NUREG-0800

DRAFT 17 (02/13/09)

U.S. NUCLEAR REGULATORY COMMISSION

STANDARD REVIEW PLAN

BRANCH TECHNICAL POSITION 18-1
GUIDANCE FOR THE EVALUATION OF MINIMUM INVENTORY OF ALARMS, CONTROLS, AND DISPLAYS FOR NEW LIGHT WATER REACTOR PLANT DESIGNS

The following Branch Technical Position is to be cited as the acceptance criteria for the minimum inventory of controls, displays, and alarms in Revision 2 (March, 2007) of the Standard Review Plan (SRP) Chapter 18. Section II. A. 7. SRP Acceptance Criteria, "A minimum inventory of controls, displays, and alarms," for those design certification applicants that have not been certified prior to the date of this Branch Technical Position.

BRANCH TECHNICAL POSITION 18-1
GUIDANCE FOR THE EVALUATION OF MINIMUM INVENTORY OF ALARMS, CONTROLS, AND DISPLAYS FOR NEW LIGHT WATER REACTOR PLANT DESIGNS

Review Responsibilities

Primary - Organization responsible for the review of human factors engineering
Secondary – Organization responsible for the review instrumentation and controls

A. BACKGROUND

The concept of minimum inventory originated as part of the NRC's general resolution of the level of control room design detail to be provided by design certification applicants as stated in SECY 92-053, "Use of Design Acceptance Criteria During 10 CFR Part 52 Design Certification Reviews." The minimum inventory contributes to assuring that the staff has sufficient information available to make a safety determination at the time of design certification. Another important contributor to the need for minimum inventory is the potential for common-cause failures of computer-based human system interfaces

(HSIs)[1]. If there is a loss or degradation of the computer-based, normally-used HSIs[2] in the main control room (MCR) or if evacuation of the MCR becomes necessary, alternative HSIs are needed to ensure the reactor can be shutdown safely and maintained in a safe condition.

1. Regulatory Basis
   TBD
2. Relevant Guidance
   TBD
3. Purpose
   TBD

B BRANCH TECHNICAL POSITION

1. Introduction
   TBD

2. Definitions

The MCR minimum inventory is that set of MCR alarms, controls, and displays (i.e., the HSIs) needed by operators to bring the reactor to a safe shutdown condition and maintain it in a safe shutdown condition when there is a loss or degradation of normally-used HSIs.

The RSF minimum inventory is that set of remote shutdown (RSF) HSIs needed by operators upon MCR evacuation for prompt hot shutdown of the reactor, to maintain the unit in a safe condition during hot shutdown, and for the potential capability of subsequent cold shutdown of the reactor.

3. Information To Be Reviewed
   TBD
4. Acceptance Criteria

General:

1. A minimum inventory of HSIs should be developed for the MCR, for use when there is a loss or degradation of normally-used HSIs, that includes the HSIs that the operator needs to:

   A. perform those credited manual actions necessary to bring the reactor to a safe shutdown condition and maintain it in a safe shutdown condition

---

[1] The term "human-system interfaces," in the context of defining minimum inventory, is limited to alarms, controls, and displays. The term is not used in a broader sense as has been used, for example, in NUREGs-0700 and 0711.

[2] These designs use non-safety, computer-driven alarms, controls, and displays as the instruments operators normally use to control and monitor the plant from the MCR. These are referred to as "normally-used human-system interfaces (HSIs)."

B. monitor safety functions, accident monitoring displays, and automatic success paths needed by operators to bring the reactor to a safe shutdown condition and maintain it in a safe shutdown condition

C. perform manual actions credited in the applicant's diversity and defense-in-depth (D3) evaluation needed by operators to bring the reactor to a safe shutdown condition and maintain it in a safe shutdown condition

D. perform manual actions determined to be risk-important by the applicant's probabilistic risk assessment (PRA) and needed by operators to bring the reactor to a safe shutdown condition and maintain it in a safe shutdown condition

2. A minimum inventory of HSIs should be developed for the RSF that includes the HSIs that the operator needs to safely shut down the reactor upon control room evacuation using those HSIs needed "for prompt hot shutdown of the reactor, including necessary instrumentation and controls to maintain the unit in a safe condition during hot shutdown, and [(2)] with a potential capability for subsequent cold shutdown of the reactor through the use of suitable procedures" (10 CFR 50, Appendix A, "*General Design Criterion 19, Control Room").*

Design Certification Applicants:

1. Applicants for new plant design certification should include the following with the Design Control Document (DCD) Tier 1 information:

A. A description of the process used to develop the MCR and RSF minimum inventories of HSIs. The description should address each of the process steps below and the application of the Minimum Inventory HSI Development Criteria Matrix provided in Appendix 18.A. The description should identify the sources of information that were used during the development process and how each was used to comprehensively identify all of the functions and tasks and the associated HSIs needed for operators to bring the reactor to a safe shutdown condition and maintain it in a safe shutdown condition when there is a loss or degradation of normally-used HSIs or evacuation of the MCR. Specifically the description should address:

