NEW

Branch Technical Position HICB-16

Guidance on the Level of Detail Required for Design Certification Applications Under 10 CFR Part 52

A. Background

This branch technical position (BTP) identifies (1) the level of detail of the approach and (2) information the Staff needs in order to review digital computer-based instrumentation and control (I&C) systems for design certification in accordance with 10 CFR 52. This guidance supplements and modifies the guidance of Reg. Guide 1.70, "Standard Format and Content of Safety Analysis Reports for Nuclear Power Plants."

1. Regulatory Basis

10 CFR 52.47 requires in part that applications for design certification include the non-site-specific technical information required of applicants for construction permits and operating licenses by 10 CFR 50 and its appendices. The applicant shall also provide information regarding the TMI-related requirements (10 CFR 50.34(f)), the resolution of unresolved safety issues, the technical resolution of medium- and high-priority generic safety issues, a design-specific probabilistic risk assessment, and inspections, test, analyses, and acceptance criteria (ITAAC). The application shall contain a level of design information sufficient to enable the NRC staff to reach a final conclusion on all safety questions associated with the design, and to judge the applicant's proposed means of ensuring that construction conforms to the design.

The NRC staff's conclusions are documented in a safety evaluation report (SER) and a standardized design certification, which is a rule describing the certified design. However, incorporating all safety analysis report (SAR) material directly into the rule would prevent combined license (CL) applicants from incorporating advancements in technology and equipment into the plant when it is eventually built. Therefore, to maintain necessary flexibility in the detailed design, the SAR is composed of Tier 1, Tier 2, and Tier 2* material as defined below.

2. Definitions

The *design certification document (DCD)* is the master document that contains the information that is referenced by the design certification rule. The DCD includes both the Tier 1 information that is certified by the design certification rule and the Tier 2 information that is approved by and supports the rule. The DCD is composed of the certified design material and the non-proprietary version of the SAR, including all material incorporated by reference.

Tier 1 is the design-related information contained in the DCD that constitutes the certified standard design. This information identifies the scope of the standard design and consists of the certified design descriptions, the ITAAC, the site parameters, and the interface requirements. Tier 1 material becomes part of the design certification rule and may be changed only by rule-making.

Tier 2 consists of the remainder of the design-related information contained in the DCD. It supports the certification of a standard design by providing additional details about the proposed implementation. The Tier 2 information generally consists of the SAR with the proprietary information removed for purposes of rule-making. Although Tier 2 information is not certified by the design certification rule, it consists of "those matters resolved in connection with the issuance or renewal of a design certification" within the meaning of 10 CFR 52.63(a)(4). Tier 2 material is approved by the design certification rule, but is not part of the rule. Tier 2 material may be changed by a process similar to that described in 10 CFR 50.59, unless designated as Tier 2* in the SER.

*Tier 2** is a subset of Tier 2 material that the NRC SER and DCD for the standardized plant design approval identifies as requiring NRC approval prior to modification or change by the applicant/licensee.

Design acceptance criteria (DAC) are a set of prescribed limits, parameters, procedures, and attributes upon which the NRC relies in making a final safety determination to support design certification when detailed design information is not available. The DAC are part of the Tier 1 information. The DAC may be used to compensate for the lack of design detail in areas of rapidly changing technology where it would be detrimental to freeze design details many years before an actual plant is ready to be constructed. Computer-based I&C systems typically meet this criterion. The DAC are objective and are verified as a part of the ITAAC performed to demonstrate that the as-built facility conforms to the certified design. Using DAC will result in less detail about the design, but more detail regarding how the design will be accomplished. Conformance review points are specified for the Staff to assess the design development process at various stages of detailed design and subsequent construction and testing. The CL applicant is required to develop the procedures and test programs necessary to demonstrate that the DAC requirements are met at each conformance review point.

Certified design material (CDM) aggregates all Tier 1 material for reference by the design certification rule. It includes general provisions, ITAAC, certified design descriptions, interface requirements, and site parameters for the design.

3. Purpose

The purpose of this BTP is to provide guidance for NRC reviewers to verify that the previously cited regulatory basis and standards are met by a design certification applicant's submittal. This BTP has the following objectives:

- Confirm that the documentation that supports design certification applications contains sufficient information about I&C systems important to safety to support an evaluation of whether a plant constructed to the certified design can be operated without undue risk to the health and safety of the public.

