U.S. NUCLEAR REGULATORY COMMISSION

STANDARD REVIEW PLAN

BRANCH TECHNICAL POSITION 7-17

GUIDANCE ON SELF-TEST AND SURVEILLANCE TEST PROVISIONS

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 the design of the self-test and surveillance test provisions. These guidelines are based on reviews of applicant/licensee submittals and vendor topical submittals describing self-test and surveillance test assumptions, terminology, methodology, and experience gained from NRC inspections of operating plants.

1. Regulatory Basis

10 CFR 50.55a(h), "Protection and Safety Systems," requires compliance with Institute of Electrical and Electronics Engineers (IEEE) Standard. 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 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 5.7, requires that capability for testing and calibration of safety system equipment be provided while retaining the capability of the safety systems to accomplish their safety functions.

IEEE Std. 603-1991, Clause 5.1, requires that the safety system be able to perform its safety function required for a design basis event in the presence of (1) any single detectable failure within the safety systems concurrent with all identifiable, but non-detectable, failures, (2) all failures caused by the single failure, and (3) all failures and spurious system actions that cause or are caused by the design basis event requiring the safety functions.

10 CFR Part 50 Appendix A, General Design Criterion (GDC) 21, "Protection System Reliability and Testability," requires in part that the protection system be designed for high functional reliability and in-service testability commensurate with the safety functions to be performed. It also requires a design that permits periodic testing of its functioning when the reactor is in operation, including the capability to test channels independently to determine failures and losses of redundancy that may have occurred.

GDC 22, "Protection System Independence," requires in part that the protection system be designed to assure that the effects of natural phenomena and of normal operating, maintenance and testing do not result in loss of protection function.

10 CFR Part 50 Appendix B, Criterion XII, "Control of Measuring and Test Equipment," requires in part that measures be established to assure that measuring and testing devices used in activities affecting quality are properly controlled, calibrated, and adjusted at specified periods to maintain accuracy within necessary limits.

2. Relevant Guidance

Regulatory Guide 1.22, "Periodic Testing of Protection System Actuation Functions," describes acceptable methods of including actuation devices in the periodic tests of the protection system during reactor operations.

Regulatory Guide 1.47, "Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems," describes an acceptable method of complying with the requirements of IEEE Std. 279-1971 with regard to indicating the inoperable status of a portion of the protection system, systems actuated or controlled by the safety system, or auxiliary supporting features and other auxiliary features. IEEE Std 603-1991, Clause 5.8.3, gives the equivalent requirements for safety systems.

Regulatory Guide 1.53, "Application of the Single-Failure Criterion to Safety Systems," which endorses IEEE Std. 379-2000, "IEEE Standard Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems," states that the protection system must be capable of accomplishing the required protective function in the presence of any single detectable failure concurrent with all identifiable, but non-detectable, failures. Consequently, self-testing and periodic testing are important elements in the design's ability to meet the single-failure criterion.

Regulatory Guide 1.118, "Periodic Testing of Electric Power and Protection Systems," states that the criteria of IEEE Std. 338-1987, "IEEE Standard Criteria for the Periodic Surveillance Testing of Nuclear Power Generating Station Safety Systems," are considered acceptable methods for the periodic testing of protection systems (subject to the specific exceptions discussed in Regulatory Guide 1.118). IEEE Std. 338-1987 provides design and operational criteria for the performance of periodic and automatic testing; its criteria are supplementary to IEEE Std. 603-1991.

Regulatory Guide 1.152, "Criteria for Digital Computers in Safety Systems of Nuclear Power Plants," endorses IEEE Std. 7-4.3.2-2003, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations," systems. The Regulatory Guide and endorsed standard provide guidance applicable to the development of self-test software and to making safety functions independent from self-test functions.

3. Definitions

Periodic tests are tests performed at scheduled intervals to detect failures and verify operability (IEEE Std. 338-1987). Periodic tests include surveillance tests.

A self-test is a test or series of tests performed by a device upon itself. Self-tests include on-line continuous self-diagnostics, equipment-initiated self-diagnostics, and operator-initiated self-diagnostics.

Surveillance tests are conducted specifically to confirm compliance with technical specification surveillance requirements.

A watchdog timer is a form of interval timer that is used to detect a possible malfunction (IEEE Std. C37.1-1994, "IEEE Standard Definition, Specification, and Analysis of Systems Used for Supervisory Control, Data Acquisition, and Automatic Control").

4. Purpose

The purpose of this BTP is to provide guidance for NRC staff to verify that the previously cited regulatory basis and standards are met by an applicant/licensee's submittal. The objectives of this BTP are to confirm that:

- The safety system (including self-test) is designed for in-service testability commensurate with the safety functions to be performed through all modes of plant operation.
- The positive aspects of self-test features are not compromised by the additional complexity that may be added to the safety system by the self-test features.
- Hardware and software design support the required periodic testing.
- Failure modes assumed to be detectable by the single-failure analysis are in fact detectable. Failures may be detectable by observing operational characteristics as well as other methods.

B. BRANCH TECHNICAL POSITION

1. Introduction

Surveillance testing taken together with automatic self-testing should provide a mechanism for detecting all detectable failures.

Digital computer-based instrumentation and control (I&C) systems are more prone to different kinds of failures than traditional analog systems are. Self-testing and watchdog timers should reduce the time to detect and identify failures. Computer self-testing is most effective at detecting random hardware failures.

The characteristics of digital systems should be considered in the review of technical specification surveillance features. Architectural differences between digital and analog systems warrant careful consideration during the review of surveillance test provisions. Furthermore, the concepts used to determine test intervals for hardware-based systems do not apply directly to the software used in digital computer-based I&C systems. Therefore, previous reliability analysis used to establish test intervals will address the effects of software usage. Similar reviews are performed as necessary to verify the self-test and periodic test provisions for non-safety systems.

