

# Minimum Inventory of Human-System Interfaces

EPRI 1015089

Draft Report, December 2007

DRAFT

EPRI Project Manager  
Joseph Naser



## **DISCLAIMER OF WARRANTIES AND LIMITATION OF LIABILITIES**

THIS DOCUMENT WAS PREPARED BY THE ORGANIZATION(S) NAMED BELOW AS AN ACCOUNT OF WORK SPONSORED OR COSPONSORED BY THE ELECTRIC POWER RESEARCH INSTITUTE, INC. (EPRI). NEITHER EPRI, ANY MEMBER OF EPRI, ANY COSPONSOR, THE ORGANIZATION(S) BELOW, NOR ANY PERSON ACTING ON BEHALF OF ANY OF THEM:

(A) MAKES ANY WARRANTY OR REPRESENTATION WHATSOEVER, EXPRESS OR IMPLIED, (I) WITH RESPECT TO THE USE OF ANY INFORMATION, APPARATUS, METHOD, PROCESS, OR SIMILAR ITEM DISCLOSED IN THIS DOCUMENT, INCLUDING MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, OR (II) THAT SUCH USE DOES NOT INFRINGE ON OR INTERFERE WITH PRIVATELY OWNED RIGHTS, INCLUDING ANY PARTY'S INTELLECTUAL PROPERTY, OR (III) THAT THIS DOCUMENT IS SUITABLE TO ANY PARTICULAR USER'S CIRCUMSTANCE; OR

(B) ASSUMES RESPONSIBILITY FOR ANY DAMAGES OR OTHER LIABILITY WHATSOEVER (INCLUDING ANY CONSEQUENTIAL DAMAGES, EVEN IF EPRI OR ANY EPRI REPRESENTATIVE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES) RESULTING FROM YOUR SELECTION OR USE OF THIS DOCUMENT OR ANY INFORMATION, APPARATUS, METHOD, PROCESS, OR SIMILAR ITEM DISCLOSED IN THIS DOCUMENT.

ORGANIZATION(S) THAT PREPARED THIS DOCUMENT

**CDF Services, Inc.**

### **NOTE**

For further information about EPRI, call the EPRI Customer Assistance Center at 800.313.3774 or e-mail [askepri@epri.com](mailto:askepri@epri.com).

Electric Power Research Institute, EPRI, and TOGETHER...SHAPING THE FUTURE OF ELECTRICITY are registered service marks of the Electric Power Research Institute, Inc.

Copyright © 2007 Electric Power Research Institute, Inc. All rights reserved.



## CITATIONS

---

*[Later]*

DRAFT



## PRODUCT DESCRIPTION

---

*[Later]*

DRAFT



# ABSTRACT

---

*[Later]*

DRAFT



## ACKNOWLEDGMENTS

---

*[This page will acknowledge the members of the NEI Task Force and other contributors to the preparation of this report.]*

DRAFT



# PREFACE

---

This report provides guidance on identifying and implementing a minimum inventory of human-system interfaces (HSIs) that are needed in addition to the selectable displays and controls provided on computer-based workstations normally used by the operators. The phrase “minimum inventory” has been used in a number of regulatory guidance documents such as NUREG 0711 and NUREG 0800 Chapter 18, and in documents related to design certification reviews for advanced light water reactor (ALWR) designs. NUREG 0711 and 0800 use this phrase to refer to the complete set of HSIs needed by the operators to perform their tasks based on task analysis. As applied in various ALWR design reviews, the term was used to refer either to a minimum set of fixed position or spatially dedicated HSIs, or to HSIs needed in the case of failure of the HSIs normally used by the operators.

It is the intent of this industry guidance report to clear up the confusion regarding the use of this term, and to define the “minimum inventory HSIs” as those that are needed beyond the selectable HSIs provided on the nonsafety-related, computer-based workstations normally used by the operators to monitor and control the plant. This includes:

- The minimum set of HSIs that need to be implemented using safety-related equipment
- The minimum set of HSIs that should be spatially dedicated and continuously visible, and
- The HSIs needed (beyond the safety-related HSIs noted above) to support the plant’s concept of operations for situations in which the HSIs normally used are failed or degraded.



