ATTACHMENT 71111.21

INSPECTABLE AREA: Safety System Design and Performance Capability

CORNERSTONES: Mitigating Systems (90%)
Barrier Integrity (10%)

INSPECTION BASES: Inspection of safety system design and performance verifies the initial design and subsequent modifications and provides monitoring of the capability of the selected system to perform its design basis functions. As plants age, their design bases may be lost and an important design feature may be altered or disabled during a modification. The plant risk assessment model assumes capability of safety systems to perform its intended safety function successfully. This inspectable area verifies aspects of the Mitigating Systems and Barrier Integrity cornerstone for which there are no indicators to measure performance.

LEVEL OF EFFORT: Biennially review one or two risk-significant systems, or select a dominant accident sequence and review systems and components associated with that sequence.

71111.21-01 INSPECTION OBJECTIVE

To verify that design bases have been correctly implemented for the selected risk-significant system(s) to ensure that the system(s) can be relied upon to meet functional requirements.

71111.21-02 INSPECTION REQUIREMENTS

02.01 Inspection Preparation

a. System Selection. Select one or two risk-significant systems used for mitigating an accident or maintaining barrier integrity or select a dominant accident sequence and review systems and components associated with that sequence.

b. Component Selection. Select a sample of at least two significant components for in-depth inspection.

c. Obtain Information. Obtain necessary information for determining design and licensing basis functional requirements for the selected system(s).

02.02 Inspection Activities

a. Review System Needs. Select a sample of inspection attributes for review and verify that system needs are met. Selection of inspection attributes should focus on those attributes that are not fully demonstrated by testing, have not received recent in-depth NRC review, or are critical for the system function. The table below, "System Needs," is a listing of attributes that are needed for a system to perform its required function. During inspection preparation, identify which attributes are to be inspected. Perform the inspection activities associated with the selected attributes.

System Needs	
Attributes	**Inspection Activity**
Process Medium • water • air • electrical signal	Verify that process medium will be available and unimpeded during accident/event conditions. • Example: For an auxiliary feedwater system, verify that the alternate water source will be available under accident conditions.
Energy Source • electricity • steam • fuel + air • air	Verify energy sources, including those used for control functions, will be available and adequate during accident/event conditions • Example: For a diesel driven auxiliary feedwater pump, verify that diesel fuel is sufficient for the duration of the accident. • Example: For an air-operated pressurizer PORV, verify that either sufficient reservoir air will exist or instrument air will be available to support feed and bleed operation. • Example: For a standby DC battery, verify adequacy of battery capacity.
Controls • initiation actions • control actions • shutdown actions	Verify control system will be functional and provide desired control during accident/event conditions. • Example: For refueling water storage tank level instrumentation providing signal for suction swap-over to containment sump, verify that the setpoint established to ensure sufficient water inventory and prevent loss of required net positive suction head is acceptable.

System Needs	
Attributes	**Inspection Activity**
Operator Actions • initiation • monitoring • control • shutdown	Verify operating procedures (normal, abnormal, or emergency) are consistent with operator actions for accident/event conditions. • Example: If accident analyses assume containment fan coolers are running in slow speed, verify that procedures include checking of this requirement. • Example: If accident analyses assume that containment spray will be manually initiated within a certain time, verify that procedures ensure manual initiation within assumed time and that testing performed to validate the procedures was consistent with design basis assumptions. Verify instrumentation and alarms are available to operators for making necessary decisions. • Example: For swap-over from injection to recirculation, verify that alarms and level instrumentation provide operators with sufficient information to perform the task.
Heat Removal • cooling water • ventilation	Verify that heat will be adequately removed from system • Example: For an emergency diesel generator, verify heat removal through service water will be sufficient for extended operation.

b. Review System Condition and Capability. Verify that the system condition and tested capability is consistent with the design bases and is appropriate. The table below, “System Condition and Capability,” is a listing of applicable attributes that could be inspected. Perform the inspection activities associated with the selected attributes.

