction should continue through the entire life cycle of the computer system. These V&V processes are used to determine whether the development products of an activity conform to the requirements of that activity, and whether the system performs according to its intended use and user needs. This determination of suitability includes assessment, analysis, evaluation, review, inspection, and testing of products and processes. In general, a thorough V&V effort will take as much effort as the design effort, and require an equivalent level of expertise. Reviewers should be careful to assess the quality and quantity of the licensee or vendor V&V team to ensure an adequate V&V effort is available.

IEEE Std 7-4.3.2-2003 adopts the IEEE Std 1012-1998, "IEEE Std for Software Verification and Validation," terminology of process, activity and task, in which software V&V processes are subdivided into activities, which are further subdivided into tasks. The term V&V effort is used to reference this framework of V&V processes, activities, and tasks.

V&V processes should address the computer hardware and software, integration of the digital system components, and the interaction of the resulting computer system with the nuclear power plant.

The V&V activities and tasks should include system testing of the final integrated hardware, software, firm-ware, and interfaces.

The software V&V effort should be performed in accordance with IEEE Std 1012-1998 which is endorsed by NRC Regulatory Guide 1.168, Revision 1. The IEEE Std 1012-1998 V&V criteria for the highest integrity level (level 4) apply to systems developed using IEEE Std 7-4.3.2-2003.

5.3.4 <u>Independent V&V (IV&V) Requirements</u> (IEEE Std 7-4.3.2-2003 Sub-Clause 5.3.4)

The previous subsection addresses the V&V activities to be performed. This subsection defines the levels of independence required for the V&V effort. IV&V activities are defined by three parameters: technical independence, managerial independence, and financial independence.

The development activities and tests should be verified and validated by individuals or groups with appropriate technical competence, other than those who developed the original design.

Oversight of the IV&V effort should be vested in an organization separate from the development and program management organizations. The V&V effort should independently select:

- The segments of the software and system to be analyzed and tested,
- The V&V techniques, and
- The technical issues and problems upon which to act.

The V&V activities and tasks should include system testing of the final integrated hardware, software, firm-ware, and interfaces. The V&V effort should be allocated resources that are independent of the development resources.

The reviewer of the V&V effort should evaluate the overall effectiveness of the V&V process. Since the NRC staff can not perform a review of every requirement and every line of code, the staff relies on the V&V completeness and rigor of the V&V effort to provide reasonable assurance of high quality software development. With this in mind, the items the reviewer should check include, but are not limited to the following:

i. Is the V&V organization independent and given sufficient time and resources to avoid pressure to perform in a hurried or insufficient review? The reviewer should Interview the V&V personnel, and observe the relationship between the V&V staff and the design staff. There may be cases where the organizational relationship indicates there is independence, when in fact, the V&V personnel are subject to pressure to perform a rapid review and to show that the software product is of high quality when the level of effort or the quality of the effort does not justify that determination.

ii. Are the V&V personnel qualified to perform the task? The V&V personnel should be at least equally experienced and qualified as the design personnel.

iii. Is the V&V organization effective? If a thread audit of selected functions reveals errors that were not found by the V&V effort, the indication is that V&V may not be finding other errors as well. In addition to checking the outputs of the various design stages to verify that the output properly reflects the requirements, and validates that the outputs are designed so that the product will fulfill its intended use, the V&V effort should determine that the design outputs actually work. As an example, a filter may have been specified, and that filter properly designed and implemented. However, if the filter does not actually filter the required frequencies, or does not actually reduce or eliminate the noise it is intended to filter, the quality of the V&V effort is suspect.

iv. Are the V&V problem reports properly addressed, corrections made, and the resulting correction itself properly checked? There have been cases where a V&V problem report was not effectively resolved, or that the correction resulting from a V&V problem report was in itself in error, and the analysis for the correction was so limited that the new error was not found. The reviewer should check the problem reports carefully, and determine that each problem was addressed and that correction did, in fact, correct the problem without introducing new errors.

The review of the V&V is an important step in the determination of high quality software and a high quality design process, and as such, any concerns the reviewer has about the quality of the V&V effort should be resolved prior to acceptance of the digital system. If the reviewer identifies concerns with quality or effectiveness, those issues should be raised to NRC management to determine the next steps up to and including non-acceptance of the V&V effort of the digital system for use in a safety-related application at nuclear power plants.