## LIST OF ACRONYMS

---

AFW	Auxiliary feedwater
ALWR	Advanced light water reactor
ATWS	Anticipated transient without scram
BTP	Branch technical position
BWR	Boiling water reactor
C&I	Control and information
CCF	Common cause failure
D3	Diversity and defense-in-depth
DCS	Distributed control system (or digital control system)
EOP	Emergency operating procedures
EPG	Emergency procedure guidelines
ESFAS	Engineered safety features actuation system
HFE	Human factors engineering
HSI	Human-system interface
I&C	Instrumentation and control
LCO	Limiting condition of operation
MCR	Main control room
NRC	Nuclear Regulatory Commission
NSR	Nonsafety-related

PRA	Probabilistic risk assessment
PWR	Pressurized water reactor
RTS	Reactor trip system
SAR	Safety analysis report
SDCV	Spatially dedicated, continuously visible
SPDS	Safety Parameter Display System
SR	Safety-related
SRM	Staff Requirements Memorandum
SRP	Standard review plan
RG	Regulatory guide
VDU	Video display unit

# CONTENTS

---

<b>1 INTRODUCTION .....</b>	<b>1-1</b>
1.1 Background and Purpose.....	1-1
1.2 Contents of this Report.....	1-3
<b>2 RELEVANT REGULATORY REQUIREMENTS, STANDARDS AND REGULATORY GUIDES .....</b>	<b>2-1</b>
2.1 Regulatory Requirements and Guidance .....	2-1
NUREG-0800, Standard Review Plan – Chapter 18, Human Factors Engineering [10].....	2-2
Regulatory Guide 1.97, Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants (Rev. 3 - 1983; Rev. 4 - 2006) [14,15].....	2-2
Regulatory Guide 1.47, Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems [12] .....	2-6
Regulatory Guide 1.62 Manual Initiation of Protective Actions [13] .....	2-6
NUREG-0800, Standard Review Plan Chapter 7, Branch Technical Position BTP 7-19, Guidance for Evaluation of Defense-in-Depth and Diversity in Digital Computer-Based Instrumentation and Control Systems [10].....	2-7
2.2 Industry Standards .....	2-7
IEEE 603 – IEEE Standard Criteria for Safety Systems for Nuclear Power Plants (1998) [6].....	2-7
IEEE 497 - IEEE Standard Criteria for Accident Monitoring Instrumentation for Nuclear Power Generating Stations (2002) [5] .....	2-8
<b>3 PROCESS FOR IDENTIFYING AND IMPLEMENTING THE MINIMUM INVENTORY .....</b>	<b>3-1</b>
3.1 Overview .....	3-1
3.1.1 Categories of Functions and Tasks .....	3-3
3.1.2 HSI Resources Needed.....	3-5
3.1.3 HSI Design Requirements .....	3-7
3.1.4 HSI Failure Modes and Backup Operational Capabilities.....	3-10
3.1.4.1 Control and Information System and HSI Failure Modes.....	3-10
3.1.4.2 Concept of Operations for Failed/Degraded Conditions .....	3-12

