EPRI | ELECTRIC POWER RESEARCH INSTITUTE

Minimum Inventory

Human Factors Task Working Group Meeting

May 31, 2007

Objectives of Discussion

- Discuss how we are defining “minimum inventory”
- Provide a walk-through of the draft industry guidance report recently provided to NRC
- Discuss the overall approach and process recommended in the report
- Identify key issues
- Answer questions and discuss any areas of concern
- Understand how this information will be incorporated into regulatory guidance

Minimum Inventory – Definition

- Minimum inventory HSIs are:
  - Those HSIs needed beyond the non-safety, selectable, computer-driven HSIs normally used by the operators and typically driven by a distributed control system (DCS)
    - Safety related HSIs needed to meet regulatory requirements
    - Minimum set of spatially dedicated human-system interfaces
    - Minimum set of HSIs needed to handle failure of the normally used HSIs

Industry Guidance Report (EPRI 1015089) - Draft in Progress

1 Introduction

2 Relevant Regulatory Requirements, Standards and Regulatory Guides

3 Process for Identifying and Implementing the Minimum Inventory

4 Design Requirements for Minimum Inventory HSIs

5 Implementation Options and Selecting a Design Concept

6 Minimum Inventory in the Licensing Process

7 References

Appendix – Comparison to Reg. Guide 1.97 Rev. 4

Objectives of the Guidance Document

- Clarify purpose of the minimum inventory HSIs
- Provide a method for identifying those that are needed
- Identify design requirements applicable to different categories of minimum inventory HSIs, specifically:
  - Requirements for safety-related/qualified HSIs
  - Diversity and independence requirements (e.g., diverse and independent from DCS)
  - Accessibility requirements (e.g., need for spatially dedicated, continuously visible HSIs)
- Clarify and fill in the gaps in current regulatory requirements and guidance documents

Objectives (cont'd)

- Address credible failures of I&C and normally-used HSIs
- Address HSIs resulting from D3 coping analysis
- Provide guidance on implementation of the minimum inventory HSIs as part of overall control room design
- Provide guidance on documentation and licensing submittals related to minimum inventory
- Address both new plant designs and modernization of operating plants
- Address designs that provide control of safety and non-safety equipment through a single interfacea and designs that do not have this feature

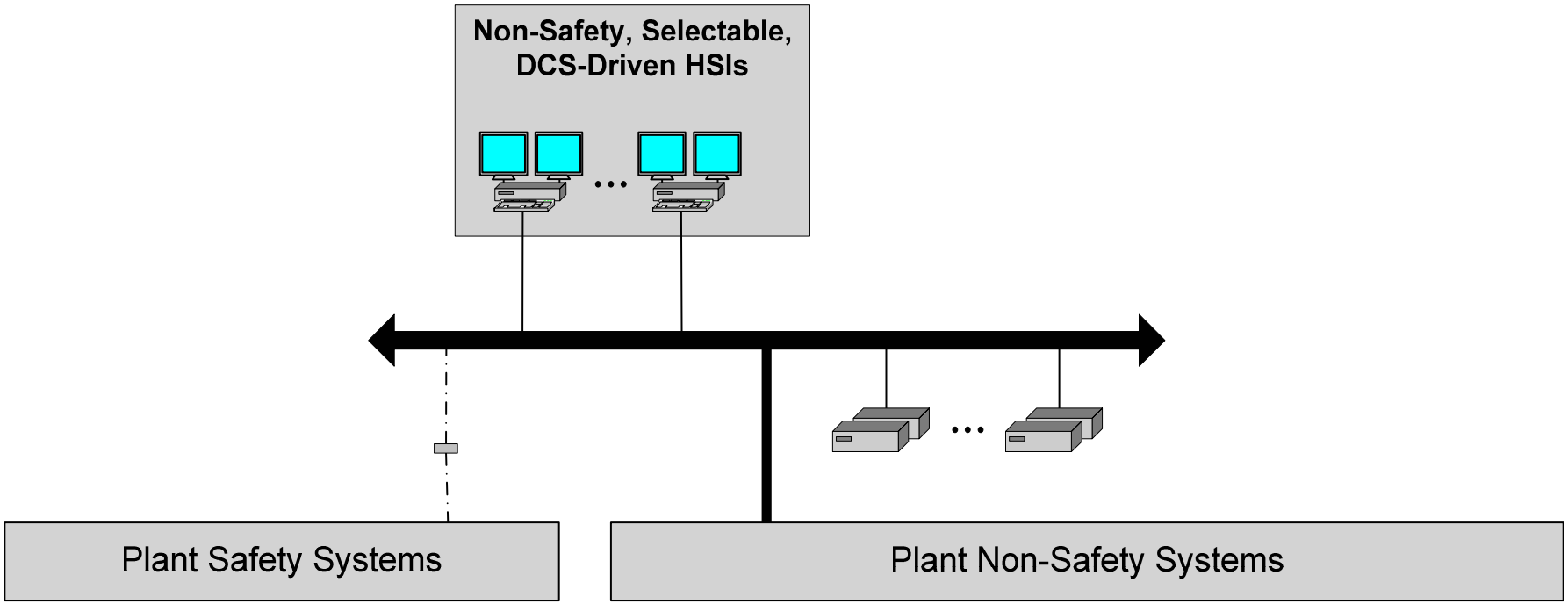
Basis

- Current regulatory requirements, standards, and guides
- Recently developed EPRI guidance on minimum inventory
  - EPRI 1010042 (primarily Section 6.5)
  - Peer reviewed by industry working group
- Based on methods developed in early modernization studies for operating plants
- Also based on approaches used in ALWR design certifications and regulatory interactions
- Input and direction from NEI Human Factors Task Force and other industry experts

