DRAFT-jb-r3jjp
2007
INTERIM STAFF GUIDANCE

MINIMUM INVENTORY OF HUMAN SYSTEM INTERFACES (ALARMS, CONTROLS, AND DISPLAYS)

Background:

Origin of Minimum Inventory

As stated in SECY 92-053, "to resolve the difficulties being experienced in obtaining detailed design information for selected areas of the plant…" for design certification reviews, the staff developed a two-part approach to review the man/machine *[human-system interface (HSI)]* aspects of the control room design.

The first part of the approach was "a detailed review to establish the minimum inventory of fixed alarms, displays, and controls necessary for the operators to the implement emergency operating procedures and to carry out those human actions shown to be important from the applicant's PRA *[probabilistic risk assessment]*. This minimum inventory will be included in the design certification."

(The second part of the staff's approach was to develop Design Acceptance Criteria (DAC) to ensure the applicant for design certification commits to implement a systematic approach to the design of HSIs in its plant design development process and is not discussed in this interim guidance document.)

Purpose of Minimum Inventory

The purpose of a minimum inventory (MI) is to provide defense-in-depth approach to protection against a common cause failure (CCF) that renders the plant's primary HSIs in the control room (e.g., networked digital control and information system-driven) inoperable by designating a minimum set of fixed alarms, displays and controls needed to the implement emergency operating procedures and to carry out important human actions identified in the applicant's PRA .

Definition of Minimum Inventory

The minimum inventory is the set of spatially-dedicated HSIs (i.e., alarms, controls, and displays) that are readily accessible to the operators, needed to handle potential failures of the primary control room HSIs, and are electronically diverse from the primary control system. These HSIs are in addition to the primary workstations HSIs that are non-safety equipment and rely on selectable HSIs (i.e., the operator must select the particular display

or control screen needed to support a given task). The MI includes safety-related HSIs that meet regulatory requirements for accident mitigation and safe shutdown.

Minimum Inventory Development Process and Acceptance Criteria:

Development Process

In developing its minimum inventory, the applicant provides the following information as Tier 1 level information submitted for design certification:

A. a description of:

    1. the process for developing the minimum inventory of alarms, controls, and displays
    2. the selection criteria for determining the minimum inventory

B. ITAAC to verify that reports exist that describe how:

    1. the process for developing the inventory was implemented
    2. the selection criteria for determining the minimum inventory were applied
    3. the minimum inventory was validated using a full-scope simulator that meets:
        i. The guidance in ANSI/ANS 3.5, "Nuclear Power Plant Simulators for Use in Operator Training," and
        ii. The description in SECY 93-087 for a fully functional, integrated control room prototype to demonstrate, prior to fuel load, that functions and tasks are as the basis for the human-system interface design
    4. the as-built control room was evaluated to assure that it contains the minimum inventory identified through implementing the Tier 1 process and selection criteria

In developing its minimum inventory, the applicant provides the following information as Tier 2* level information submitted for design certification:

A. alarms, controls, and displays required to accomplish each of the GTG (Owners Groups' Generic Technical Guidelines) steps
B. the GTGs and supporting documentation (e.g., step description and basis documents)
C. a list of alarms, controls, displays which includes:

    a. dedicated controls for manual safety system actuation (e.g., reactor trip, turbine trip, engineered safety feature actuation)
    b. Regulatory Guide 1.97 Type A and Category I variables for plants committed to Revision 3 or Type A, B, and C variables for plants

committed to Revision 4 (The complete list may be revised as the design matures)

c. alarms, controls, displays required to support important operator actions specified as a result of the design's PRA/HRA
d. task analysis of operator actions needed to safely shutdown the reactor under conditions where the operators' primary, instrumentation has failed
e. alarms to alert the operator to perform safety functions in response to design-basis events for which there is no automatically actuated safety function
f. dedicated controls for operator actions credited for diversity and defense-in-depth

The staff review of an applicant's minimum inventory will be multi-disciplinary: consisting of inputs from human factors engineering; instrumentation and control engineering; risk assessment; and plant, reactor, and electrical engineering.