3.1.4.3 Implementing the Backup HSIs.....	3-14
3.2 New Plant Designs.....	3-14
3.3 Modernization of Operating Plants.....	3-15
<b>4 DESIGN REQUIREMENTS .....</b>	<b>4-1</b>
4.1 Perform Manual Credited Actions .....	4-10
4.2 Monitor Safety Functions and Back Up Automatic Success Paths .....	4-13
4.3 Carry Out Preferred Manual Safety Success Paths .....	4-18
4.4 Carry Out Preferred Manual Non-Safety Success Paths .....	4-20
4.5 Perform Additional Post-Accident Monitoring for Radioactivity Releases .....	4-21
4.6 Monitor Safety System Availability .....	4-22
4.7 Monitor Plant Safety Parameters .....	4-23
4.8 Continue Operation Under Conditions of Failed/Degraded HSIs .....	4-24
4.9 Perform Other Important Tasks During Normal Operation With All HSIs Available .....	4-26
<b>5 IMPLEMENTATION OPTIONS AND SELECTING A DESIGN CONCEPT .....</b>	<b>5-1</b>
5.1 Automation to Reduce Manual Actions .....	5-1
5.2 Capabilities and Trade-Offs of Available HSI Technologies.....	5-2
5.3 Minimizing the Number of Different Types of HSIs .....	5-4
5.4 Impact on Tech Specs and Emergency Plan .....	5-4
5.5 Impact on Procedures and Training .....	5-4
<b>6 REFERENCES .....</b>	<b>6-1</b>
<b>A COMPARISON TO REG. GUIDE 1.97 REV. 4 .....</b>	<b>A-1</b>

## LIST OF FIGURES

---

Figure 3-1 Different Types of Minimum Inventory HSIs .....	3-2
Figure 3-2 Examples Showing Types of HSI Resources Needed to Support a Manual Control Task.....	3-6
Figure 3-3 Process for Identifying and Implementing Minimum Inventory HSIs as Part of Control Room Modernization .....	3-18

DRAFT



# LIST OF TABLES

---

Table 2-1 Relevant Criteria in Reg. Guide 1.97 Rev. 4 and IEEE Std 497-2002 by Variable Type .....	2-5
Table 4-1 Minimum Inventory HSI Design Requirements Matrix .....	4-3
Table 4-2 Summary List of Safety-Related and SDCV or One-Step Accessible HSIs.....	4-9
Table 5-1 Comparison of Conventional and Newer Computer-Based HSI Technologies.....	5-2
Table A-1 Comparison of Industry Guidance Report to Reg. Guide 1.97 Rev. 4 and IEEE Std 497-2002.....	A-2

DRAFT



# 1

## INTRODUCTION

---

This report addresses design requirements for human-system interfaces (HSIs) that are needed in addition to the nonsafety, selectable computer-based HSIs normally used by the operators to monitor and control the plant. The report describes an overall approach and specific guidelines that can be followed to identify the needed HSIs and their design requirements.

### 1.1 Background and Purpose

In a modern control room employing digital technology, the primary HSIs used by the control room operators during normal operation typically are based on nonsafety workstations with selectable displays and controls, often driven by a distributed control system (DCS). These may be in the form of compact workstations designed for seated operation, distributed workstations built into stand-up control panels, or some combination of the two. The DCS workstations provide the operators with the displays, controls and alarms needed to support normal plant operation. Some designs also provide capability to control safety equipment, allowing the workstations to be used for periodic testing, operating and maintenance bypasses and emergency operations as well. However, there are requirements for additional HSIs to support both normal and emergency plant operations, which cannot be met by the operator workstations because these workstations typically use nonsafety-related equipment and rely primarily on selectable displays.

While nonsafety computer-based workstations have demonstrated outstanding reliability, suitable for normal and emergency nuclear plant operations, it is recognized that these are complex systems that could experience large-scale HSI failure (e.g., blackout of workstation displays). Therefore, it is important to consider the potential for large-scale failures of the primary HSIs.