I. how operator actions credited in the safety analysis for safety success paths were identified,

II. how the generic technical guidelines, design-specific guidelines for developing emergency operating procedures, or plant-specific emergency operating procedures (if available) were used to develop the minimum inventory,

III. how the initial plant system design was considered in the development of the minimum inventory,

IV. how predecessor designs were used to develop the minimum inventory

V. how the concept of operations for conditions of degraded

or failed normally-used HSIs was considered in the development of the minimum inventory,

VI. how the results of a failure modes analysis for the normally used HSIs were considered in the development of minimum inventory,

VII. how function and task analyses (or surrogate based on either an applicable predecessor plant design or an abbreviated, high-level, design-specific task analysis) that describe the operator actions necessary to bring the reactor to and maintain it in a safe shutdown condition when the normally-used MCR HSIs are lost or degraded because of evacuation of the MCR, were used to develop the minimum inventory,

VIII. how the applicant's PRA was used to identify operator actions or tasks that are risk important and necessary for achieving and maintaining safe shutdown conditions after a loss or degradation of normally-used HSIs, and

ITAAC for the MCR and RSF minimum inventories of HSIs describing that:

I. the process approved by the NRC in the Design Control Rule (DCR) for developing the MCR and RSF minimum inventories of HSIs was applied,

II. a results summary report exists and demonstrates that the MCR and RSF minimum inventories were developed in accordance with the process approved by the NRC in the DCR and,

III. the as-built MCR and RSF contain the minimum inventories of HSIs developed from implementing the process approved by the NRC in the DCR.

2. Applicants for new plant design certification should include with the DCD Tier 2* information:

   A. The MCR minimum inventory of HSIs that was derived from implementing the NRC-approved process.
   B. The RSF minimum inventory of HSIs that was derived from implementing the NRC-approved process.

Appendix 18.B provides a recommended format that may be used to identify the MCR and RSF minimum inventories.

Combined License (COL) Applicants:

1. COL applicants should include in their application, a description of how they determined the applicability of the minimum inventory contained in the certified DCD to their plant:

   A. COL applicants should provide the basis for any information sources that differ from the sources used by the certified design applicant.

B. COL applicants should provide the bases for site-specific differences from the MCR and RSF Tier 2* minimum inventories of the certified design applicant prior to license issuance. The COL MCR and RSF minimum inventories should be provided to the NRC in accordance with the requirements in 10 CFR 52.99 and using the format provided in Appendix 18.B.

2. COL applicants should describe their process to verify and document that, for their site-specific MCR and RSF minimum inventories:

   A. the NRC-approved process for developing the MCR and RSF minimum inventories of HSIs was applied,
   B. a results summary report exists and demonstrates that the MCR and RSF minimum inventories were developed in accordance with the NRC-approved process and,
   C. the as-built MCR and RSF contain the minimum inventories of HSIs developed from implementing the NRC-approved process.

5. Review Procedures

The staff's review and approval of both the design certification and COL applicants' MCR and RSF minimum inventories of HSIs will be multi-disciplinary. In addition to the acceptance criteria for minimum inventory, to determine the acceptability of the applicant's minimum inventory of HSIs, the staff should use applicable guidance from source materials such as "Human Factors Engineering Program Review Model" (NUREG-0711, Rev. 2), "Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants" (Regulatory Guide 1.97, Rev. 4), and Chapter 14.3.9 "Human Factors Engineering – Inspections, Tests, Analyses, and Acceptance Criteria" of NUREG-0800.

C. REFERENCES

1. NRC (2006). Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants (Regulatory Guide 1.97, Rev. 4). Washington, D.C.: U.S. Nuclear Regulatory Commission.
2. NRC (2004). Human Factors Engineering Program Review Model (NUREG-0711, Rev. 2). Washington, D.C.: U.S. Nuclear Regulatory Commission.
3. NRC (1992). Use of Design Acceptance Criteria During 10 CFR Part 52 Design Certification Process (SECY 92-053). Washington, D.C.: U.S. Nuclear Regulatory Commission.
4. Institute of Electrical and Electronics Engineers (1991). IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations (IEEE Std. 603-1991). New York: Institute of Electrical and Electronics Engineers.
5. RC (2002). Human-System Interface Design Review Guidelines (NUREG-0700, Rev. 2). Washington, D.C.: U.S. Nuclear Regulatory Commission.
6. NRC (1993). Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs (SECY 93-087). Washington, D.C.: U.S. Nuclear Regulatory Commission.

