NUREG-0800

U.S. NUCLEAR REGULATORY COMMISSION

STANDARD REVIEW PLAN

BRANCH TECHNICAL POSITION 7-21

GUIDANCE ON DIGITAL COMPUTER REAL-TIME PERFORMANCE

REVIEW RESPONSIBILITIES

Primary - Organization responsible for the review of instrumentation and controls

Secondary - None

A. BACKGROUND

This branch technical position (BTP) provides guidelines for reviewing digital system real-time performance and system architectures in instrumentation and control (I&C) systems. These guidelines are based on reviews of licensee submittals and the analysis of these issues documented in NUREG/CR-6083, "Reviewing Real-Time Performance of Nuclear Reactor Safety Systems," and NUREG/CR-6082, "Data Communications."

1. Regulatory Basis

10 CFR 50.55a(h), "Protection and Safety Systems," requires compliance with 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 before January 1, 1971, the applicant/licensee may elect to comply instead with the plant-specific licensing basis. For nuclear power plants with construction permits issued between January 1, 1971, and May 13, 1999, the applicant/licensee

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 # ML070550070.

may elect to comply instead with the requirements stated in IEEE Std. 279-1971, "Criteria for Protection Systems for Nuclear Power Generating Stations." IEEE Std. 603-1991, Clause 4.10, requires in part that safety system design bases document the critical points in time or plant conditions after the onset of a design basis event. This information establishes requirements for system response times. IEEE Std. 603-1991, Clause 5.5, requires in part that safety systems be designed to accomplish their safety functions under the full range of applicable conditions enumerated in the design basis.

10 CFR 50 Appendix A, General Design Criterion (GDC) 10, "Reactor Design," requires in part that control and protection systems be designed with appropriate margin to assure that specified acceptable fuel damage limits are not exceeded. This includes timing and performance margins.

GDC 12, "Suppression of Reactor Power Oscillations," requires in part that reactor power oscillations are either (1) not possible or (2) detected and suppressed. This requirement places strict real-time constraints on any protection system components that detect and suppress power oscillations.

GDC 13, "Instrumentation and Control," requires in part that instrumentation be provided to monitor variables and systems over their anticipated ranges for normal operations, for anticipated operational occurrences, and for accident conditions as appropriate to assure adequate safety. Digital instrumentation must respond quickly enough so that the behavior of variables can be ascertained by operators.

GDC 19, "Control Room," requires in part that applicants establish a control room from which actions can be taken to operate the nuclear power unit safely under normal conditions, and to maintain the nuclear power unit in a safe condition during an accident. In addition, a remote shutdown capability is required to permit the reactor to be safely shut down.

GDC 20, "Protection System Functions," requires in part that the reactor protection system provide automatic initiation so that (1) fuel design limits are not exceeded and (2) accidents are sensed and mitigated. Both require timely operation of protection system components, thus establishing the timing requirements for detecting parameters exceeding their setpoints and equipment actuation in the protection system.

GDC 21, "Protection System Reliability and Testability," requires in part high functional reliability of safety systems. Timely operation is necessary for high functional reliability of safety systems.

GDC 23, "Protection System Failure Modes," requires in part the protection system to be designed so that if it fails, it fails into a safe state given the anticipated failure modes and conditions in which the failure occurs. This is a design architectural issue aimed at staying within timing limits.

GDC 25, "Protection System Requirements for Reactivity Control Malfunctions," requires in part reactivity control to prevent fuel design limits from being exceeded. This requires timely operation of the protection features of the reactivity control system.

GDC 28, "Reactivity Limits," requires in part a limited reactivity rate-of-change to prevent (1) fuel limits from being exceeded and (2) a non-coolable core geometry. The protection system must meet the timing requirements imposed by this criterion.

GDC 29, "Protection Against Anticipated Operational Occurrences," requires in part defense against anticipated operational transients to assure an extremely high probability of accomplishing safety functions. To assure this, the protection system must be demonstrated to operate within the time constraints of each anticipated operational transient.

2. Relevant Guidance

IEEE Std. 603-1991 is a system-level standard that contains requirements related to performance and timing. This standard requires in part that a reactor safety system have a documented design basis consisting of the following:

- Clause 4.4 - limits, ranges, and rates of change of variables should be included in the documented design basis.

- Clause 4.10 - critical points in time should be specified for:

  – Initiation of protective action.

  – Completion of protective action.

  – Time when automatic control of protective action is required.

  – Time when protective system may be returned to normal.

- Clause 6.1 - timely automatic control action is required when events occur too quickly for operator intervention.

Appendix 7.1-C provides Standard Review Plan (SRP) acceptance criteria for safety system compliance with 10 CFR 50.55a(h).