Important Drivers and Inputs in Defining Minimum Inventory

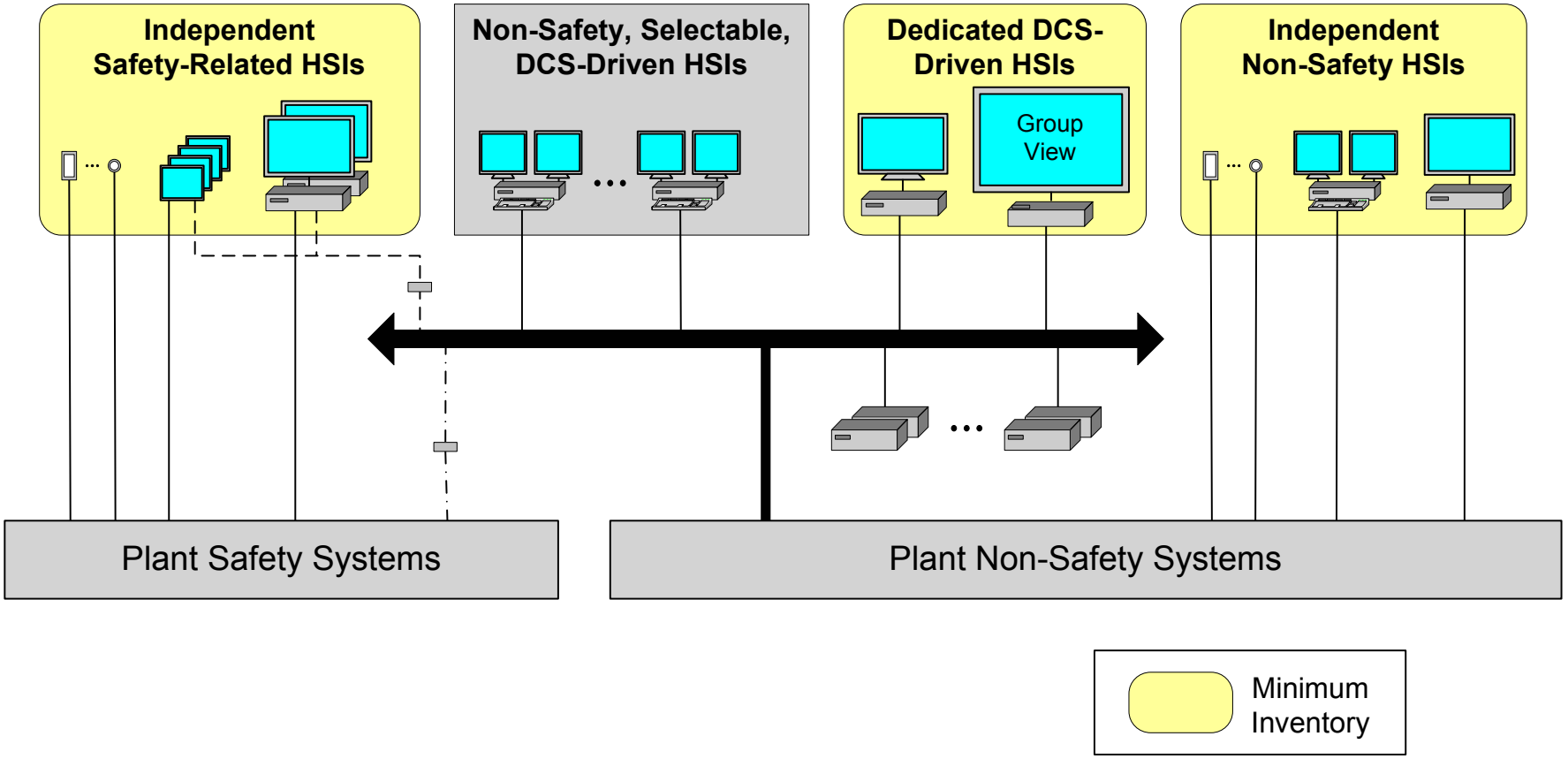
- Regulatory requirements and standards
- Regulatory guides on post-accident monitoring and other post-TMI requirements
- Plant's concept of operations for normal and emergency operation
- Plant I&C and information systems architecture
- I&C and HSI failure modes and degraded conditions
- Diversity & defense-in-depth (D3) evaluation
- Emergency response procedure guidelines (EPGs) or plant-specific emergency operating procedures (EOPs)
- Plant probabilistic risk assessment (PRA)

What additional HSIs are needed?