System Condition and Capability	
Attributes	**Inspection Activity**
Installed Configuration • elevations • flowpath components	Verify, by walkdown or other means, that system installed configuration will support system function under accident/event conditions • Example: Verify level or pressure instrumentation installation is consistent with instrument setpoint calculations. Verify that component configurations have been maintained to be consistent with design assumptions.
Operation	Verify that operation and system alignments are consistent with design and licensing basis assumptions • Example: For a containment spray system, verify emergency operating procedure changes have not impacted design assumptions and requirements. • Example: For a service water system, verify flow balancing will ensure adequate heat transfer to support accident mitigation.
Design • calculations • procedures	Verify that design bases and design assumptions have been appropriately translated into design calculations and procedures.
Testing • flowrate • pressure • temperature • voltage • current	Verify that acceptance criteria for tested parameters are supported by calculations or other engineering documents to ensure that design and licensing bases are met. • Example: Verify that flowrate acceptance criteria is correlated to the flowrate required under accident conditions with associated head losses, taking setpoint tolerances and instrument inaccuracies into account. Verify that individual tests and/or analyses validate integrated system operation under accident/event conditions. • Example: Verify that EDG sequencer testing properly simulates accident conditions and the equipment response is in accordance with design requirements.

c. Inspect Selected Components. From the table below, select and inspect attributes which are significant for the selected components.

Attributes	Component Inspection Activity
Component Degradation	Verify that potential degradation is monitored or prevented. • Example: For ice condensers, verify that inspection activities ensure air channels have been maintained consistent with design assumptions. Verify that component replacement is consistent with inservice/equipment qualification life. Verify that the numbers of cycles are appropriately tracked for operating cycle sensitive components.
Equipment/ Environmental Qualification • Temperature • Humidity • Radiation • Pressure • Voltage • Vibration	Verify that equipment qualification is suitable for the environment expected under all conditions. • Example: Verify equipment is qualified for room temperatures under accident conditions.
Equipment Protection • fire • flood • missile • high energy line break • HVAC • freezing	Verify equipment is adequately protected. • Example: Verify freeze protection adequate for CST level instrumentation. • Example: Verify that conditions and modifications identified by the licensee's high energy line break analysis have been implemented.
Component Inputs/Outputs	Verify that component inputs and outputs are suitable for application and will be acceptable under accident/event conditions. • Example: Verify that valve fails in the safe configuration. • Example: Verify that required inputs to components, such as coolant flow, electrical voltage, and control air necessary for proper component operation are provided.

Attributes	Component Inspection Activity
Operating Experience	Verify that applicable insights from operating experience have been applied to the selected components. • Example: Verify that component functioned appropriately when challenged during transients.

02.03 Identification and Resolution of Problems. Verify that the licensee is identifying design issues at an appropriate threshold and entering them in the corrective action program. As it relates to design issues, select a sample of problems in the selected system(s) and other risk-significant systems documented by the licensee, and verify effectiveness of corrective actions. See Inspection Procedure 71152, "Identification and Resolution of Problems," for additional guidance.

71111.21-03 INSPECTION GUIDANCE

03.01 General Guidance on System and Component Selection

a. System Selection. Consider the following guidance for system selection. Consult the regional SRA and the SRI for plant specific information. System selection should focus on:

1. Systems with high probabilistic risk analysis (PRA) rankings and high values for importance measures, such as risk achievement worth(RAW)and risk reduction ratio (RRR).

2. Systems with design attributes which are not fully demonstrated through testing.

3. Systems which have had significant modifications, changes to design bases, and operating procedure changes.

4. Systems which have not received recent NRC review.

5. Systems which have multiple maintenance rule functions or which support multiple systems.

6. If more than one system is selected, the systems should complement each other, such as in mitigating the same type of accident. For small break LOCAs (PWRs), the important systems could be high head safety injection and residual heat removal. For station blackout (BWRs), the important systems could be the 125 VDC system and the automatic depressurization system. The system(s) selected should be from the dominant accident sequences for core damage frequency (CDF).

7. Systems contained in the NRC risk-informed inspection notebook for the plant.

The following table provides additional guidance and examples.