Appendix 7.1-B provides SRP acceptance criteria for protection system compliance with 10 CFR 50.55a(h).

Appendix 7.1-D provides SRP acceptance criteria for digital I&C compliance with IEEE Std. 7-4.3.2-2003, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations," as endorsed by Regulatory Guide 1.152, Revision 2, "Criteria for Digital Computers in Safety Systems of Nuclear Power Plants."

IEEE Std. 7-4.3.2-2003, Clause 2, states that this standard shall be used in conjunction with additional standards, including:

- IEEE Std. 1012-1998, "IEEE Standard for Software Verification and Validation," which is endorsed by Regulatory Guide 1.168, Revision 1, "Verification, Validation, Reviews and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants."

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

IEEE/EIA Std. 12207.0-1996 is a software standard for organizing and managing software life cycle processes. This standard states in part:

- Clause 5.3.4.1 - performance requirements shall be established and documented as part of software requirements analysis.

- Clauses 5.3.5.6, 5.3.6.7, 5.3.7.5, 5.3.8.5, 5.3.9.3, 5.3.10.3 and 5.3.11.2 - software requirements, including performance requirements, shall be traced through architectural design, detailed design, coding, testing, software integration, software qualification testing, system integration, and system qualification testing.

- Clauses 6.4.2 and 6.5.2 - requirements, including performance requirements, shall be verified and validated throughout the software life cycle.

IEEE Std. 1012-1998 is a standard for software verification and validation (V&V). Detailed criteria for the V&V tasks are given in IEEE Std. 1012-1998, Table 1. This table states in part:

- Clause 5.4.2, "Requirements V&V Activity," (2) "Software Requirements Evaluation" - performance requirements (including timing, sizing, speed, capacity, accuracy, precision, safety and security) shall be evaluated for correctness, completeness, consistency and testability.

- Clause 5.4.2, "Requirements V&V Activity," (5) "System V&V Test Plan Generation and Validation" - system test plans shall include test designs, cases, procedures and results for, among other requirements, system performance requirements, performance at boundaries (such as data and interfaces), and under-stress conditions.

- Clause 5.4.3, "Design V&V Activity," (2) "Software Design Evaluation" - design elements shall be evaluated to ensure that performance requirements are correctly and completely included.

- Clause 5.4.3, "Design V&V Activity," (5) "Component V&V Test Plan Generation and Validation" - testing shall be planned so as to validate timing criteria, performance at boundaries and interfaces, and performance under stress conditions.

- Clause 5.4.4, "Implementation V&V Activity," (2) "Source Code and Source Code Evaluation Documentation" - source code elements shall be evaluated to ensure that performance requirements are correctly and completely included.

- Clause 5.4.4, "Implementation V&V Activity," (7) "Component V&V Test Execution and Validation" - components shall be evaluated to assure that the implementation, including performance, satisfy the design.

- Clause 5.4.5, "Test V&V Activity" - integration, system, and acceptance testing shall be carried out, including performance aspects.

- Various clauses require that requirements, including performance requirements, be traced from requirements through design, implementation, and testing.

- Annex G (informative) as modified by Regulatory Position 7 of Regulatory Guide 1.168, "Optional V&V Task Descriptions" - various tasks are described, including:

  – Performance monitoring - performance information is continually collected and analyzed under operational conditions to assure that system and software performance requirements are satisfied.

  – Sizing and timing analysis - data about the software functions and resource utilization is collected and analyzed to determine if system and software requirements for speed and capacity are satisfied.

Regulatory Guide 1.105, Revision 3, "Setpoints for Safety-Related Instrumentation," endorses ISA-S67.04-1994, Part 1, "Setpoints for Nuclear Safety-Related Instrumentation," as an acceptable method for initially setting and maintaining instrument calibrations in nuclear reactor I&C systems in order to assure their proper response on demand. System time delays are an important consideration in establishing instrument setpoints. Additional guidance on the application of Regulatory Guide 1.105, Revision 3, is provided by SRP BTP 7-12.

In addition to the above, NUREG/CR-6082 describes data communication systems, including aspects related to system performance and timing. NUREG/CR-6083 describes real-time systems with respect to performance, timing, and complexity. These documents include detailed guidance for reviewing such systems and a glossary of related terms.

3. Purpose

The purpose of this BTP is to provide guidance for NRC staff to verify conformance with the previously cited regulatory bases and standards in the design of digital computer systems. This BTP has three objectives:

- To verify that system timing requirements calculated from the design basis events and other criteria have been allocated to the digital computer portion of the system as appropriate, and have been satisfied in the digital system design and implementation.