- Confirm that appropriate design details and commitments are identified for certification and approval by the standard design certification rule (Tier 1 material).

- Confirm that appropriate design details supporting the standard design certification rule are identified in the SAR as unchangeable without NRC approval (Tier 2* material).

- Confirm that appropriate additional design details supporting the standard design certification rule are included in the SAR either directly or by reference (Tier 2 material).

B. Branch Technical Position

1. Introduction

During the review of design certification applications, the Staff developed a two-tier review approach to allow a CL applicant some flexibility in the implementation of a certified design. A variation of Tier 2 was also added (Tier 2*). (The development of Staff policy is discussed in a memorandum from W. T. Russell to B. A. Boger, et al.; Reg. Guide 1.152, "Criteria for Digital Computers in Safety Systems of Nuclear Power Plants;" SECY-90-241; SECY-90-377; SECY-92-053; SECY-92-087; and SECY-93-087.)

The use of DAC allows approval of fundamental design requirements and commitments to an effective detailed design process in lieu of detailed design information for design certification. ITAAC will be provided to verify that DAC have been satisfied. The ITAAC for the DAC will be performed by the CL applicant, and reviewed by the NRC throughout the design implementation and construction process. Refer to SRP Chapter 14 for guidance on ITAAC.

2. Information to be Reviewed

The information to be reviewed is the SAR (including information incorporated by reference), CDM, and detailed design information available for audit.

3. Acceptance Criteria

3.1 Content of Design Certification Applications

In addition to the material identified in Reg. Guide 1.70, the SAR should include the information described below. Detailed documentation that supports the summary information described below should be available for audit.

3.2 Section 7.1

In addition to the material identified by Reg. Guide 1.70, Section 7.1 should (1) describe the resolution of unresolved and generic safety issues applicable to the I&C systems, (2) describe the interface requirements to be met by portions of the plant for which the application does not seek certification and which are necessary to ensure proper functioning of the I&C systems, and (3) identify and describe the validation of innovative means of accomplishing I&C system safety functions. Furthermore, applications that propose the use of computers for systems important to safety should describe the computer system development process. Applications that propose the use of computers for reactor trip system (RTS) or engineered safety features actuation system (ESFAS) functions should also describe the design of the overall I&C systems with respect to defense-in-depth and diversity (D-in-D&D) requirements. Since the discussion of these topics will apply to several I&C systems, these topics will normally be located in Section 7.1. Details on the content expected in these discussions are described below.

Computer Development Process

The software and hardware development process used or planned for use to ensure that computer systems have the necessary quality and functionality should be discussed. This discussion should include a commitment to a design process compatible with that described in Reg. Guide 1.152 and BTP HICB-14.

Plans addressing the review topics described in Section B.2.1 of BTP HICB-14 should be available for review at the time of design certification. The process and acceptance criteria for qualifying predeveloped software (including tools) should be described.

For completed designs, documentation of development process implementation as described in Section B.2.2 of BTP HICB-14, and design output documents as described in Section B.2.3 of BTP HICB-14, should be available for inspection. An applicant may choose not to request design certification of a completed design, in which case the information described in Sections B.2.2 and B.2.3 of BTP HICB-14 will be unavailable. In such cases applicants may commit to DAC to compensate for the lack of design detail. In this case, the DAC will be accompanied by ITAAC proposed to demonstrate that the as-built system conforms to the certified design. Chapter 14 of the SRP describes the review of ITAAC submitted in conjunction with DAC.

The provisions to ensure that computer systems maintain necessary functional capability under conditions described in the SAR should be discussed. This discussion should include a description of design, analysis, and test techniques used or planned to be used, to ensure that computer systems will have acceptable real-time performance. BTP HICB-21 describes the review of real-time performance.

Defense-in-Depth and Diversity

Analyses should be provided to demonstrate compliance of the overall I&C system design with defense-in-depth and diversity guidance. BTP HICB-19 describes the characteristics of such analyses. Provisions for ensuring appropriate diversity should be described in the applicable section of the SAR. Primary backup systems should be described to a level of detail commensurate with that described below for Sections 7.2 and 7.3.

3.3 Section 7.2 through 7.7

A complete set of final system drawings may not be available for computer-based systems at the design certification stage. In this case, system-specific DAC may be substituted for the final system drawings requested by Reg. Guide 1.70.