Cornerstone	Inspection Objective	Risk Priority	Examples
Mitigating Systems Barrier Integrity	Verify system design bases have been maintained. Verify system availability, reliability, and functional capability has been maintained. Verify that safety margins have been maintained. Verify that defense-in-depth philosophy has been maintained.	Design and functional capability of components that are not validated by in-plant testing Emphasis on changes to design bases and normal and emergency procedures Risk significant design features and assumptions not reviewed previously	Residual Heat Removal Auxiliary Feedwater RCIC CCW Service Water EDGs DC Power Containment Isolation RCS/RHR Boundary

b. Component Selection. Component selection should focus on the following:

1. Components whose failure will result in loss of system or train function.

2. Components which support multiple systems or trains.

3. Components with risk significant design features which are not validated by testing.

4. Passive as well as active components.

5. Components which have safety/non-safety related interfaces.

c. Using Probabilistic Analyses to Select Risk-Significant Systems and Components

1. RAW indicates the CDF increase if a component or system is unavailable typically for a year; a RAW of 2 indicates a doubling of the baseline CDF.. RRR measures the amount by which the CDF decreases if a component or system was always available. Multiple importance measures should be considered. RAW and RRR provide insights regarding the significance of design problems in the systems selected.

2. Altering a PRA for inclusion of a design flaw could change the dominant accident sequences so that different systems become more risk-significant. The use of dominant accident sequences in PRAs to select systems and components may be appropriate for SSCs that are more significant to LERF than CDF; external events (e.g., floods) than internal events (e.g., LOCAs); or risk during shutdown than during normal operation.

3. Inspectors may select a dominant accident sequence and review systems and components associated with that sequence. PRAs generate combinations of initiating events and equipment failures that lead to core damage. The frequency of the dominant sequences that lead to core damage are generally provided in the PRAs. Systems and components that are most significant for mitigating accidents are generally included in these sequences. Another good source for the significance of core damage sequences is the ROP SDP notebooks for each plant. The sequences that have a higher initiating event frequency with the least amount of mitigating equipment are generally safety significant.

4. Since PRAs do not explicitly model design flaws, there is no mathematical technique for extracting a risk ranking of unknown design flaws. However, PRAs can focus inspection activities in areas where design findings have a greater chance of being safety significant. In addition to risk insights from internal events, inspectors should consider impacts on containment performance (LERF) and external events (fire, seismic, flood).

d. Sources of Information. The following table shows the suggested sources of information necessary to perform this inspection.

System Information	Suggested Sources
Design Bases	Updated Final Safety Analysis Report (UFSAR) Design Basis Documentation System Descriptions Design Calculations Design Analyses Piping & Instrumentation Drawings Significant Design Drawings Significant Surveillance Procedures Pre-operational Test Documents Vendor Manuals
Licensing Bases	NRC Regulations Plant Technical Specifications UFSAR NRC Safety Evaluation Reports

System Information	Suggested Sources
Applicable Accidents/Events	UFSAR Individual Plant Examination PRA analyses Emergency Operating Procedures (EOPs)
System Changes	System Modification Packages (including post modification test documents) 10 CFR 50.59 Safety Evaluations Temporary Modifications Work Requests Setpoint Changes EOP Changes
Industry Experience	Licensee Event Reports Bulletins Information Notices
PRA Information	Individual Plant Examinations (IPE) or Updated PRA model results Risk-informed inspection notebooks Risk importance rankings for SSCs Dominant accident sequences Important operator actions Individual Plant Examinations for External Events

Based on the information obtained, inspectors should be able to identify:

1. System flowpaths
2. Safety feature actuation signals
3. Applicable accident scenarios
4. Failure modes
5. System alignment during accident mitigation
6. System interfaces and interactions
7. Safety interlocks
8. Functional requirements for active components during abnormal/ accident conditions
9. Operator actions required to support system functions
10. Modifications made to the system that could have potentially changed the licensing and/or design bases

03.02 General Design Inspection Guidance

a. Walkdowns. During the walkdown of the selected system(s), inspectors should consider the following questions:

1. Is the installed system consistent with the piping and instrument diagram?

2. Will equipment and instrumentation elevations support the design function?

3. Has adequate sloping of piping and instrument tubing been provided?

4. Are required equipment protection barriers (such as walls) and systems (such as freeze protection) in place and intact?

5. Does the location of the equipment make it susceptible to flooding, fire, high energy line breaks, or other environmental concerns?