5.3.5 Software Configuration Management (IEEE Std 7-4.3.2-2003 Sub-Clause 5.3.5)

Regulatory Guide 1.169, “Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants,” which endorses IEEE Std 828-1990, “IEEE

Standard for Software Configuration Management Plans," provides guidance for the development of software configuration management (CM) plans. Software configuration management should be performed in accordance with IEEE Std 1042-1987, "IEEE Guide to Software Configuration Management." SRP BTP 7-14 Subsection B.3.1 provides additional guidance on CM plans, and Subsection B.3.2 provides additional guidance on CM activities.

The minimum set of activities should address the following:

i. Identification and control of all software designs and code

ii. Identification and control of all software design functional data (e.g., data templates and data bases)

iii. Identification and control of all software design interfaces

iv. Control of all software design changes

v. Control of software documentation (user, operating, and maintenance documentation)

vi. Control of software vendor development activities for the supplied safety system software

vii. Control and retrieval of qualification information associated with software designs and code

viii. Software configuration audits

ix. Status accounting.

Some of these functions or documents may be performed or controlled by other quality assurance activities. In this case, the software configuration management plan should describe the division of responsibility.

A software baseline should be established at appropriate points in the software life cycle process to synchronize engineering and documentation activities. Approved changes that are created subsequent to a baseline should be added to the baseline.

The labeling of the software for configuration control should include unique identification of each configuration item, and revision and/or date time stamps for each configuration item. This labeling should be unambiguous, and clearly identify this particular product and version from all others.

Changes to the software/firmware should be formally documented and approved consistent with the software configuration management plan. The documentation should include the reason for the change, identification of the affected software/firmware, and the impact of the change on the system. Additionally, the documentation should include the plan for implementing the change in the system (e.g., immediately implementing the change, or scheduling the change for a future version).

There may be two different software configuration management programs to evaluate, that being used by the software vendor during the design process, and that used by the licencee after the software has been delivered and installed in the nuclear power plant. Both of these programs should be evaluated. Appendix B of 10 CFR Part 50, in Section I, “Organization”, states, “The applicant may delegate to others, such as contractors, agents, or consultants, the work of establishing and executing the quality assurance program, or any part thereof, but shall retain responsibility therefor.” The reviewer should determine if a vendor software configuration management program has been approved by the licensee, and if it fits into the licensee’s overall software configuration management program.

IEEE Std 828-1990 and IEEE Std 1042-1987, which are endorsed by Regulatory Guide 1.169, should provide acceptable guidance for a software configuration management system, but the use of these standards is not mandatory. If referenced by the licensee, the reviewer should make an independent determination that the software configuration management system as implemented is appropriate for safety-related software used in nuclear power plants. If the vendor or licensee is using methods other than that prescribed by IEEE Std 828-1990 and IEEE Std 1042-1987, the determination of adequacy will be more difficult. In this case, the reviewer should be familiar with the software configuration control objectives, and examine the methodology used by the vendor and licensee in sufficient detail to determine that an equivalent level of control is provided as those that would have been provided by previously reviewed and approved methods, such as those found in IEEE Std 828-1990 and IEEE Std 1042-1987.

The reviewer of the software configuration management system should evaluate that the system used by both the vendor and the licensee ensures that any software modifications during the design process and after acceptance of the software for use will be made to the appropriate version and revision of the software. This will involve not only a review of the Software Configuration Management documentation, but also a review of the actual methods being used at both the vendor and licensee sites, to ensure that the methods discussed in the plans are properly implemented.

5.3.6 Software Project Risk Management (IEEE Std 7-4.3.2-2003 Sub-Clause 5.3.6)

Software project risk management is a tool for problem prevention: identifying potential problems, assessing their impact, and determining which potential problems should be addressed to assure that software quality goals are achieved. Risk management should be performed at all levels of the digital system project to provide adequate coverage for each potential problem area. Software project risks may include technical, schedule, or resource-related risks that could compromise software quality goals, and thereby affect the ability of the safety computer system to perform safety-related functions. Risk factors that should be addressed include system risks, mechanical/electrical hardware integration, risks due to size and complexity of the product, the use of pre-developed software, cost and schedule, technological risk, and risks from program interfaces (maintenance, user, associate contractors, subcontractors, etc.).

