NEW

Branch Technical Position HICB-21

Guidance on Digital Computer Real-Time Performance

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 Systems," requires in part that protection systems satisfy the criteria of IEEE Std 279, "Criteria for Protection Systems for Nuclear Power Generating Stations." Section 3 of the standard requires, in part, specification of the protection system design basis, including system response times. Section 4.1 requires in part that the protection system automatically initiate protective action within the range of performance 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 ensure that specified acceptable fuel damage limits are not exceeded. This includes timing and performance margins.

10 CFR 50 Appendix A, 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.

10 CFR 50 Appendix A, 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 ensure adequate safety. Digital instrumentation must respond quickly enough so that the behavior of variables can be ascertained by operators.

10 CFR 50 Appendix A, 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.

10 CFR 50 Appendix A, GDC 20, "Protection System Functions," requires in part that the reactor protection system provide automatic initiation so that fuel design limits are not exceeded and so that accidents are sensed and mitigated. Both of these goals 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.

10 CFR 50 Appendix A, GDC 21, "Protection System Reliability and Testability," requires in part the high functional reliability of safety systems. Timely operation is necessary for high functional reliability of safety systems.

10 CFR 50 Appendix A, 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.

10 CFR 50 Appendix A, 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.

10 CFR 50 Appendix A, 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.

10 CFR 50 Appendix A, GDC 29, "Protection Against Anticipated Operational Occurrences," requires in part defense against anticipated operational transients to ensure an extremely high probability of accomplishing safety functions. To ensure this, the protection system must be demonstrated to operate within the time constraints of each anticipated operational transient.

2. Relevant Guidance

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," which is a system-level standard that contains some 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:

- Section 4.4 — limits, ranges, and rates of change of variables should be included in the documented design basis.
- Section 4.5 — minimum times should be specified for manual actions, below which such actions cannot be considered to be accomplished.
- Section 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.

In addition, timely automatic control action is required when events occur too quickly for operator intervention.

Reg. Guide 1.152, "Criteria for Power, Instrumentation, and Control Portions of Safety Systems," endorses the guidance of IEEE Std 7-4.3.2, "IEEE Standard for Digital Computers in Safety Systems of Nuclear Power

Generating Stations," as an acceptable method for complying with the NRC's regulations for safety systems that use digital computers. The main body of IEEE Std 7-4.3.2 does not add to the guidance of IEEE Std 603 regarding timing and performance. However, Annexes E and F, although not endorsed by Reg. Guide 1.152, contain useful guidance on certain timing and architectural requirements.

Annex E E.2.2.1(k) states that timing, response time, and performance requirements must be validated and verified.

E.2.2.8.2 states that sizing and timing analyses are suggested to assess the feasibility of meeting response time and performance requirements mentioned in E.2.2.1(k).

Annex F F.2.3.3(b) states that sizing and timing anomalies in requirements are considered abnormal conditions.

F.2.3.5(g) states that failure of code to run within timing and sizing constraints imposed by validated requirements is considered an abnormal condition.

Draft Reg. Guide DG-1045, proposed revision 3 to Reg. Guide 1.105, "Instrument Setpoints for Safety Systems," endorses ISA-S67.04, Part 1, "Setpoints for Nuclear Safety-Related Instrumentation Used in Nuclear Power Plants," as an acceptable method for initially setting and maintaining instrument calibrations in nuclear reactor I&C systems in order to ensure their proper response on demand. System time delays are an important consideration in establishing instrument setpoints.

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.

- 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 BTP HICB-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[1], 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, and topical reports or other applicant/licensee documentation. The SAR and referenced documents typically contain the architectural description, the 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.

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 the 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 Reactor Systems Branch (SRXB), Electrical Engineering Branch (EELB) and the Plant Systems Branch (SPLB) before accepting their use as a basis for timing requirements.

[1]In this context, using multiple processors means using separate computer systems assigned to separate functions or groups of functions. Shared-memory multiprocessors are not implied.

Digital Computer Timing Requirements

Digital computer timing should be shown to be consistent with the limiting response times and the characteristics of the computer hardware, software, and data communications systems. Computer system timing requirements that should be addressed in a software requirements specification are described in BTP HICB-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 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 (Annex E of IEEE Std 7-4.3.2) so that the entire system meets its timing requirements. See also Sections 2.2, 2.3.1, and 2.3.2 of NUREG/CR-6083, 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 BTP HICB-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.

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. Where 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 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 should be chosen by persons independent of the persons who designed the system.

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

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

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 (Annex E of IEEE Std 7-4.3.2, and Sections 2.1.3 and 2.1.4 of NUREG/CR-6083).

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 (Annex F of IEEE Std 7-4.3.2).

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 Part 52, or preliminary SARs or topical reports, the level of detail will typically include 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 inspections, tests, analyses and acceptance criteria (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 that 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 the latter two acceptance criteria groups, *performance verification* and *use of part-scale prototypes*.

C. References

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

Draft Regulatory Guide DG-1045. Proposed Revision 3 to Regulatory Guide 1.105, "Instrument Setpoints for Safety Systems." Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1997.

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."

ISA-S67.04-1994. "Setpoints for Nuclear Safety-Related Instrumentation Used in Nuclear Power Plants."

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

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

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, January 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.