The report addresses two key questions that affect both design and licensing of a modern control room:

1. What HSIs will be required beyond the primary computer-based workstations? (These HSIs will be referred to hereafter as “minimum inventory HSIs<sup>1</sup>”)

---

<sup>1</sup> The phrase “minimum inventory” has been used in a number of regulatory guidance documents such as NUREG 0711 [8] and NUREG 0800 Chapter 18 [10], and in documents related to design certification reviews for advanced light water reactor (ALWR) designs. NUREG 0711 and 0800 use this phrase to refer to the complete set of HSIs needed by the operators to perform their tasks based on task analysis. As applied in various ALWR design reviews, the term was used to refer either to a minimum set of fixed position or spatially dedicated HSIs, or to HSIs needed in the case of failure of the HSIs normally used by the operators. It is the intent of this industry guidance report to clear up the confusion regarding the use of this term, and to define the “minimum inventory HSIs” as those

## 2. What are the design bases and requirements for these minimum inventory HSIs?

There are several factors driving the need for minimum inventory HSIs.

Some are required by regulations or licensing commitments. For example, to comply with IEEE 603 [6] and Regulatory Guide 1.97 [14,15] qualified, safety-related HSIs must be provided for accident mitigation, to achieve safe shutdown, and for post accident monitoring. This is true even if the design allows for control of safety equipment via the nonsafety workstations, that is, conformance to these requirements cannot rely solely on the nonsafety HSIs. These are not new requirements – most of these requirements are met today in conventional control rooms. However, many of the HSIs in a conventional control room are safety-related simply because the monitoring instruments are safety-related or the components being controlled are safety-related. This is because in analog designs it was more cost effective for suppliers to provide safety-related HSIs than to isolate conventional circuits to allow for nonsafety-related HSIs. But in a modern design based on digital control and monitoring systems, nonsafety HSIs tend to be more cost effective, regardless of the device being monitored or controlled, and allow for greater functionality for a more effective interface. Therefore, this report examines what safety-related HSIs are required to comply with IEEE 603 and Reg. Guide 1.97.

Other minimum inventory HSIs may be needed to handle failures of the nonsafety HSIs that could occur during normal operation. Because safety-related HSIs are required to achieve safe shutdown as discussed above, additional minimum inventory HSIs provided to allow continued operation may be largely discretionary, driven in large part by the plant's chosen concept of operations for anticipated failure conditions. Still others may be needed to provide capabilities or design characteristics that are desired but are not provided by standard operator workstations employing selectable displays and controls – for example, a large overview display of important information used by the entire operating crew to enhance crew interaction<sup>2</sup>. Regulatory requirements and guidelines related to which HSIs should be continuously displayed and which ones can be selected by the operator on demand are not always clear. Another consideration is what design requirements apply to HSIs that will be needed as backups to be used in the event of failure of the safety systems, as determined by a diversity and defense-in-depth (D3) evaluation to address postulated common cause failures of the protection systems.

This industry guidance report provides an acceptable approach for addressing these issues, ensuring that the applicable regulatory requirements are met, and answering questions such as:

- How the minimum inventory HSIs should be identified

---

that are needed beyond the selectable displays and controls provided on nonsafety-related, computer-based workstations that are normally used by the operators to monitor and control the plant.

<sup>2</sup> This is not to say that a large overview display cannot be driven by the same system that drives the workstations. As will be discussed later, such displays can and in many cases should be provided and driven from the same system. The question posed here is what HSIs are needed beyond the *selectable* displays and controls provided on typical operator workstations.

- Which safety related instrumentation and plant components must have safety-related HSIs for accident mitigation and to achieve safe shutdown based on the applicable regulatory requirements and guidance<sup>3</sup>
- Which HSIs need to be independent of the normally-used operator workstations, providing backup capabilities that allow the operators to deal with credible failures or degradation of those workstations. These include the safety-related HSIs, but additional HSIs may also be desirable.
- Which HSIs need to be presented in fixed positions, i.e., spatially dedicated and continuously visible to the operators versus selectable or displayed “on demand.”

The intent is that when the approach presented in this report is followed, the various issues related to minimum inventory will have been properly addressed, the applicable regulatory requirements will be met, and the needed minimum inventory HSIs will be provided as part of an integrated control room design solution, providing an effective interface for the operators for both normal and emergency operations.