Appendix 18 A
Minimum Inventory HSI Development Criteria Matrix

Functions/Tasks (F/T) and Associated HSIs	Minimum HSI Accessibility Criteria[1]	Applicable Regulatory Requirements and NRC and Industry Guidance[2]
1. Perform credited manual actions to bring the reactor to a safe shutdown condition and maintain it in a safe shutdown condition		
Alarms needed to prompt action (without additional diagnosis)	SD-CV for at least one channel SD-SR for other channel	SRM to SECY-93-087[3] NUREG-0800 (SRP) Section 7.5 (III.1.O)[3]
"Type A" alarms	SD-CV for at least one channel SD-SR for other channel	Reg. Guide 1.97 Rev. 4 (Type A)
Pre-action support displays (e.g., displays required to confirm the need for action, evaluate conditions prior to taking action, or define/plan the specific action)	SD-CV for at least one channel SD-OSA for other channel	IEEE 603 (§5.8.1, §5.8.4)
	SD-CV for at least one channel SD-OSA for other channel	Reg. Guide 1.97 Rev. 4 (Type A)
Controls & immediate feedback displays	SD-CV SD-OSA is acceptable if supported by appropriate HFE analyses	IEEE 603 (§6.2)
Performance alarms	SD-SR	None
Performance displays	SD-SR	None
2. Monitor safety functions, accident monitoring displays, and automatic success paths needed by operators to bring the reactor to a safe shutdown condition and maintain it in a safe shutdown condition		
Displays of the status of critical safety functions	SD-CV for at least one channel SD-OSA for the other channel	Reg. Guide 1.97 Rev. 4 (Type B)
Alarms indicating challenges to critical safety functions	SD-CV	NUREG 0700
Displays of the status of fission product barriers	SD-OSA	Reg. Guide 1.97 Rev. 4 (Type C)
Displays of safety system performance	SD-OSA	Reg. Guide 1.97 Rev. 4 (Type D)
Alarms on fission product barriers and safety system performance	SD-SR	None
Displays of the magnitude of the release of radioactive materials	SD-OSA	Reg. Guide 1.97 Rev. 4 (Type E)

Functions/Tasks (F/T) and Associated HSIs	Minimum HSI Accessibility Criteria[1]	Applicable Regulatory Requirements and NRC and Industry Guidance[2]
Manual system-level actuation controls	SD-CV SD-OSA is acceptable if supported by appropriate HFE analyses	Reg. Guide 1.62 IEEE 603 (§6.2a)
3. Perform manual actions credited in the D3 evaluation needed by operators to bring the reactor to a safe shutdown condition and maintain it in a safe shutdown condition		
Prompting alarms	SD-SR	BTP 7-19, Points 1-3
Pre-action support displays	As determined by appropriate HFE analysis	
Manual controls		
Safety function alarms	SD-SR	BTP 7-19, Point 4
Safety function indications displays	SD-OSA	
Manual controls for system level actuations	SD-OSA	
4. Perform manual actions determined to be risk-important based on the plant-specific PRA and needed by operators to bring the reactor to a safe shutdown condition and maintain it in a safe shutdown condition		
Controls and displays needed in the main control room to support the identified risk-important operator actions (not already covered in 1- 3 above)	SD-OSA (Some may be SDCV, depending on HFE evaluations, which consider the task being performed and how time-critical the task is)	SECY-93-087
Alarms needed in the main control room to support the identified risk-important operator actions (not already covered in 1- 3 above)	SD-SR (Some may be SDCV, depending on HFE evaluations, which consider the task being performed and how time-critical the task is)	SECY-93-087
5. Perform manual actions for prompt hot shutdown of the reactor, and, maintaining the unit in a safe condition during hot shutdown, and subsequent cold shutdown of the reactor.		
Controls and displays needed to reach and maintain safe shutdown in the event of control room evacuation	SD-OSA	NUREG 0800 (SRP) Section 7.4.III.1.D ANSI/ANS-58.6
Alarms needed to reach and maintain safe shutdown in the event of control room evacuation	SD-SR	NUREG 0800 (SRP) Section 7.4.III.1.D ANSI/ANS-58.6

Notes:

[1] This column specifies the amount of effort required by the user to access a specific HSI resource. It is meant to identify minimum criteria. For example, if something is listed as SD-OSA or SD-SR in the column, it could be implemented as SD-CV (i.e., more accessible) and that would be acceptable.

SD (Spatially Dedicated) means that the HSI always appears in the same fixed location.

CV (Continuously Visible) means that the HSI is always visible. For an alarm it would be visible at all times whether in an alarmed or a cleared state.

SR (Self Revealing)) means that the HSI would automatically become visible when needed without the need for an operator action for it to become visible. For an alarm it would be visible only when in an alarmed state.

OSA (One-Step Accessible) means that the HSI would become visible by a single operator action.

[2] This column identifies regulatory and industry guidance documents related to the accessibility criteria

[3] The SRM to SECY-93-087 states that alarms for manual actions required for the safety systems to accomplish their safety functions in Advanced Light Water Reactors (ALWRs) should meet 1E requirements. NUREG-0800 (SRP) Section 7.5 (III.1) has similar provisions.

Appendix 18 B
Minimum Inventory Format

(For MCR and RSF)

Parameter Description ***(e.g., Containment Pressure)***	***Functions/Tasks (F/T)*** **(e.g., Perform credited manual actions to bring the reactor to a safe shutdown condition…)**	***Minimum HSI Accessibility Criteria***	***Alarm***	***Control***	***Display***	***Applicable Regulatory/*** ***Industry Requirements/*** ***Guidance***