NEW

Branch Technical Position HICB-17

Guidance on Self-Test and Surveillance Test Provisions

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 Systems," requires in part that protection systems satisfy the criteria of ANSI/IEEE Std 279, "Criteria for Protection Systems for Nuclear Power Generating Stations." Section 4.10 of ANSI/IEEE Std 279 requires the capability to test and calibrate protection system channels and devices. Section 4.21 states that protection systems must be designed to facilitate the recognition and location of malfunctioning components or modules. Additionally, Section 4.2 requires that any single failure within the protection system shall not prevent proper protective action at the system level. Reg Guide 1.153, "Criteria for Power, Instrumentation, and Control Portions of Safety Systems," which endorses IEEE Std 603, "Standard Criteria for Safety Systems for Nuclear Power Generating Stations," contains similar requirements. Reg. Guide 1.53, "Application of the Single-Failure Criterion to Nuclear Power Protection Systems," which endorses ANSI/IEEE Std 379, "Standard Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems," amplifies this requirement by noting 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 a design's ability to meet the single-failure criterion.

10 CFR 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 a capability to test channels independently to determine failures and losses of redundancy that may have occurred.

10 CFR 50 Appendix A, GDC 22, "Protection System Independence," requires in part that the protection system be designed to ensure that the effects of natural phenomena, and of normal operating, maintenance and testing do not result in loss of protection function.

10 CFR 50 Appendix B, Criterion 12, "Control of Measuring and Test Equipment," requires in part that measures be established to ensure 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

Reg. 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.

Reg. Guide 1.47, "Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems," describes an acceptable method of complying with the requirements of ANSI/IEEE Std 279 with regard to indicating the inoperable status of a portion of the protection system, systems actuated or controlled by the safety system, or essential auxiliary support systems.

Reg. Guide 1.53 "Application of the Single-Failure Criterion to Nuclear Power Plant Protection Systems," clarifies the application of the single-failure criterion and endorses ANSI/IEEE Std 379, "Standard Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems." ANSI/IEEE Std 379 discusses the credit taken for testing in the application of the single-failure criterion.

Reg. Guide 1.118, "Periodic Testing of Electric Power and Protection Systems," states that the requirements and recommendations of IEEE Std 338, "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 Reg. Guide 1.118). IEEE Std 338 provides design and operational criteria for the performance of periodic and automatic testing; its requirements and criteria are supplementary to ANSI/IEEE Std 279 and IEEE Std 603.

Reg. Guide 1.152, . "Criteria for Digital Computers in Safety Systems of Nuclear Power Plants," which endorses IEEE Std 7-4.3.2, "IEEE Standard for Digital Computers in Safety Systems of Nuclear Power Generating Stations," and IEC Std 880, "Software for Computers in the Safety Systems of Nuclear Power Stations," recommend characteristics for self-testing in digital computer-based protection systems.

Reg. Guide 1.153 "Criteria for Power, Instrumentation, and Control Portions of Safety Systems," endorses IEEE Std 603, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," as an alternative to ANSI/IEEE Std 279.

3. Definitions

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

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

Surveillance tests are tests 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 (ANSI/IEEE Std C37.1, "Standard Definitions, 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

Digital computer-based instrumentation and control systems are prone to different kinds of failures than are traditional analog systems. Self-testing and watchdog timers may reduce the time to detect and identify failures, but are not a guarantee of hardware or software error detection. Computer self-testing is most effective at detecting random hardware failures.

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

The characteristics of digital systems must 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 directly apply to the software used in digital computer-based instrumentation and control systems. Therefore, previous reliability analysis used to establish test intervals may not apply.

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 mode and effect analyses, and plant technical specifications should be considered in the review.

3. Acceptance Criteria

Surveillance test and self-test features for digital computer-based protection systems should conform to the guidance of Reg. Guide 1.22, Reg. Guide 1.118, and Reg. Guide 1.153, "Criteria for Power, Instrumentation,

and Control Portions of Safety Systems." Bypasses necessary to enable testing should conform with the guidance of Reg. 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 instrumentation and control systems should include self-test features to confirm computer system operation upon system initialization.

Digital computer-based instrumentation and control 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, correctness verification of transferred parameters, and the use of assertions (see IEC Std 880). BTP HICB-14 discusses a number of functional characteristics for software design outputs, such as robustness and timing, which could give rise to self-testing features.

Hardware and software used to perform automatic self-testing should be of equivalent safety classification, quality, and reliability as the tested system. The design 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 testing should be designed to minimize the complexity of the software logic and data structures. The hardware and software used to perform automatic self-testing should be of equivalent safety classification 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.

Periodic Testing

Systems should provide the ability to conduct periodic testing consistent with the technical specifications and plant procedures.

As required by ANSI/IEEE Std 279, Section 4.13 and Reg. Guide 1.47, if the protective action of some part of a protection 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.

Reg. 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 self-test features are credited with automatically performing surveillance test functions, provisions must be made to confirm the execution of the automatic tests during plant operation. The capability to periodically test and calibrate the automatic test equipment must also be provided.

Hardware and software used to perform periodic self-testing should be of equivalent safety classification and quality as 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 upon 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 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

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

ANSI/IEEE Std 379-1988. "Standard Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems."

ANSI/IEEE Std C37.1-1987. "Standard Definitions, Specification, and Analysis of Systems Used for Supervisory Control, Data Acquisition, and Automatic Control."

IEC Std 880. "Software for Computers in the Safety Systems of Nuclear Power Stations." IEC Publication 1986.

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

IEEE Std 7-4.3.2-1993. "IEEE Standard for Digital Computers in Safety Systems of Nuclear Power Generating Stations."

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

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.

Regulatory Guide 1.53. "Application of the Single-Failure Criterion to Nuclear Power Protection Systems." Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1973.

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

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, 1996.

Regulatory Guide 1.153. "Criteria for Power, Instrumentation, and Control Portions of Safety Systems." Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1996.