6. Has adequate physical separation/electrical isolation been provided?

7. Are there any non-seismic structures, systems, and components (SSCs) surrounding the system which require evaluation for impact upon the system?

8. Does the location of equipment facilitate manual operator action, if required?

9. Are baseplates, hangers, and struts installed properly?

10. Are their indications of degradations of SSCs?

b. Design Review. The purpose of the design inspection is to verify that the system(s) will function as required. In the process of reviewing the design, inspectors should verify the appropriateness of design assumptions, boundary conditions, and models. Independent calculations by the inspectors may be required to verify appropriateness of the licensee's analysis methods. The interfaces between safety related and non-safety related systems should also be reviewed.

In reviewing the functional adequacy of the selected system(s), the inspectors should determine whether the design basis is met by the installed and tested configuration. The inspectors should understand not only the original purpose of the design but the manner and conditions under which the system will actually be required to function during transients and accidents. For example, if UFSAR information was used as inputs for design or procedures, these inputs should be verified to be consistent with the design bases.

During the design review, inspectors should consider the following questions:

Valves

1. Are the permissive interlocks appropriate?

2. Will the valve function at the pressures that will exist during transient/accident conditions?

3. Will the control and indication power supply be adequate for system function?

4. Is the control logic consistent with the system functional requirements?

6. What manual actions are required to back up and/or correct a degraded function?

Pumps

7. Is the pump capable of supplying required flow at required pressures under transient/accident conditions?

8. Is adequate net positive suction head (NPSH) available under all operating conditions?

9 Is the permissive interlock and control logic appropriate for the system function?

10. Is the pump control adequately designed for automatic operation?

11. When manual control is required, do the operating procedures appropriately describe necessary operator actions?

12. What manual actions are required to back up and/or correct a degraded function?

13. Has the motive power required for the pump during transient/accident conditions been correctly estimated and included in the normal and emergency power supplies?

14. Do vendor data and specifications support sustained operations at low flow rates?

15. Is the design and quality of bearing and seal cooling systems acceptable?

Instrumentation

16. Are the required plant parameters used as inputs to the initiation and control system?

17. If operator intervention is required in certain scenarios, have appropriate alarms and indications been provided?

18. Are the range, accuracy, and setpoint of instrumentation adequate?

19. Are the specified surveillance and calibrations of such instrumentation acceptable?

Circuit Breakers and Fuses

20. Is the breaker control logic adequate to fulfill the functional requirements?

21. Is the short circuit rating in accordance with the short circuit duty?

22. Are the breakers and fuses properly rated for the load current capability?

23. Are breakers and fuses properly rated for DC operation?

Cables

24. Are cables rated to handle full load at the environments temperature expected?

25. Are cables properly rated for short circuit capability?

26. Are cables properly rated for voltage requirements for the loads?

Electrical Loads

27. Have electrical loads been analyzed to function properly under the expected lowest and highest voltage conditions?

28. Have loads been analyzed for their inrush and full load currents?

29. Have loads been analyzed for their electrical protection requirements?

As-built System

30. Are service water flow capacities sufficient with the minimum number of pumps available under accident conditions?

31. Have modified equipment components falling under the scope of 10 CFR 50.49 been thoroughly evaluated for environmental equipment qualifications considerations such as temperature, radiation, and humidity?

32. Are the modifications to the system consistent with the original design and licensing bases?

71111.21-04 RESOURCE ESTIMATE

This inspection procedure is estimated to take an average of 475 hours at a one-unit site and 500 hours at multi-unit sites.

The inspection team should be multi-disciplinary with expertise relevant to the system(s) being reviewed. Preferably, an inspection team would include individuals with design experience in mechanical engineering, electrical engineering, and instrumentation and controls. If the system(s) selected for review require significant operator actions, consideration should also to given to including an individual with an operations background.

71111.21-05 COMPLETION STATUS

Inspection of the minimum sample size will constitute completion of this procedure in the RPS. That minimum sample size consists of one or two safety system reviews, or systems and components associated with a dominant accident sequence, regardless of the number of units at the site.

71111.21-06 REFERENCES

Inspection Procedure 71152, “Identification and Resolution of Problems.”

END