Risk management should include the following items:

i. Determine the scope of risk management to be performed for the digital system

ii. Define and implement appropriate risk management strategies

iii. Identify risks to the software project in the project risk management strategy and as they develop during the conduct of the project

iv. Analyze risks to determine the priority for their mitigation

v. Develop risk mitigation plans for risks that have the potential to significantly impact software quality goals, with appropriate metrics for tracking resolution progress. (These risks may include technical, schedule, or resource-related project risks that could compromise the ability of the safety computer system to perform safety related functions)

vi. Take corrective actions when expected quality is not achieved

vii. Establish a project environment that supports effective communications between individuals and groups for the resolution of software project risks.

Additional guidance on the topic of risk management is provided in IEEE/EIA 12207.0-1996 and IEEE Std 1540-2001, "IEEE Standard for Life Cycle Processes – Risk Management."

Software project risk management differs from hazard analysis. A hazard is a condition that is prerequisite to an accident. Hazards include external events as well as conditions internal to computer hardware or software. The software and hardware safety plan addresses the identification, evaluation and resolution of hazards. Hazard analysis is the process that explores and identifies conditions that are not identified by the normal design review and testing process. The scope of hazard analysis extends beyond plant design basis events by including abnormal events and plant operations with degraded equipment and plant systems. The software safety plan should include the safety analysis implementation tasks that are to be carried out by the applicant/licensee. The acceptance criterion for software safety analysis implementation is that the tasks in that plan have been carried out in their entirety. Documentation should exist that shows that the safety analysis activities have been successfully accomplished for each life cycle activity group. In particular, the documentation should show that the system safety requirements have been adequately addressed for each activity group; that no new hazards have been introduced; that the software requirements, design elements, and code elements that can affect safety have been identified; and that all other software requirements, design, and code elements will not adversely affect safety.

SRP BTP 7-14 Subsection B.3.1.9 has additional details on the management, implementation and resource characteristics of the software safety plan.

Another item for risk management is the security considerations in the life cycle processes of digital computer-based systems. Guidance for the treatment of security items in the life cycle process is provided in Regulatory Guide 1.152, Revision 2 which endorses IEEE Std 7-4.3.2-2003.

The reviewer, when analyzing the risk management program, should keep in mind that licensee acceptance of risk is not necessarily sufficient or acceptable. As an example, if the licensee decides to use highly complex software in lieu of a simpler system, the licensee should demonstrate that the complexity is acceptable. The reviewer should look for alternative solutions, and analysis of those alternatives, and a reason why the complexity offered sufficient advantages to outweigh the disadvantages. The risk management program is intended to manage risk, not to only state that risk is acceptable.

5.4 **Equipment Qualification** (IEEE Std 7-4.3.2-2003 Clause 5.4)

In addition to the equipment qualification criteria provided by IEEE Std 603-1991 and Subsection 5.4 of SRP Appendix 7.1-C the following criteria are necessary to qualify digital computers for use in safety systems.

5.4.1 **Computer System Testing** (IEEE Std 7-4.3.2-2003 Sub-Clause 5.4.1)

Computer system equipment qualification testing should be performed with the computer functioning with software and diagnostics that are representative of those used in actual operation. All portions of the computer necessary to accomplish safety functions, or those portions whose operation or failure could impair safety functions, should be exercised during testing. This includes, as appropriate, exercising and monitoring the memory, the central processing unit, inputs, outputs, display functions, diagnostics, associated components, communication paths, and interfaces. Testing should demonstrate that the performance criteria related to safety functions have been met.

5.4.2 **Qualification of Existing Commercial Computers** (IEEE Std 7-4.3.2-2003 Sub-Clause 5.4.2)

EPRI TR-106439, as accepted by the NRC safety evaluation dated July 17, 1997, provides guidance for the evaluation of existing commercial computers and software to comply with the criteria of Sub-Clause 5.4.2 of IEEE Std 7-4.3.2-2003. The guidance of SRP BTP 7-14 may be applied to the evaluation of vendor processes described in EPRI TR-106439.

EPRI TR-107330, “Generic Requirements Specification for Qualifying a Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants, as accepted by the NRC safety evaluation dated July 30, 1998, provides more specific guidance for the evaluation of existing programmable logic controllers (PLC).

The fundamental criteria for demonstrating reasonable assurance that the computer will perform its intended safety functions is presented in this portion of IEEE Std 7-4.3.2-2003 and additional guidance is provided in EPRI TR-106439 and EPRI TR-107330.