## 1.2 Contents of this Report

This report begins in Section 2 by summarizing the relevant regulatory requirements, standards and regulatory guides. Requirements of the relevant industry standards also are summarized. Then, Section 3 describes a process that can be used to identify the minimum inventory HSIs and their design requirements, addressing both new plants and modernization of currently operating plants.

Section 4 addresses in some detail the various design requirements for minimum inventory HSIs. These are summarized in a Minimum Inventory HSI Design Requirements Matrix.

Section 5 discusses options for implementing the minimum inventory HSIs and provides associated guidance.

Section 6 lists references cited in the report.

Finally, Appendix A provides a comparison of the minimum inventory HSI treatment in this report to the guidance provided in Regulatory Guide 1.97 Revision 4 [15].

---

<sup>3</sup> This report discusses a number of regulatory guides issued by the NRC. Provisions contained in regulatory guides are not regulatory requirements, but provide guidance to NRC reviewers and licensees on acceptable ways to meet the regulations. However, new plant designers and owners/operators of existing plants often commit to meeting certain regulatory guides, which has the effect of making them requirements. When this document refers to “requirements” of a regulatory guide, this means provisions that would be required in order to comply with the approach specified in that regulatory guide.

### **A Note Regarding Treatment of the Remote Shutdown Station**

The recently published Interim Staff Guidance on minimum inventory included the remote shutdown station (RSS) as well as the main control room. The industry is still evaluating whether and how to address the RSS in the treatment of minimum inventory provided in this report. There are several considerations here:

- As defined in this report, the minimum inventory issue primarily addresses what HSIs need to be safety-related, and which ones need to be spatially dedicated and continuously visible. Minimum inventory as applied to the RSS should not, therefore, address what set of HSIs are needed to fulfill the remote shutdown function, but rather which of those (if any) need to be safety-related and/or spatially dedicated. Although the RSS has been addressed in the minimum inventory for some new design certifications, it is not clear that the definition used here has been applied when dealing with the HSIs at the remote shutdown station.
- The regulatory requirements for the remote shutdown station are contained in 10 CFR 50 Appendix A, GDC 19 (Control Room) and 10 CFR 50 Appendix R (Fire Protection). Guidance for reviewers is provided in the Standard Review Plan (SRP) Chapter 7 (Section 7.4-7). As noted in the SRP, remote shutdown is not an accident analyzed in the SAR accident analyses. A fire impacting the control room is a key event that defines the needed RSS capability. An accident does not have to be assumed concurrent with the fire, nor does a single failure have to be assumed. However, for other events causing the control room to be uninhabitable, a single failure should be assumed in demonstrating capability to reach safe shutdown at the RSS. This can have implications regarding whether safety or nonsafety equipment can be used at the RSS. Those implications need to be explored further.
- The need for spatially dedicated, continuously visible (SDCV) HSIs at the remote shutdown station should also be examined. Because the RSS is designed for a specific purpose, its use is procedure-driven, and due to its narrow purpose it does not have large numbers of HSIs competing for attention, the need for SDCV HSIs may be much less than for the main control room. Again, this should be explored further to determine what criteria should apply.
- We should ensure that any criteria or guidance we provide for the RSS HSIs is consistent with the design and licensing bases for remote shutdown stations in currently operating plants (or at a minimum understand the implications for current plants), which likely are plant-specific.

# 2

## RELEVANT REGULATORY REQUIREMENTS, STANDARDS AND REGULATORY GUIDES

---

The pertinent regulatory requirements, standards and guidelines are summarized briefly below, organized in two categories: (1) regulatory requirements and guidance, and (2) industry standards.

### 2.1 Regulatory Requirements and Guidance

10 CFR 50 Appendix A specifies a number of General Design Criteria (GDCs), including two that directly relate to I&C and the main control room:

Criterion 13, *Instrumentation and control*, states that “Instrumentation shall be provided to monitor variables and systems over their anticipated ranges for normal operation, for anticipated operational occurrences, and for accident conditions as appropriate to assure adequate safety...Appropriate controls shall be provided to maintain these variables and systems within prescribed operating ranges.”