- To make the reviewer aware that more extensive efforts are required to verify certain timing design and implementation techniques, such as interrupts.

- To assess the technical basis for concluding that the installed plant systems perform as predicted when enlarged from small-scale or partial-system engineering prototypes used in the design phases.

B. BRANCH TECHNICAL POSITION

1. Introduction

System architecture needs to be considered in evaluating real-time performance.

Digital system architecture affects performance because communication between components of the system takes time, and allocation of functions to various system components affects timing. The architecture may also affect timing because an arrangement of otherwise simple components may have unexpected interactions. Requirements for redundancy and diversity may complicate timing analysis because they result in additional components and interconnections. General guidance on evaluating a system architecture is given in SRP BTP 7-14.

Specific timing requirements may affect system architecture because it may not be possible to get sufficient computational performance for a specific function or group of functions from a single processor, or the locations where functions are performed may be widely separated. Timing requirements may also increase complexity, either by fragmenting the system into multiple processors or by code tuning, which makes the software product harder to understand, verify, or maintain.

The digital instrumentation loop often includes the sensor, transmitter, analog-to-digital converter, multiplexer, data communication equipment, demultiplexer, computers, memory devices, controls, and displays. Timing analysis should consider the entire loop.

2. Information to be Reviewed

Information to be reviewed is contained in the safety analysis report (SAR), revisions to the SAR, license amendment requests, topical reports, and other applicant/licensee documentation. The SAR and referenced documents typically contain the architectural description, design basis events and analyses, and certain design commitments. Inspections, tests, analyses and acceptance criteria (ITAAC) or detailed design documents describe designs, tests, analyses, or other methods of demonstrating satisfaction of design commitments for applications made under 10 CFR 52, "Early Site Permits; Standard Design Certifications; and Combined Licenses for Nuclear Power Plants."

3. Acceptance Criteria

If the following criteria are met, the Staff may conclude that the design or completed system will meet timing requirements, can be verified as correct and timely, or that a prototype system accurately reflects the performance and correctness expected of the actual plant. Some of the criteria described herein may be met by submissions describing a software development process or verification methods that include real-time concerns.

Limiting Response Times

Limiting response times should be shown to be consistent with safety requirements (e.g., suppress power oscillations, prevent fuel design limits from being exceeded, prevent a non-coolable core geometry). Setpoint analyses and limiting response times should also be shown to be consistent. The reviewer should verify that limiting response times are acceptable to the organizations responsible for reactor systems, electrical systems, and plant systems before accepting the limiting response times as a basis for timing requirements.

Digital Computer Timing Requirements

Digital computer timing should be shown to be consistent with the limiting response times and characteristics of the computer hardware, software, and data communications systems. Computer system timing requirements that should be addressed in a software requirements specifications are described in SRP BTP 7-14.

Architecture

The level of detail in the architectural description should be sufficient that the Staff can determine the number of message delays and computational delays interposed between the sensor and the actuator. An allocation of time delays to elements of the system and software architecture should be available. In initial design phases (e.g., at the point of design certification application), an estimated allocation of time delays to elements of the proposed architecture should be available. Subsequent detailed design and implementation should develop refined timing allocations down to unit levels in the software architecture.

A design should be feasible with currently known methods and representative equipment. Design timing feasibility may be demonstrated by allocating a timing budget to components of the system architecture so that the entire system meets its timing requirements. See NUREG/CR-6083, Sections 2.2, 2.3.1, and 2.3.2, and NUREG/CR-6082. The timing budget should include internal and external communication delays, with adequate margins.

Any non-deterministic delays should be noted and a basis provided that such delays are not part of any safety functions, nor can the delays impede any protective action.

Software architectural timing requirements should be addressed in a software architectural description as described in SRP BTP 7-14. Databases, disk drives, printers, or other equipment or architectural elements subject to halting or failure should not be able to impede protective system action.

Design Commitments

Design basis documents should describe system timing goals.

Timing requirements should be satisfied by design commitments.

A design should consider data rates, data bandwidths, and data precision requirements for normal and off-normal operation, including the impact of environmental extremes. There should be sufficient excess capacity margins to accommodate likely future increases in demands or software or hardware changes to equipment.

Design basis documents should identify design practices that the applicant/licensee will use to avoid timing problems. Risky design practices such as non-deterministic data communications, non-deterministic computation, use of interrupts, multitasking, dynamic scheduling, and event-driven design should be avoided. When such practices are allowed, the applicant/licensee should describe methods for control of the associated risk. NUREG/CR-6082 and NUREG/CR-6083 describe risky design practices in more detail.

Performance Verification

The means proposed, or used, for verifying a system's timing should be consistent with the design.