The qualification process should be accomplished by evaluating the hardware and software design using the criteria of IEEE Std 7-4.3.2-2003. Acceptance should be based upon evidence that the digital system or component, including hardware, software, firmware, and interfaces, can perform its required functions. The acceptance and its basis should be documented and maintained with the qualification documentation.

In those cases in which traditional qualification processes cannot be applied, an alternative approach to verify that a component is acceptable for use in a safety-related application is commercial grade dedication. The objective of commercial grade dedication is to verify that the item being dedicated is equivalent in quality to equipment developed under a 10 CFR Part 50 Appendix B program.

The dedication process for the computer should entail identification of the physical, performance, and development process requirements necessary to provide adequate confidence that the proposed digital system or component can achieve the safety function. The dedication process should apply to the computer hardware, software, and firmware that are required to accomplish the safety function. The dedication process for software and firmware should include an evaluation of the design process.

The preliminary and detailed phase activities for commercial grade item dedication are described in Sub-Clauses 5.4.2.1 through 5.4.2.2 of IEEE Std 7-4.3.2-2003.

5.5 System Integrity (IEEE Std 7-4-3.2-2003 Clause 5.5)

In addition to the system integrity criteria provided by IEEE Std 603-1991, and the guidance in Subsection 5.5 of SRP Appendix 7.1-C, IEEE Std 7-4.3.2-2003 includes criteria in Sub-Clauses 5.5.1 through 5.5.3 for designs for computer integrity, test and calibration, and fault detection and self-diagnostics activities. The following are necessary to achieve system integrity in digital equipment for use in safety systems:

- Design for computer integrity
- Design for test and calibration
- Fault detection and self-diagnostics.

5.6 Independence (IEEE Std 7-4.3.2-2003 Clause 5.6)

Consistent with the requirements of IEEE Std 603-1991, data communication between safety channels or between safety and non-safety systems should not inhibit the performance of the safety function. Additional guidance on physical, electrical, and communication independence is provided in SRP Appendix 7.1-C Subsection 5.6.

IEEE Std 603-1991 requires that safety functions be separated from non-safety functions such that the non-safety functions cannot prevent the safety system from performing its intended functions. In digital systems, software performing both safety and non-safety functions may reside on the same computer and use the same computer resources. However, IEEE Std 603-1991, Sub-Clause 5.6.3.1 also requires that equipment that is used for both safety and non-safety functions shall be classified as part of the safety system. The term "equipment" includes both software and hardware of the digital systems. For this reason, any software providing non-safety functions that resides on a computer providing a safety function must be classified as a part of the safety system. If an applicant/licensee desires that a non-safety 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 non-safety software.

In some instances, vendors or applicants/licensees may wish to implement systems having some communication between the safety systems and non-safety systems. GDC 24, “Separation of protection and control systems,” requires that the protection system be separated from control systems to the extent that failure of any single control system component or channel, or failure or removal from service of any single protection system component or channel which is common to the control and protection systems leaves intact a system satisfying all reliability, redundancy, and independence requirements of the protection system, and that interconnection of the protection and control systems shall be limited so as to assure that safety is not significantly impaired.

In practical terms, this means that for communications between safety and non-safety systems, the communications must be such that the safety system does not require any non-safety input to perform its safety function, and that any failure of the non-safety system, communications system, or data transmitted by the non-safety system will not prevent or influence that independent safety determination. The portion of the safety software which actually performs the safety function, i.e., determining whether or not to trip based on sensor inputs, should not receive input or influence from any non-safety system while the safety system is on-line and performing that safety function.

The following provides some of the possible design approaches that a reviewer may encounter for data communications. It is neither exhaustive nor limiting in the possible approaches. If the reviewer is not sufficiently familiar with the communications systems and methods being used, the reviewer should seek the assistance of other NRC personnel and/or supervisor for the appropriate review strategy to determine that the communications can not interfere with the safety function.

- A communications system which broadcasts data from the safety system to the non-safety system without the use of handshaking and acknowledgment signals would satisfy these requirements.

- If the communications system allows two way communications between the safety and non-safety systems, the determination may require more detailed examination of the communications method, including memory allocation methods, communications protocols and message formatting methodology.