Criterion 19, *Control room*, states that “A control room shall be provided from which actions can be taken to operate the nuclear power unit safely under normal conditions and to maintain it in a safe condition under accident conditions...”

In 10 CFR 50.34(f), several requirements were established to improve safety monitoring and control after the Three Mile Island (TMI) accident, including:

- 50.34(f)(2)(iv) Safety Parameter Display System (SPDS)
- 50.34(f)(2)(v) Bypass and operable status indication for safety systems
- 50.34(f)(2)(xii) Automatic and manual AFW system initiation and flow indication in control room (PWRs only)
- 50.34(f)(2)(xviii) Indication of inadequate core cooling such as saturation meters in PWRs, and signals from indicators of coolant level in the reactor vessel and in-core thermocouples in PWRs and BWRs
- 50.34(f)(2)(xix) Post-accident monitoring instrumentation
- 50.34(f)(2)(xxiv) Capability to record reactor vessel water level in one location on recorders that meet post-accident recording requirements (BWRs only)
- 50.34(f)(2)(xxvii) In-plant radiation monitoring for a broad range of routine and accident conditions

The regulations, however, provided little guidance on how these systems, functions, and capabilities were to be implemented. In order to provide guidance on meeting these requirements, numerous NRC documents were developed. The key points of several are discussed below, including:

- NUREG-0800, Standard Review Plan [10] Chapter 18, Human Factors Engineering (and related NRC guidance on SPDS)
- Regulatory Guide 1.97, Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants (Rev. 3 - 1983; Rev. 4 - 2006) [14,15]
- Regulatory Guide 1.47, Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems [12]
- Regulatory Guide 1.62, Manual Initiation of Protective Actions [13]
- Branch Technical Position BTP 7-19, Guidance for Evaluation of Defense-in-Depth and Diversity in Digital Computer-Based Instrumentation and Control Systems (NUREG-0800 Chapter 7) [10]

*NUREG-0800, Standard Review Plan – Chapter 18, Human Factors Engineering [10]*

The intent of the SPDS requirement was to improve the ability of plant personnel to monitor critical safety functions and rapidly determine when safety challenges arise. Numerous guidelines were published in NUREG-0800 specifically addressing the characteristics of safety parameter displays. Additional guidance was provided in Supplement 1 of NUREG-0737 [9] and NUREG-1342 [11]. The NRC review criteria for the HFE aspects of SPDS were subsequently moved from NUREG-0800 to NUREG-0700, Rev 2 (Section 5, Safety Function and Parameter Monitoring System) [7].

NUREG-1342 notes that SPDS parameters should be continuously displayed, not just continuously available. However, the NRC has accepted SPDS systems that provide either: (1) a dedicated, single display that continuously shows plant variables, or (2) a hierarchy of selectable display pages on a single display device, along with continuously-displayed perceptual cues to alert the user to changes in the safety status of the plant (such as when safety functions are challenged).

*Regulatory Guide 1.97, Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants (Rev. 3 - 1983; Rev. 4 - 2006) [14,15]*

This regulatory guide addresses instrumentation for accident monitoring and describes an acceptable method to meet regulatory requirements as they relate to post-accident monitoring instrumentation. Revision 3 of the regulatory guide, to which many operating plants are committed, defines types of variables to be monitored and lists specific variables of each type, along with associated ranges, for BWRs and PWRs. It also defines the categories of instrumentation, specifies what category should be used for each variable, and identifies design and qualification criteria for each category; criteria cover equipment qualification, redundancy, power source, channel availability, quality assurance, display and recording, range, equipment

identification, interfaces, servicing, testing and calibration, human factors, and direct measurement criteria.

Table 2 of Regulatory Guide 1.97 Rev. 3 identifies types of variables based on their use by operations personnel. They are:

Type A – Those variables to be monitored that provide the primary information required to permit the control room operator to take specific manually controlled actions for which no automatic control is provided and that are required for safety systems to accomplish their safety functions for design basis accidents.

