**NUREG-0800**
(Formerly NUREG-75/087)

U.S. NUCLEAR REGULATORY COMMISSION

# STANDARD REVIEW PLAN

OFFICE OF NUCLEAR REACTOR REGULATION

## Section 7.7. Control Systems

**Review Responsibilities**

Primary — Instrumentation and Controls Branch (HICB)

Secondary — None

## I. Areas of Review

This SRP section describes the review process and acceptance criteria for those control systems used for normal operation that are not relied upon to perform safety functions following anticipated operational occurrences or accidents, but those that control plant processes having a significant impact on plant safety. These control systems are those systems that can, through normal operation, system failure or inadvertent operation, affect the performance of critical safety functions. Table 7.7-1 lists examples of control system functions that may be included in the scope of Section 7.7 for boiling water and pressurized water reactors. The actual list of system functions and systems included in the scope of Section 7.7 will be plant specific. A specific plant may not necessarily incorporate all of the functions listed in Table 7.7-1, may require functions beyond those listed in Table 7.7-1, or may group functions into systems differently than indicated in Table 7.7-1.

These systems are reviewed to ensure that they conform to the acceptance criteria and guidelines, that the controlled variables can be maintained within prescribed operating ranges, and that effects of operation or failure of these systems are bounded by the accident analyses in Chapter 15 of the SAR.

HICB also has secondary review responsibility for instrumentation and control systems which are reviewed by the Staff as part of the controlled system. These systems include I&C for support systems and plant

process systems. The acceptance criteria and review procedures of Section 7.7 are also applicable to these other I&C systems. Table 7.7-2 lists examples of control system functions for which HICB may have secondary review responsibility. Table 7.7-2 is not grouped according to plant type. The actual list of system functions and systems within the scope of HICB's secondary review responsibility will be plant-specific. A specific plant may not necessarily incorporate all of the functions listed in Table 7.7-2, may require functions beyond those listed in Table 7.7-2, or may group functions into systems differently than indicated in Table 7.7-2.

SRP Section 7.0 describes the coordination of reviews, including the information to be reviewed and the scope required for each of the different types of applications that the Office of Nuclear Reactor Regulation (NRR) may review. Refer to that section for information regarding how the areas of review are affected by the type of application under consideration and for a description of coordination between HICB and other branches.

In addition to the coordinated reviews discussed in SRP Section 7.0, the review of Section 7.7 should be coordinated with the Reactor Systems Branch (SRXB) and Plant Systems Branch (SPLB) to confirm the adequacy of control systems with respect to maintaining variables within operational limits during plant operation and to confirm that the impact of control system failures are appropriately included in the design basis accident analyses.

For those areas being reviewed as part of the primary review responsibility of other branches, the acceptance criteria necessary for the review, and their methods of application, are contained in the SRP sections identified in Appendix 7.1-A item 2.d.

## II. Acceptance Criteria

Acceptance criteria and guidelines applicable to control systems are identified in SRP Section 7.1. The review of Section 7.1 of the SAR confirms that the appropriate acceptance criteria and guidelines have been identified for these systems. The review of the control systems confirms that these systems conform to the requirements of the acceptance criteria and guidelines.

Acceptance criteria for the review of control systems are based on meeting the relevant requirements of the following regulations:

**1. Acceptance criteria applicable to any control systems**

10 CFR 50.55a(a)(1), "Quality Standards."

10 CFR 50.55a(h), "Protection Systems," requires compliance with ANSI/IEEE Std 279, "Criteria for Protection Systems for Nuclear Power Generating Stations." For control systems isolated from the protection system, the only applicable requirement from ANSI/IEEE Std 279 is item 4.7.2, "Isolation Devices."

10 CFR 50.34(f), "Additional TMI-Related Requirements," or equivalent TMI action plan requirements imposed by Generic Letters.

(2)(xxii), "Failure Mode and Effect Analysis of Integrated Control System" (applies only to B&W plants).

General Design Criterion 1, "Quality Standards and Records."

General Design Criterion 13, "Instrumentation and Control."

General Design Criterion 19, "Control Room."

General Design Criterion 24, "Separation of Protection and Control Systems."

Item II.Q, "Defense Against Common-Mode Failures in Digital Instrument and Control Systems," of the Staff Requirements Memorandum on SECY-93-087, "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs."

**2. Additional acceptance criteria applicable to control systems proposed for design certification under 10 CFR 52**

10 CFR 52.47(a)(1)(iv), "Resolution of Unresolved and Generic Safety Issues."

10 CFR 52.47(a)(1)(vi), "ITAAC in Design Certification Applications."

10 CFR 52.47(a)(1)(vii), "Interface Requirements."

10 CFR 52.47(a)(2), "Level of Detail."

**3. Additional acceptance criteria applicable to control systems proposed as part of combined license applications under 10 CFR 52**

10 CFR 52.79(c), "ITAAC in Combined Operating License Applications."

Section 7.1, Table 7-1 and Appendix 7.1-A list standards, regulatory guides, and branch technical positions that provide information, recommendations, and guidance that describe a basis acceptable to the NRC staff for implementing the relevant requirements of the NRC regulations identified above for control systems.