  One possibility may be to determine that the communications method is deterministic, that is, the same information is transmitted in the same way to the safety system, and is then used by the safety system in the same manner. This could be done by having the non-safety system write data to a specific location in shared memory, and the safety system would read that data. The safety system would know what the data means and what to do with the data because the data in that memory location would be the latest written value of the same data. There would have to be appropriate provisions for out-of-date data, garbled data, and communications link failure. This is, of course, one, but not the only possible method of deterministic communications.

The objective in the review is to determine that the applicant/licensee has satisfactorily demonstrated that the applicable requirements of 10 CFR 50.55a(h) and GDC-24 are met.

Additional guidance on communications independence is provided in SRP Appendix 7.0-A, SRP Appendix 7.1-C, and SRP Section 7.9.

5.7 <u>Capability for Test and Calibration</u> (IEEE Std 7-4.3.2-2003 Clause 5.7)

Sub-Clause 5.5.2 of IEEE Std 7-4.3.2-2003 recommends that test and calibration functions should not adversely affect the ability of the computer to perform its safety function. The reviewer should check to ensure this has been accomplished.

Sub-Clause 5.5.3 of IEEE Std 7-4.3.2-2003 recommends that fault detection and self-diagnostics are one means that can be used to assist in detecting partial system failures that could degrade the capabilities of the computer system, but may not be immediately detectable by the system.

The reviewer should carefully examine the capability of the software to test itself. From experience with a number of digital failures, the failures, were not in the operational code but in the diagnostic code. One of the reasons for this may be that the diagnostic code may be much more complex than the operational code. The reviewer should examine the portion of the analysis in the Factory Mutual Engineering Associates (FMEA) on diagnostic code failure. Assertions that failure of the operation code is not credible because the system and software diagnostics will find every failure should be carefully examined.

The total amount of software code should be compared to the amount of operational code. Large amounts of test and diagnostic software increase the complexity of the total software, and this increase in complexity should be balanced against the potential gain in confidence in the system provided by that test and diagnostic software. This may also be balanced by the extensive previous use of these diagnostic routines. The test and diagnostic software may have been well tested and extensively used in the past, while the operational code is likely new for this application. The reviewer's judgement should be used.

A non-software watchdog timer is critical in the overall diagnostic scheme. A software watchdog will fail to operate if the processor freezes and no instructions are processed. The reviewer should look for a hardware watchdog timer whose only software input is reset after the safety processor completes its function. Even then, the reviewer should look to ensure that there is no possibility of a software failure causing a jump to the reset function, thereby nullifying the effectiveness of the watchdog timer.

5.8 **Information Displays** (IEEE Std 7-4.3.2-2003 Clause 5.8)

In the past, information displays only provided a display function, and therefore required no two-way communications. More modern display systems may also have included control functions, and therefore the reviewer should ensure that incorrect functioning of the information displays does not prevent the safety function from being preformed when necessary. This is the same issue as in subsection 5.6, “Independence”, and similar methods are appropriate. If the communications path is one-way from the safety system to the displays, or if the displays and controls are qualified as safety related, the safety determination is simplified. Two-way communications with non-safety control systems have the same isolation issues as any other non-safety to safety communications. In addition, however, the reviewer should ensure that inadvertent actions, such as an unintended touch on a touch sensitive display can not prevent the safety function.

5.9 **Control of Access** (IEEE Std 7-4.3.2-2003 Clause 5.9)

Guidance is provided in Subsection 5.9 of SRP Appendix 7.1-C and Regulatory Guide 1.152, Revision 2.

5.10 **Repair** (IEEE Std 7-4.3.2-2003 Clause 5.10)

Guidance is provided in Subsection 5.10 of SRP Appendix 7.1-C.

5.11 **Identification** (IEEE Std 7-4.3.2-2003 Clause 5.11)

To provide assurance that the required computer system hardware and software are installed in the appropriate system configuration, the following identification requirements specific to software systems should be met:

i. Firmware and software identification should be used to assure the correct software is installed in the correct hardware component.

ii. Means should be included in the software such that the identification may be retrieved from the firmware using software maintenance tools.

iii. Physical identification requirements of the digital computer system hardware shall be in accordance with the identification requirements in IEEE Std 603-1991.

iv. The identification should be clear and unambiguous. The identification should include the revision level, and should be traceable to configuration control documentation which identifies the changes made by that revision.

Additional guidance on identification is provided in Subsection 5.11 of SRP Appendix 7.1-C.