Type B – Those variables that provide information to indicate whether plant safety functions are being accomplished.

Type C – Those variables that provide information to indicate the potential for being breached or the actual breach of the barriers to fission product releases.

Type D – Those variables that provide information to indicate the operation of individual safety systems and other systems important to safety.

Type E – Those variables to be monitored as required for use in determining the magnitude of the release of radioactive materials and continually assessing such releases.

The human factors considerations given in Rev. 3, applicable to all categories, include:

- instrumentation should be designed to facilitate the recognition, location, replacement, repair, or adjustment of malfunctioning components or modules
- instrumentation design should minimize conditions that would cause anomalous indications; human factors analysis should be used in determining type and location of displays
- to the extent practicable, the same instruments should be used for accident monitoring as are used for normal operation

For each variable listed, Table 2 of Regulatory Guide 1.97 Rev. 3 identifies which of three categories of design and qualification criteria are needed for the instrumentation providing the variables. The aspects of these criteria directly related to HSI design are summarized below in terms of the need for qualified HSIs, information redundancy, and continuous information presentation.

For Category 1 instrumentation:

- *Qualification* – “Qualification applies to the complete instrumentation channel from sensor to display where the display is a direct indicating meter or recording device. If the instrumentation channel signal is to be used in a computer-based display, recording, or diagnostic program, qualification applies from the sensor up to and including the channel isolation device.” Although this implies that no qualification is needed for computer-based HSIs, it is important to remember that this regulatory guide was written at a time when computer-based systems were relatively new and not widely used in nuclear plant control

rooms. As computer-based displays play a more significant role in the control room, it should be expected that they will require some level of qualification if they are used to support accident mitigation or safe shutdown.

- *Redundancy* – For Category 1 instrumentation - “Where failure of one accident-monitoring channel results in information ambiguity (that is, the redundant displays disagree), that could lead operators to defeat or fail to accomplish a required safety function, additional instrumentation should be provided to allow the operators to deduce the actual conditions in the plant. This may be accomplished by providing additional independent channels of information on the same variable (addition of an identical channel) or by providing an independent channel to monitor a different variable that bears a known relationship to the multiple channels (addition of a diverse channel).”
- *Display and Recording* – Continuous real-time display should be provided. The indication may be on a dial, digital display, CRT, or strip chart recorder.

For Category 2 instrumentation:

- *Qualification* – Similar to Category 1, but no seismic qualification required, no redundancy requirements, and power sources only required to be highly reliable and battery backed where necessary; same provision regarding computer-based displays as is specified for Category 1. Quality assurance requirements applied should be consistent with the importance to safety of the instrumentation, allowing a graded approach to QA.
- *Redundancy* – No specific provisions
- *Display and Recording* – The instrumentation signal may be displayed on an individual instrument or it may be processed for display on demand.

For Category 3 instrumentation:

- *Qualification* – No specific provisions – allows for high quality commercial grade equipment.
- *Redundancy* – No specific provisions
- *Display and Recording* – Same as Category 2

The latest revision (Rev. 4) of Regulatory Guide 1.97 takes an updated approach based on IEEE Std 497-2002, discussed below. It defines the types of variables to be monitored and how they should be selected, along with design and qualification requirements for each type. Compared to earlier revisions of the regulatory guide, it takes a less prescriptive approach and relies heavily on the plant emergency procedure guidelines or plant-specific emergency operating procedures for identifying the required instrumentation.

Revision 4 of the Regulatory Guide, following IEEE Std 497-2002, specifies design and qualification criteria by the type of variable. It does not use the categories that were defined in Revision 3 and are summarized above. Table 2-1 summarizes design and qualification requirements of Regulatory Guide 1.97 Rev. 4 and IEEE Std 497-2002, addressing only those that are pertinent to this discussion of minimum inventory.