The staff reviw should also consider the possibility for failures of the primary HSIs during normal plant operation. The nature and extent of failures that can occur, how often they may occur over the life of the plant, and their potential duration will guide decisions on what alternate or backup capability are provided beyond the safety-related HSIs already required by regulation. The extent of backup HSI capability needed will depend on the applicant's concept of operations for these situations – that is, how the operators will respond to loss of the normal HSIs, and what operational capabilities are desired for these failed or degraded conditions.

Acceptance Criteria

For the minimum inventory to be satisfactory, the staff will determine that the following acceptance criteria have been met by the applicant:

1) S**cope of the GTGs** is adequately addressed. That is, a description of the dedicated, fixed position alarms, controls, and displays necessary to accomplish the GTGs tasks as they are applied to the specific design and preferred/credited success path performance is provided. The plant design basis was reviewed to identify any specific operator actions credited in the safety analysis. The GTGs (or plant-specific EOPs, if available) was reviewed to identify operator actions for safety and non-safety success paths.

2) **Probabilistic Risk Assessment and Human Reliability Analysis (PRA/HRA)** are adequately addressed. That is, critical operator actions identified through the applicant's PRA/HRA are provided. The plant PRA/HRA was reviewed to identify any operator actions that are risk significant. The results of the diversity and defense-in-depth evaluation were reviewed to identify any specific operator actions credited for coping with common cause failures of digital protection systems.

3) **Analysis of operator actions** required to support safe shutdown of the reactor is addressed. That is, a function-based task analysis that describes the operator actions that are necessary to bring the reactor to a safe shutdown under conditions where the primary instrumentation is both available and unavailable is provided.

The following categories of operator functions and tasks need to be addressed in defining the minimum inventory (the listing is not meant to be inclusive):

- Operator actions that are credited in the plant's safety analyses, for which no automated actions are provided
- Monitoring actions and, when necessary, back up automatic protective actions or automated success paths called out in the GTGs or plant-specific EOPs; this includes manual system-level actuations and use of manual component-level controls when necessary
- Operator actions that are needed to accomplish the preferred manual safety success paths called out in the GTGs/EOPs for accident mitigation and safe shutdown, for which there are no automated success paths
- Operator manual actions needed to accomplish preferred manual non-safety success paths called out in the GTGs/EOPs
- Monitoring safety system availability
- Monitoring plant safety parameters (includes monitoring conditions that could lead to safety system actuation and potentially taking pre-emptive action prior to actuation)
- Functions and tasks, other than the above that are needed to support continued operation under conditions of failure or degradation of the normally-used HSIs – the extent of the functions and tasks that need to be performed depends on the plant's concept of operations for these conditions
- Other important functions and tasks needed during normal operation, with all HSIs available, which may require HSI capabilities or characteristics not provided by the primary HSIs (e.g., display of parameters important to maintaining situation awareness on a spatially dedicated display that is visible to the entire crew).

4) **Regulatory Guide 1.97**, Type A and Category 1 for plants committed to Revision 3 and Type A, B, and C variables for plants committed to Revsion 4 for accident monitoring are considered in the development of the minimum inventory (i.e., important system alarms, controls, and displays described in the Design Certification Tier 1 system design descriptions necessary for transient mitigation are included [safety-related equipment to verify safe shutdown and indications and controls to verify critical safety functions]. Additional post-accident monitoring – use of Regulatory Guide 1.97 instrumentation for additional functions beyond the credited operator manual actions and backing up of the automatic systems covered in 1 and 2 above.)

5) **Design of the I&C architecture**. Developing the minimum inventory considers the digital control and information system, the potential failure modes of the system and the normally-used HSIs, and the plant's concept of operations for dealing with failures or degradation of the normally-used HSIs.