5.12 **Auxiliary Features** (IEEE Std 7-4.3.2-2003 Clause 5.12)

There is no guidance beyond the requirements of IEEE Std 603-1991.

5.13 **Multi-Unit Stations** (IEEE Std 7-4.3.2-2003 Clause 5.13)

There is no guidance beyond the requirements of IEEE Std 603-1991.

5.14 **Human Factors Considerations** (IEEE Std 7-4.3.2-2003 Clause 5.14)

There is no guidance beyond the requirements of IEEE Std 603-1991. SRP Chapter 18 provides additional guidance.

5.15. **Reliability** (IEEE Std 7-4.3.2-2003 Clause 5.15)

In addition to the requirements of IEEE Std 603-1991, when reliability goals are identified, the proof of meeting the goals should include the software. The method for determining reliability may include combinations of analysis, field experience, or testing. Software error recording and trending may be used in combination with analysis, field experience, or testing.

Additional guidance is provided in Subsection 5.15 of SRP Appendix 7.1-C. As stated, in Regulatory Guide 1.152, The NRC does not endorse the concept of quantitative reliability goals as the sole means of meeting the NRC’s regulations for reliability of digital computers in safety systems. 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 system.

Since there is not a widely accepted view on software reliability value, determining a failure probability and therefore a reliability value is not possible. The reviewer should be cautious if vendors or licensees offer such a value. The NRC staff relies on the vendor using a high quality process of software design to obtain high quality software. The reviewer should expect the software to be of the highest quality, but should not depend on the software being perfect.

6. SENSE AND COMMAND FEATURES — FUNCTIONAL AND DESIGN REQUIREMENTS (IEEE Std 7-4.3.2-2003 Clause 6)

There is no guidance beyond the requirements of IEEE Std 603-1991.

7. EXECUTE FEATURES — FUNCTIONAL AND DESIGN REQUIREMENTS (IEEE Std 7-4.3.2-2003 Clause 7)

There is no guidance beyond the requirements of IEEE Std 603-1991.

8. POWER SOURCE REQUIREMENTS (IEEE Std 7-4.3.2-2003 Clause 8)

The reviewer should refer to Subsection 8 of SRP Appendix 7.1-C for guidance on implementation of the requirements of IEEE Std 603-1991.

9. CYBER SECURITY CRITERIA

Sub-Clause 5.9 of IEEE Std 603-1991 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. There should be no access via network connections, and access via maintenance equipment should be limited to those times the maintenance equipment is actually being used for maintenance. 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 safety systems (including hardware and software) should be secured against both physical and electronic threats. The consideration of hardware should ensure there is limited physical access control, and that there are no modems or connectivity to external networks. Security of computer-based system software relates to the ability to survive 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 deterred, detected, and mitigated. 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 that do not contain undocumented codes (e.g., back door coding, logic and/or time bomb codes) and that are resilient against malicious programs (e.g., viruses, worms, and Trojan horses), and (3) installing and maintaining those systems in accordance with the station administrative procedures and the licensee’s security program.

Regulatory Position 2 of Regulatory Guide 1.152, Revision 2, presents the waterfall lifecycle phases 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 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.

9.1 **Concepts Phase** (Regulatory Guide 1.152, Revision 2, Regulatory Position 2.1)

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.

9.2 **Requirements Phase** Regulatory Guide 1.152, Revision 2, Regulatory Position 2.2)

9.2.1 **System Features** (Regulatory Guide 1.152, Revision 2, Regulatory Position 2.2.1)

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).

9.2.2 <u>Development Activities</u> (Regulatory Guide 1.152, Revision 2, Regulatory Position 2.2.2)

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.

9.3 <u>Design Phase</u> (Regulatory Guide 1.152, Revision 2, Regulatory Position 2.3)

9.3.1 <u>System Features</u> (Regulatory Guide 1.152, Revision 2, Regulatory Position 2.3.1)

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.

9.3.2 <u>Development Activities</u> (Regulatory Guide 1.152, Revision 2, Regulatory Position 2.3.2)

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.

9.4 <u>Implementation Phase</u> (Regulatory Guide 1.152, Revision 2, Regulatory Position 2.4)

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].

9.4.1 <u>System Features</u> (Regulatory Guide 1.152, Revision 2, Regulatory Position 2.4.1)

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

9.4.2 **Development Activities** (Regulatory Guide 1.152, Revision 2, Regulatory Position 2.4.2)

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 effects 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.