Testing and/or analytic justification should show that the system meets limiting response times for a reasonable, randomly selected subset of system loads, conditions, and design basis events. The subset should include some limiting load conditions and be chosen by persons independent of the persons who designed the system.

Both analytical and test techniques of timing analysis have drawbacks. It is difficult to demonstrate completeness of timing tests. Completeness is easier to demonstrate for analyses, but analyses predict extreme times that are not actually possible. Therefore, analysis and testing are often combined in a complementary manner to confirm that a system can meet the limiting response times.

Measurement methods should be appropriate to the resolution and detail required.

Timing measurements should meet projections or the anomalies should be satisfactorily explained (NUREG/CR-6083, Sections 2.1, 2.3.3, and 2.3.4).

Use of Cyclic Real-Time Executive

In systems that include a cyclic real-time executive (operating system), a typical cycle includes application modules, diagnostic modules, and other support modules. A watch-dog timer is normally set at the beginning of each cycle and reset at the end. If the cycle is not completed before the watch-dog timer period is complete, an error is generated.

A basis should be provided that describes the cycle and demonstrates that the watch-dog timer is correctly implemented, the time required for the application modules does not exceed the allotted time given in the architecture timing budget, and diagnostic and other support modules will not cause the allotted time to be exceeded.

Examples of solutions acceptable to the Staff may be found in the Safety Evaluation Reports for the Palo Verde Nuclear Generating Station, Units 1, 2, and 3, "Issuance of Amendments on the Core Protection Calculator System Upgrade," dated October 24, 2003, and the Siemens Power Corporation, Topical Report EMF-2110(NP), "Teleperm XS: A Digital Reactor Protection System," dated May 5, 2000.

Use of Part-Scale Prototypes

In systems that have not been implemented and tested on a full scale, expected system delays on scale-up should be calculated and shown to be less than limiting system response times (NUREG/CR-6083, Sections 2.1.3 and 2.1.4).

A basis should be provided that describes the effects of adding sensors, divisions, communication links, controllers, computer nodes, or actuation devices required to scale the test system to full scale.

Test data should confirm scaling as well as performance projections. Exceptions are considered anomalies or abnormal events.

Prototypes designed to demonstrate scaling should include all significant architectural elements plus enough additional elements to show the scaling effects to be measured.

4. Review Procedures

Based on review of the available information and applicant/licensee commitments, the reviewer should reach a conclusion appropriate to the level of detail and type of submittal. For certified designs under 10 CFR 52, preliminary SARs, or topical reports, the level of detail typically includes only information to verify limiting response times, digital computer timing requirements, architecture, and design commitments. For this level of detail, the reviewer verifies that system timing requirements calculated from the design basis events and other criteria have been allocated to the digital computer portion of the system as appropriate, and have been satisfied in the digital system architectural design.

When ITAAC or detailed design documents that describe designs, tests, analyses, or other methods of demonstrating satisfaction of design commitments are available, the reviewer verifies that the installed plant systems perform as predicted and appropriate measurement and analysis techniques have been used to compensate for the uncertainties introduced by certain design and implementation practices, such as the use of interrupts. This level of review verifies satisfaction of two acceptance criteria groups - performance verification and use of part-scale prototypes.

C. REFERENCES

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

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

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

4. IEEE/EIA Std. 12207.0-1996, "Industry Implementation of International Standard ISO/IEC 12207: 1995 (ISO/IEC 12207) Standard for Information TechnologySoftware Life Cycle Processes," March 1998.

5. IEEE Std. 1012-1998, "IEEE Standard for Software Verification and Validation," March 1998.

6. ISA-S67.04-1994, "Setpoints for Nuclear Safety-Related Instrumentation."

7. NUREG/CR-6082, "Data Communications," August 1993.

8. NUREG/CR-6083, "Reviewing Real-Time Performance of Nuclear Reactor Safety Systems," August 1993.

9. Regulatory Guide 1.105, Revision 3, "Setpoints for Safety-Related Instrumentation." Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1999.

10. Regulatory Guide 1.152, Revision 2, "Criteria for Digital Computers in Safety Systems of Nuclear Power Plants," Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, January 2006.

11. Regulatory Guide 1.168, Revision 1, "Verification, Validation, Reviews and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," February 2004.

12. Safety Evaluation Report for the Palo Verde Nuclear Generating Station, Units 1, 2 and 3, "Issuance of Amendments on the Core Protection Calculator System Upgrade," October 24, 2003.

13. Safety Evaluation Report for Siemens Power Corporation, Topical Report EMF-2110(NP), "Teleperm XS: A Digital Reactor Protection System," May 5, 2000.

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.