The failure analysis will be reviewed to determine if the following types of failures, at a minimum were considered:

- Loss of one or more primary workstations, such that displays go dark or freeze or are impaired in some other way; this should consider potential failures that could affect multiple or all of the workstations normally used by the operators
- Loss or degradation of a data network, control network, or other information pathway that causes loss or delay of information to displays, or loss of communication capability among controllers or between controllers and field devices
- Loss of a server, or multiple redundant servers (e.g., common cause failure due to software error or software maintenance error), providing applications important to the control room HSIs
- Loss of automatic control functions; proper segmentation or distribution of control functions to control processors and input/output units can prevent large-scale loss of automatic control capability – however, if more advanced control functions or integrated control capabilities are provided involving interconnection or interaction among control functions, greater vulnerability to such failures may be introduced
- Loss of power causing failure or degradation of the HSIs.

6) Concept of Operations. The desired concept of operations has been defined for the identified failure conditions, a number of options are possible, including, but not limited to the following (all assume that the reactor is at power and no secondary event or accident has occurred):

- **Trip**. Immediately trip the plant and use the safety-related controls and displays already provided in the control room, plus local controls and indications as necessary to reach a safe shutdown condition.
- **Safely shut down using preferred success paths**. Use of normal or preferred means of reaching safe shutdown (e.g., rod insertion and boration rather than trip, normal depressurization cooldown rather than vent and bleed) may be more desirable than using only safety means, which often present a significant economic burden on the plant.
- **Hold for a pre-determined finite time**. Maintain the current plant operating conditions for a specified period of time with no power increases or load following maneuvers, and monitor for conditions requiring plant shutdown. This could be based on the expected time to return the HSIs to service and may require establishing a Limiting Condition of Operation (LCO) or suitable administrative limits, and gaining relief from Technical Specifications related to periodic surveillances that may not be practical to conduct if the normal HSIs are failed or degraded.
- **Continue operating indefinitely**. Continue operating the plant for an indefinite period of time at the current power level with no power increases or load following maneuvers, but potentially supporting down-power maneuvers such as a power reduction to handle loss of a major piece of equipment. This would require that there be no LCO dictating a plant shutdown after a specified period of time.

6**) Design of the HSI.** Design requirements are determined for the HSIs needed for the operator functions and tasks. These are based on the applicable regulatory requirements and guidelines (e.g., NUREG-0700) and the plant's concept of operations. The following design requirements need to be addressed:

- Requirements regarding which HSIs need to be safety-related

- Accessibility requirements – in particular, which HSIs need to be spatially dedicated and continuously visible (SDCV), which ones can be one-step accessible (only one action is required in order to access the needed HSI), and which HSIs can be selectable
- Requirements for diversity and independence – which HSIs need to be independent of the normally-used HSIs (i.e., not subject to the postulated failure modes of the normally-used HSIs). Also, which HSIs are needed for coping with CCFs of the protection systems, as determined by a diversity and defense-in-depth evaluation and need to be independent and diverse with respect to the CCFs for which they provide coping capability.

In defining design requirements applicable to the minimum inventory HSIs, the following regulatory and industry requirements and guidance are addressed:

- 10 CFR 50.34(f) – post-TMI requirements for improved safety monitoring and control
- NUREG-0800 Chapter 18 – guidance on Safety Parameter Display Systems
- NUREG-0700 – guidance on reviewing human factors aspects of HSI design
- NUREG-0711 – guidance on task analysis, PRA/HRA, risk-important operator actions
- Regulatory Guide 1.97 – criteria for accident monitoring instrumentation
- Regulatory Guide 1.47 – guidance on bypassed and inoperable status indication
- Regulatory Guide 1.62 – guidance on manual initiation of protective actions
- NUREG-0800 Chapter 7, Branch Technical Position (BTP) 7-19 – guidance on diversity and defense-in-depth
- IEEE 603 – standard criteria for safety systems
- ANSI/ANS 3.5 - guidance for the design and application of nuclear power plant simulators
- SECY 92-053 – guidance on the use of DAC
- SECY 93-087 – guidance on policy, technical and licensing issues related to ALWR designs