EPRI ELECTRIC POWER RESEARCH INSTITUTE

Minimum Inventory HSIs



EPRI ELECTRIC POWER RESEARCH INSTITUTE

Process for Defining Minimum Inventory

- Determine what functions and tasks need to be supported by the HSIs
- Identify specific HSI resources needed
  - Alarms
  - Controls
  - Displays
  - Procedures
- Determine what design requirements apply to the HSIs

Categories of Functions and Tasks - Emergency Operations

- Manual operator actions credited in the safety analysis
- Monitoring and backing up automatic protective actions and automatic success paths in EPGs/EOPs
- Manual actions needed to accomplish preferred manual safety success paths in EPGs/EOPs
- Manual actions needed to accomplish preferred manual non-safety success paths in EPGs/EOPs
- Additional post-accident monitoring per Reg. Guide 1.97

Categories of Functions and Tasks - Non-Emergency Operations

- Monitoring safety system availability
- Monitoring plant safety parameters
- Functions and tasks needed to cope with failure of normally-used HSIs
- Other important functions and tasks needed during normal operations that may require additional HSI capabilities (e.g., group-view displays)

Identify HSI Resources Needed

- Guidance provided for identifying the different types of HSI resources required for each category of functions and tasks, for example:
  - Prompting indications and alarms
  - Controls
  - Immediate feedback indications on control action
  - Performance indications and alarms
  - Procedures

Determine HSI Design Requirements

- Safety classification / qualification requirements
  - Use of a graded approach to qualification is suggested for certain categories of HSIs
- Independence Requirements (HSIs that need to be independent of the DCS)
- Diversity Requirements (HSIs for D3 coping must be diverse from safety system CCFs for which they provide backup)
- Hardware/software simplicity requirements
- Accessibility requirements
  - Which HSIs need to be spatially dedicated, continuously visible (SDCV)
  - Which ones can be “one-step accessible”

DCS Failure Modes and Degraded Conditions

- High-level guidance provided for assessment of DCS failure modes
  - Identifies types of failures to consider
  - Discusses use of defensive measures in design and configuration to prevent or minimize the likelihood of failures
  - Recognizes the need for judgment to be applied in evaluating failure modes, frequencies and durations
- Anticipated failure modes and associated concept of operations can be key factors in determining the scope of the required backup HSIs (e.g., loss of all DCS VDUs)

Concept of Operations for Failed/Degraded HSI Conditions

- Safety-related HSIs needed for accident mitigation and achieving safe shutdown are required by regulation
- Additional HSIs required for dealing with DCS failures are discretionary – depend on the desired capabilities
- Options for dealing with failures include:
  - Trip the plant
  - Safely shut down using preferred success paths
  - Hold at power for a pre-determined finite time
  - Continue operating at power indefinitely

Minimum Inventory HSI Design Requirements Matrix

- Matrix provided as Table 4-1 of industry guidance report, along with accompanying text (Section 4)
- Addresses each category of functions/tasks
- For each category, identifies design requirements for each type of HSI resource (prompting indications, alarms, controls, procedures, etc.) including
  - Safety classification / qualification requirements
  - Independence, diversity and simplicity requirements
  - Accessibility requirements
- Identifies the applicable regulatory and industry requirements, and gives proposed approaches where existing guidance is unclear or absent

Implementation Guidance

- Wide range of options available for implementing the minimum inventory HSIs
- Guidance is provided on:
  - Use of automation to reduce manual actions
  - Capabilities and tradeoffs regarding choice of conventional or computer-based HSI technology
  - Minimizing the number of different types of HSIs
  - Impact on Tech Specs and Emergency Plan
  - Impact on procedures and training

Minimum Inventory in the Licensing Process

- Minimum inventory should be defined as part of the overall control room/HSI design process, following accepted HFE guidelines and processes
- Recommend for new plants:
  - In Tier 1 commit to the process that will be used to define the minimum inventory
  - Detailed results developed for DAC closure
- Recommend similar approach for modernization projects at operating plants for which a license amendment is required

Key Issues Addressed In Report

- Safety classification / qualification requirements
  - Class 1E HSI for RG 1.62, IEEE 497 Type A (and associated manual controls)
  - Graded approach for IEEE 497 Type B and C, and preferred safety equipment success paths defined in EOPs
  - Non-safety classification for remaining HSIs
- Independence
  - HSI to accommodate operation strategy for loss of DCS VDUs
- Diversity
  - HSI to accommodate D3
- Simplicity
  - Conformance to RG 1.62 and BTP-19, Point 4
- Accessibility requirements
  - SDCV for RG 1.62, IEEE 497 Type A and B, RG 1.47, 10 CFR 50.34 (SPDS)
  - One-step accessible for Type A controls if supported by HFE analysis

Key Issues Addressed in Report

- Back-up procedures
  - For accident mitigation and safe shutdown
    - Paper or safety-related computer platform
    - Need not include event-specific, only functional recovery EOPs
  - For coping with loss of DCS HSIs
    - These are discretionary since safe shutdown is already covered above
  - For D3 coping
    - If a common cause failure (CCF) can fail both the safety system and the computer-based procedure system, then back-up procedures are needed to cope with CCF