## III. Review Procedures

Section 7.1 describes the general procedures to be followed in reviewing any instrumentation and control system. This part of Section 7.7 highlights specific topics that should be emphasized in the control systems review.

The control systems review should address the applicable topics identified in Table 7-1. Appendix 7.1-A describes review methods for each topic. Major design considerations that should be emphasized in the review of the control systems are identified below.

- Design bases — The review should confirm that the control systems include the necessary features for manual and automatic control of process variables within prescribed normal operating limits.

- Safety classification — The review should confirm that the plant accident analysis in Chapter 15 of the SAR does not rely on the operability of any control system function to assure safety.

- Effects of control system operation upon accidents — The review should confirm that the safety analysis includes consideration of the effects of both control systems action and inaction in assessing the transient response of the plant for accidents and anticipated operational occurrences.

- Effects of control system failures — The review should confirm that the failure of any control system component or any auxiliary supporting system for control systems does not cause plant conditions more severe than those described in the analysis of anticipated operational occurrences in Chapter 15 of the SAR. This evaluation should address failure modes that can be associated with digital systems such as software design errors as well as random hardware failures. (The evaluation of multiple independent failures is not intended.)

- Effects of control system failures caused by accidents — The review should confirm that the consequential effects of anticipated operational occurrences and accidents do not lead to control systems failures that would result in consequences more severe than those described in the analysis in Chapter 15 of the SAR.

- Environmental control system — The review should confirm that I&C systems include environmental control as necessary to protect equipment from environmental extremes. This would include, for example, heat tracing of safety instruments and instrument sensing lines as discussed in Reg. Guide 1.151, "Instrument Sensing Lines" and cabinet cooling fans.

- Use of digital systems — To minimize the potential for control system failures that could challenge safety systems, control system software should be developed using a structured process similar to that applied to safety system software. Elements of the process may be tailored to account for the lower safety significance of control system software. Refer to Appendix 7.0-A for guidance on digital system review.

- Independence — The independence of safety system functions from the control system should be verified. See Appendix 7.1-B item 8 or Appendix 7.1-C item 24.

- Defense-in-depth and diversity — Control system elements credited in the Defense-in-Depth and Diversity Analysis (see BTP HICB-19) should be reviewed using the criteria for Diverse I&C systems described in Section 7.8.

- Potential for inadvertent actuation — The control systems design should limit the potential for inadvertent actuation and challenges to safety systems.

- Control of access — Physical and electronic access to digital computer-based control system software and data should be controlled to prevent changes by unauthorized personnel. Control should address access via network connections and via maintenance equipment.

In certain instances, it will be the Staff's judgment that, for a specific case under review, emphasis should be placed on specific aspects of the design, while other aspects of the design need not receive the same emphasis and in-depth review. Typical reasons for such a non-uniform emphasis are the introduction of new design features or the utilization in the design of features previously reviewed and found acceptable. However, in all cases, the review must be sufficient to conclude conformance to the acceptance criteria, i.e., the requirements of the NRC's regulations.

## IV. Evaluation Findings

The Staff verifies that sufficient information has been provided and the review supports the following conclusions as stated in the SER:

> The NRC staff concludes that the design of the control systems is acceptable and meet the relevant requirements of General Design Criteria (GDC) 1, 13, 19, and 24, and 10 CFR 50.34(f), 10 CFR 50.55a(a)(1), and 10 CFR 50.55a(h).
>
> The Staff conducted a review of these systems for conformance to the guidelines in the regulatory guides and industry codes and standards applicable to these systems. The Staff concluded that the applicant/licensee adequately classified and identified the guidelines applicable to these systems. The Staff finds that the control systems are appropriately designed and are of sufficient quality to minimize the potential for challenges to safety systems. Based upon the review of the system design for conformance to the guidelines, the Staff finds that there is reasonable assurance that the systems fully conform to the guidelines applicable to these systems. Therefore the Staff finds that the requirements of GDC 1 and 10 CFR 50.55a(a)(1) have been met.
>
> The Staff conducted a review of the plant transient response to normal load changes and anticipated operational occurrences such as reactor trip, turbine trip, upsets in the feedwater and steam bypass systems. The Staff concludes that the control systems are capable of maintaining system variables within prescribed operating limits. The applicant has also provided an environmental control system to protect safety instruments and instrument sensing lines from freezing. This system meets the guidelines of Reg. Guide 1.151, position 5; therefore, the Staff finds that the control systems satisfy this aspect of the requirements of GDC 13.
>
> The Staff review of control systems considered the features of these systems for both manual and automatic control of the process systems. The Staff finds that the features for manual and automatic control facilitate the capability to maintain plant variables within prescribed operating limits. The Staff finds that the control systems permit actions to be taken to operate the plant safely during normal operation, including anticipated operational occurrences, and therefore the control systems satisfy the requirements of GDC 19 with regard to normal plant operations.
>
> The control systems are appropriately isolated from safety systems. Therefore, the staff concludes that the isolation of these systems from safety systems satisfies the requirements of 10 CFR 50.55a(h) and the requirements of GDC 24.
>
> Based on the review of the applicant/licensee's defense-in-depth and diversity analysis and the quality of control system functions credited in this analysis, the Staff concludes that the control system complies with the criteria for defense against common-mode failure in digital