2. Information to be Reviewed

Applicant/licensee's technical description of surveillance and self-test features, single-failure analyses, failure modes and effects analyses, and plant technical specifications should be reviewed.

3. Acceptance Criteria

Surveillance test and self-test features for digital computer-based protection systems should conform to the guidance of Regulatory Guide 1.22 and Regulatory Guide 1.118. Bypasses necessary to enable testing should conform with the guidance of Regulatory Guide 1.47.

Failure Detection

Failures detected by hardware, software, and surveillance testing should be consistent with the failure detectability assumptions of the single-failure analysis and the failure modes and effects analysis.

Self-Test Features

Digital computer-based I&C systems should include self-test features to confirm computer system operation on system initialization.

Digital computer-based I&C systems should generally include continuous self-testing. Some small, stand-alone, embedded digital computers may not need self-testing. Typical self-tests include monitoring memory and memory reference integrity, using watch-dog timers or processors, monitoring communication channels, monitoring central processing unit status, and checking data integrity.

Other self-testing features that are candidates for incorporation into digital computer-based I&C systems include plausibility checks for intermediate results, evaluation using different methods, ranges of variables, array bound checking, well-defined outputs for detected failures, reporting of errors for which error recovery techniques are used, use of counters and reasonableness traps, and correctness verification of transferred parameters. SRP BTP 7-14 discusses a number of functional characteristics for software design, such as robustness and timing, which could give rise to self-testing features. Self-tests may also include automatic calibration tests such as the use of fundamental physical principles in Johnson noise thermometry to calibrate resistance temperature detectors (RTDs).

The design of automatic self-test features should maintain channel independence, maintain system integrity, and meet the single-failure criterion during testing. The scope and extent of interfaces between software that performs protection functions and software for other functions such as self-test should be designed to minimize the complexity of the software logic and data structures. The safety classification of the hardware and software used to perform automatic self-testing should be equivalent to that of the tested system unless physical, electrical, and communications independence are maintained such that no failure of the test function can inhibit the performance of the safety function.

The positive aspects of self-test features should not be compromised by the additional complexity that may be added to the safety system by the self-test features. The improved ability to detect failures provided by the self-test features should outweigh the increased probability of failure associated with the self-test feature.

Self-test functions should be verified during periodic functional tests.

Surveillance Testing

Systems should be able to conduct periodic surveillance testing consistent with the technical specifications and plant procedures. As delineated in Regulatory Guide 1.118, periodic testing consists of functional tests and checks, calibration verification, and time response measurements.

As required by IEEE Std. 279-1971, Clause 4.13, or IEEE Std. 603-1991, Clause 5.8.3, and as stated in Regulatory Guide 1.47, if the protective action of some part of a protection or safety system is bypassed or deliberately rendered inoperative for testing, that fact should be continuously indicated in the control room. Provisions should also be made to allow operations staff to confirm that the system has been properly returned to service.

Regulatory Guide 1.118 states in part that test procedures for periodic tests should not require makeshift test setups. For digital computer-based systems, makeshift test setups, including temporary modification of code or data that must be appropriately removed to restore the system to service, should be avoided.

If automatic test features are credited with performing surveillance test functions, provisions should be made to confirm the execution of the automatic tests during plant operation. The capability to periodically test and calibrate the automatic test equipment should also be provided. The balance of surveillance and test functions that are not performed by the automatic test feature should be performed manually to meet the intent of Regulatory Guide

1.118. In addition, the automatic test feature function should conform to the same requirements and considerations (e.g., test interval) as the manual function.

The safety classification and quality of the hardware and software used to perform periodic testing should be equivalent to that of the tested system. The design should maintain channel independence, maintain system integrity, and meet the single-failure criterion during testing. Commercial digital computer-based equipment used to perform periodic testing should be appropriately qualified for its function.

Actions on Failure Detection

The design should have either the automatic or manual capability to take compensatory action on detection of any failed or inoperable component. The design capability and plant technical specifications, operating procedures, and maintenance procedures should be consistent with each other.

Plant procedures should specify manual compensatory actions and mechanisms for recovery from automatic compensatory actions.

Mechanisms for operator notification of detected failures should comply with the system status indication provisions of IEEE Std. 603-1991 and should be consistent with, and support, plant technical specifications, operating procedures, and maintenance procedures.

4. Review Procedures

The surveillance test and self-test features of each digital computer-based module, as well as each system incorporating digital computers, are reviewed to verify conformance with acceptance criteria.

The review of surveillance test provisions should confirm that these provisions are adequate to fulfill the fundamental intent of each surveillance test. Because of design and architectural differences between analog and digital systems, traditional provisions for analog systems may not be adequate for digital computer-based systems.

C. REFERENCES

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

2. IEEE Std. 338-1987, "IEEE Standard Criteria for the Periodic Surveillance Testing of Nuclear Power Generating Station Safety Systems."

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

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

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

6. IEEE Std. C37.1-1994, "IEEE Standard Definition, Specification, and Analysis of Systems Used for Supervisory Control, Data Acquisition, and Automatic Control."

7. Regulatory Guide 1.22, "Periodic Testing of Protection System Actuation Functions," Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1972.

8. Regulatory Guide 1.47, "Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems," Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1973.

9. Regulatory Guide 1.53, "Application of the Single-Failure Criterion to Nuclear Power Safety Systems," Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 2003.

10. Regulatory Guide 1.118, "Periodic Testing of Electric Power and Protection Systems," Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1995.

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

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.