Regardless of whether complete final system drawings or DAC are provided, the application should include a description of the overall system architecture and the functional block diagrams for each system. Additionally, system features provided to meet the requirements of 10 CFR 50.34(f) should be identified. The functional block diagrams should contain the information described below:

- Each block of the block diagram should represent a complete functional unit. That is, there should be inputs from an external source, such as instruments or other functional blocks, and outputs to external plant systems or equipment, such as actuators or other functional blocks.

- The relationship between the inputs and the outputs should be clearly and completely specified for each block.

- Allowable timing for each block should be specified.

- It should be possible to specify from these numbers the maximum allowable total cycle time of the system and the processing time from primary input to primary output.

- For multi-processor functional blocks, the method of communication between the processors of the block should be specified (e.g., shared memory).

- The inputs and outputs of each functional block may be binary signals (0/1), analog signals, or serial synchronous or asynchronous communication lines.

- The character of each signal line and its function and name should be completely described, with the exception that voltage and current levels need not be specified.

Computer-Based Systems

For computer-based systems, the application should describe the system characteristics that the self-diagnostics and on-line testing will detect to indicate computer system failures. The application should also describe the interconnections of test and diagnostics with the system functional hardware and software. Specific machine-dependent items that may not be available during design certification should be included in the DAC. Overall maximum system reaction time should be specified for each input from the sensor to major plant systems or equipment such as actuators or pump controllers (e.g., the plant control system).

The mechanisms available to modify software (including programming, calibration data, or configuration data) in the installed systems, either directly or via network connections, should be identified. Design provisions that enable applicants to prevent unauthorized changes should be described.

The material identified above should be discussed in sufficient detail to allow Staff determination that the applicant has met the requirements related to postulated single failures, common-mode failures, appropriate signal isolation (both electrical and logic isolation), and other aspects of the Staff's review as described in Appendices 7.1-A and 7.1-C.

3.4 Section 7.8

In addition to the systems described in Reg. Guide 1.70, advanced light-water reactors (ALWRs) should include systems to mitigate the consequences of anticipated transients without scram (ATWS).

Description

The SAR should describe the I&C systems provided for ATWS mitigation and their compliance with the ATWS rule, 10 CFR 50.62. For plants that have computer-based protection systems (RTS or ESFAS), Section 7.8 should discuss the systems provided specifically to comply with the defense-in-depth and diversity criteria. These systems include the hardwired backup controls and instrumentation credited for compliance with the manual means of component actuation, and any automatic systems provided specifically to achieve the necessary level of defense-in-depth and diversity. (See BTP HICB-19.)

Section 7.8 should include design basis information for the diverse actuation systems. The ATWS, hardwired displays and controls, and automatic diverse actuation systems may have different design bases. Section 4 of IEEE Std 603, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," outlines a set of design basis information that would be acceptable. Any supporting systems should be identified and described (reference may be made to other sections of the SAR).

Diverse I&C systems should be described to a level of detail commensurate with those described for Sections 7.2 and 7.3.

Analysis

Analysis should be provided to demonstrate how the requirements of 10 CFR 50.62, General Design Criteria 1, 13, and 19, applicable regulatory guides, and other appropriate criteria and standards are satisfied. For applications involving computer-based RTS or ESFAS, the analysis should also demonstrate that the design is consistent with the assumptions of the D-in-D&D analysis described above.

3.5 Section 7.9

I&C systems utilizing digital computers may also use data communication.

Description

The SAR should describe the data communication systems provided to support the I&C systems identified in Section 7.1. For data communication systems that support I&C functions in systems important to safety, Section 7.9 should provide the design basis information recommended by Section 4 of IEEE Std 603. Design basis requirements should also be provided for data communication systems that support other I&C functions identified in Section 4 of IEEE Std 603. IEEE Std 603 outlines a set of design basis information that would be acceptable for these systems. Any supporting systems should be identified and described (reference may be made to other sections of the SAR).

Final system drawings or DAC/ITAAC should be provided as described for the supported systems above. The DAC should describe the criteria that an acceptable design will meet for the following subjects, or the final design should address the following subjects:

- All data communication protocols used should be identified and described. This description should include discussion of error handling together with the method for dealing with the indeterminacy and extra traffic that error handling might engender.

- The provisions for bypassed or inoperable status should be described, along with the coordination of communication system bypass or inoperable status with the bypass and inoperable status of the safety system of which the communication system is part.