9.5 **Test Phase** (Regulatory Guide 1.152, Revision 2, Regulatory Position 2.5)

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.

9.5.1 **System Features** (Regulatory Guide 1.152, Revision 2, Regulatory Position 2.5.1)

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.

9.5.2 **Development Activities** (Regulatory Guide 1.152, Revision 2, Regulatory Position 2.5.2)

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.

9.6 **Installation, Checkout, and Acceptance Testing** (Regulatory Guide 1.152, Revision 2, Regulatory Position 2.6)

In installation and checkout, the safety system is installed and tested in the target environment. The 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.

9.6.1 **System Features** (Regulatory Guide 1.152, Revision 2, Regulatory Position 2.6.1)

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.

9.6.2 **Development Activities** (Regulatory Guide 1.152, Revision 2, Regulatory Position 2.6.2)

The 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.

9.7 **Operation Phase** (Regulatory Guide 1.152, Revision 2, Regulatory Position 2.7)

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.

9.8 **Maintenance Phase** (Regulatory Guide 1.152, Revision 2, Regulatory Position 2.8)

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).

9.8.1 **Maintenance Activities** (Regulatory Guide 1.152, Revision 2, Regulatory Position 2.8.1)

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.

9.8.2 **Quality Assurance** (Regulatory Guide 1.152, Revision 2, Regulatory Position 2.8.2)

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.

9.8.3 **Incident Response** (Regulatory Guide 1.152, Revision 2, Regulatory Position 2.8.3)

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.

9.8.4 **Audits and Assessments** (Regulatory Guide 1.152, Revision 2, Regulatory Position 2.8.4)

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.

9.9 Retirement Phase (Regulatory Guide 1.152, Revision 2, Regulatory Position 2.9)

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 non-safety 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.

10. REFERENCES

1. EPRI Topical Report TR-106439. "Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications." Electric Power Research Institute, October 1996.

2. IEC 60880-2-2002. Software for Computers in the Safety Systems of Nuclear Power Stations - Part 2, Software Aspects of Defense Against Common Cause Failures, Use of Software Tools and of Pre-developed Software.

3. IEEE/ANS 7-4.3.2-1982. American Nuclear Society and IEEE Standard Application Criteria for Programmable Digital Computer Systems in Safety Systems of Nuclear Power Generating Stations.

4. IEEE Std 7-4.3.2-2003. "IEEE Standard for Digital Computers in Safety Systems of Nuclear Power Generating Stations."

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

6. IEEE Std 379-2000, "IEEE Standard Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems."

7. IEEE Std 603-1991. "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations."

8. IEEE Std 603-1998. "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations."
9. IEEE Std 828-1990. "IEEE Standard for Software Configuration Management Plans."

10. IEEE Std 1012-1998. "IEEE Standard for Software Verification and Validation."

11. IEEE Std 1042-1987. "IEEE Guide to Software Configuration Management."

12. IEEE Std 1061-1998, IEEE Standard for a Software Quality Metrics Methodology.

13. IEEE Std 1540-2001, IEEE Standard for Life Cycle Processes – Risk Management.

14. IEEE Std 12207.0-1996, IEEE/EIA Standard - Industry Implementation of International Standard ISO/IEC 12207:1995 (ISO/IEC 12207), Standard for Information Technology - Software Life Cycle Processes.

15. Regulatory Guide 1.152, Revision 2. “Criteria for Use of Computers in Safety Systems of Nuclear Power Plants.” Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 2006.

16. Regulatory Guide 1.168. “Verification, Validation, Reviews and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants.” Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 2004.

17. Regulatory Guide 1.169. “Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants.” Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1997.

18. Safety Evaluation by the Office of Nuclear Reactor Regulation. “EPRI Topical Report TR-106439, Guidance on the Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications.” July 17, 1997.

19. Safety Evaluation by the Office of Nuclear Reactor Regulation. “EPRI Topical Report TR-107330, Generic Requirements Specification for Qualifying a Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants”July 30, 1998.

PAPERWORK REDUCTION ACT STATEMENT

The information collections contained in the Standard Review Plan are covered by the requirements of 10 CFR Part 50 and 10 CFR Part 52, and were approved by the Office of Management and Budget, approval number 3150-0011 and 3150-0151.

PUBLIC PROTECTION NOTIFICATION

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