instrumentation and control systems. Therefore, the Staff finds that the control system functions credited as diverse means for performing safety functions satisfy the requirements of Item II.Q of the Staff Requirements Memorandum on SECY-93-087.

The Staff confirmed that the consequential effects of anticipated operational occurrences and accidents do not result in control system failures that would cause plant conditions more severe than those bounded by the analysis of the events.

The conclusions of the analysis of anticipated operational occurrences and accidents as presented in Chapter 15 of the SAR have been used to confirm that plant safety is not dependent upon the response of the control systems. The Staff also confirmed that failure of the control systems themselves or as a consequence of supporting system failures, such as loss of power sources, does not result in plant conditions more severe than those described in the analysis of design basis accidents and anticipated operational occurrences.

Note: the following findings apply only to applications under 10 CFR 52.

The control systems design appropriately addresses the applicable unresolved and generic safety issues. Therefore, the Staff finds that the control systems satisfy the requirements of 10 CFR 52.47(a)(1)(iv).

The review of the control systems examined the proposed inspections, tests, analyses, and acceptance criteria (ITAAC). Based upon the review and coordination with those having primary responsibility for ITAAC, the Staff concludes that if the inspections, tests, and analyses are performed and the acceptance criteria met, the plant will operate in accordance with the [design certification OR combined license]. Therefore, the Staff finds that the control systems satisfy the requirements of [10 CFR 52.47(a)(1)(vi) OR 10 CFR 52.79(c)].

The application for design certification does not seek certification for the following portions of the control system [insert list]. Based upon review of the completed safety analysis, the Staff finds that the requirements for these portions of the design were sufficiently detailed. Therefore, the Staff finds that the control system design satisfies the requirements of 10 CFR 52.47(a)(1)(vii).

Based upon an initial review of the scope and content of the material submitted by the applicant, and completed review with respect to the technical items above, the Staff finds that the application contained appropriate detail about the control systems design to satisfy the requirements of 10 CFR 52.47(a)(2).

Note: the following conclusion is applicable to all applications.

The conclusions noted above for the control systems are applicable to all portions of the systems except for the following, for which acceptance is based upon prior NRC review and approval as noted [List applicable system or topics and identify references].

# V. Implementation

Except in those cases in which the applicant/licensee proposes an acceptable alternative method for complying with specified portions of the NRC's regulations, the method described herein will be used by the NRC staff in its evaluation of conformance with NRC regulations.

## VI. References

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

Regulatory Guide 1.151. "Instrument Sensing Lines." Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1983.

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.

**Table 7.7-1. Examples of Control Systems Typically Included in Section 7.7**

| Boiling Water Reactor | Pressurized Water Reactor |
|---|---|
| Nuclear boiler control and instrumentation<br>Rod control<br>Rod position instrumentation<br>Neutron monitoring system<br>Recirculation flow control system<br>Pressure regulator and turbine generator control system<br>Feedwater control system<br>Internals vibration monitoring system<br>Acoustic leak monitoring system<br>Loose parts monitoring system<br>Process computer system<br>Safety system & sense line environmental control | Reactivity control system<br>Boron control system<br>Reactor power cutback system<br>Rod position instrumentation<br>In-core neutron monitoring system<br>Ex-core neutron monitoring system<br>Pressurizer pressure and level control system<br>Feedwater control system<br>In-core temperature monitoring system<br>Steam generator water level control system<br>Steam dump control system<br>Steam bypass control system<br>Internals vibration monitoring system<br>Acoustic leak monitoring system<br>Loose parts monitoring system<br>Process computer system<br>Safety system and sensing line environmental control |

**Table 7.7-2. Examples of Control Systems Typically Included in the Review of Other SAR Sections**

| | |
|---|---|
| Containment / drywell cooling system controls<br>Heating, ventilating, and air conditioning controls<br>Atmospheric control system controls<br>Reactor water cleanup system controls<br>Service water system controls<br>Chilled water system controls<br>Make-up water system controls<br>Instrument air system controls | Fire protection systems<br>Fire suppression system controls<br>Security systems<br>Spent fuel storage instrumentation and control<br>Gaseous radioactive waste system controls<br>Liquid radioactive waste system controls<br>Solid radioactive waste system controls |