- Timing and data rate requirements should be included. Message formats and the approximate frequency at which each type of message appears on each data link should be included.

- The maximum traffic rate (messages per second and bytes per second) on each line should be specified, and the conditions under which these rates will occur should be identified.

- The method for establishing communication independence between redundant channels of a communication system and between safety and non-safety systems should be described.

Final system drawings may not be available at the design certification stage. In that case, the minimum set of information described above for Sections 7.2 through 7.7 will be acceptable for Section 7.9.

Analysis

Analysis of each data communication system should be provided to demonstrate that the requirements applicable to the I&C functions supported by the data communication systems are satisfied. For data

communication systems this analysis should demonstrate that the system design, including error handling performance, supports the timing and reliability requirements of the supported systems.

Data communication system failure modes should be identified, and the effect of these failures on supported systems should be analyzed. Such analysis may be incorporated into the failure mode and effects analysis of each supported system.

The immunity of the data communication system to design basis EMI/RFI should be demonstrated. This analysis should address both resistance to noise and prevention of fault propagation between redundant channels or systems.

For data communication systems that support RTS or ESFAS functions, the analysis should demonstrate that the design is consistent with the assumptions of the D-in-D&D analysis.

3.6 Standardized Safety Analysis Report

The Staff's safety determination for design certification of a standardized design is based upon the material in the SAR. To the extent that design detail or other information reviewed in the course of inspections or audits is necessary for the Staff to reach a safety conclusion, that design detail or other information should be available to the Staff. The design detail may be an amendment to or reference in the SAR.

3.7 Tier 1, Tier 2, and Tier 2 Material*

Material identified as Tier 1 should be that information necessary to ensure that significant features of the certified design application which the Staff is relying upon to make a safety determination are captured in the DCD. Two important factors should be balanced when identifying Tier 1 material:

- The safety significance of the design feature or commitment to the Staff's safety determination.

- The likelihood that the design feature or commitment will have to be changed in the future.

If the reviewer concludes that the details of a particular design feature or commitment are likely to change (the applicant may suggest such candidates), then it is appropriate to limit the amount of detail included in Tier 1. DAC that describe the necessary design acceptance criteria for such features should be provided in lieu of the design detail. Sufficient additional detail, however, should be specified in the SAR Tier 2 material in order for the Staff to make a final safety determination for certification. If the Staff believes these additional Tier 2 details are critical to the safety determination, they should be identified as Tier 2* material in the SER and DCD, thereby requiring prior NRC staff approval if changed.

For I&C systems, Tier 1 material consists of the certified design description, ITAAC, and interface requirements as defined in 10 CFR 52.47(a)(1)(ii) and (vii). The certified design description is composed of narrative descriptions and schematic drawings needed to describe the significant design features certified by the Staff.

Design details and commitments that are important to the NRC's safety determination, but are subject to change (e.g., technology advancement and standard revisions), should be identified as Tier 2* material in the SER and the DCD. For I&C systems, Tier 2* information will normally be limited to computer design, data communication design, setpoint methodology, commercial-grade item dedication, and equipment qualification, including electromagnetic compatibility.

4. Review Procedures

The reviewer should confirm early in the review that the basic types of information outlined above are available to support the review.

The review should confirm that the CDM contains an appropriate set of Tier 1 material, and that appropriate Tier 2* material is identified.

C. References

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

Memorandum from W. T. Russell to B. A. Boger, et al. "Reviewer Guidance for Design Certification Reviews — Certified Design Descriptions; Inspections, Tests, Analyses, and Acceptance Criteria (ITAAC); Applicant SAR Level of Detail; and Staff SER Documentation." December 28, 1992.

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 1.70. "Standard Format and Content of Safety Analysis Reports for Nuclear Power Plants." Office of Standards Development, U.S. Nuclear Regulatory Commission, November 1978.

SECY-90-241. "Level of Detail Required for Design Certification Under Part 52." July 11, 1990.

SECY-90-377. "Requirements for Design Certification under 10 CFR 52." November 8, 1990.

SECY-92-053. "Use of Design Acceptance Criteria During 10 CFR 52 Design Certification Reviews." February 19, 1992.

SECY-92-287. "Form and Content of a Design Certification Rule." August 18, 1992.

SECY-93-087. "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs." April 2, 1993.

Staff Requirements Memorandum on SECY-93-087. "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs." July 15, 1993.