**Table 2-1**  
**Relevant Criteria in Reg. Guide 1.97 Rev. 4 and IEEE Std 497-2002 by Variable Type**

Relevant Criteria	Type A	Type B	Type C	Type D	Type E
Safety-related equipment criteria including single failure protection, independence and separation, Class 1E power supply, and quality assurance requirements	Safety-related requirements apply			Not required  (Uninterruptible power sources to be supplied if required, but may be non-1E)	
Equipment qualification requirements	Seismic qualification required if actions needed for a seismic event  Environmental qualification required only for accident in which action is needed	Seismic and environmental qualification required		Seismically qualified if monitoring system needed following seismic event  Environmental qualification required as needed for particular accidents	Not required
Continuous versus on-demand display	Continuous real-time display for at least one redundant channel  On-demand acceptable for other channels	On-demand display is acceptable			
Information ambiguity	Signal validation or method should be used to address channel failures that could otherwise result in information ambiguity			No requirements	
Trend or rate information	Trend information continuously available on a dedicated display for at least one channel if essential for the operator action; other channels can be selectable				
Display identification	Indications must be specifically marked to identify them as accident monitoring variables			No requirement	
Data recording	Recording capability required for at least one channel; information can be stored on nonsafety-related computers and made available on demand			No requirement	Recording capability required except for portable instruments

*Regulatory Guide 1.47, Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems [12]*

This document describes an acceptable way to meet regulatory requirements regarding status indication for safety systems. It includes the following provisions:

- Indication should be at the system level (regardless of whether indication is also provided at the component or channel level)
- The indication should be activated automatically when a bypass or other inoperability is induced deliberately for the protection system, the system it actuates to perform safety-related functions, or any auxiliary or supporting system that effectively bypasses or renders inoperable the protection system or actuated systems
- States the conditions under which such automatic activation must be provided based on expected frequency of occurrence and need for the affected system to be operable when it occurs
- Manual capability should exist in the control room to activate each system-level indicator (allows the operators to activate it when a condition occurs that is not automatically sensed and thus does not automatically activate the indication).

Note that there are no qualification or redundancy requirements stated in this regulatory guide.

*Regulatory Guide 1.62 Manual Initiation of Protective Actions [13]*

This document describes an acceptable way to meet regulatory requirements for manual initiation of protective actions, including:

- Means should be provided for manual initiation of each protective action at the system level, regardless of whether means are also provided to initiate at the component or channel level
- Manual initiation should perform all actions performed by automatic initiation (e.g., including valve sequencing, interlocks, etc.)
- Switches for manual initiation should be located in the control room and be easily accessible to the operator so that action can be taken in an expeditious manner
- The amount of equipment common to both manual and automatic initiation should be kept to a minimum and no single failure within the manual, automatic, or common portions should prevent initiation
- Manual initiation should depend on the operation of a minimum of equipment
- Manual initiation should be designed to go to completion.

*NUREG-0800, Standard Review Plan Chapter 7, Branch Technical Position BTP 7-19, Guidance for Evaluation of Defense-in-Depth and Diversity in Digital Computer-Based Instrumentation and Control Systems [10]*

This document provides acceptance guidelines for Defense-in-Depth & Diversity (D3) assessments of digital I&C system designs. The purpose of a D3 evaluation is to assess the vulnerability of the I&C systems to common cause failures due to software design errors and ensure that the plant has adequate coping capability to deal with such failures should they occur. As stated in the Standard Review Plan (NUREG-0800) Chapter 7, Appendix 7.0-A, the NRC expects that a D3 evaluation will be performed for digital upgrades involving the reactor trip system (RTS) or engineered safety features actuation system (ESFAS). (Note: EPRI 1002835 [1], *Guideline for Performing Defense-in-Depth & Diversity Assessments for Digital I&C Upgrades*, provides more detailed industry guidance for performing D3 evaluations, including use of risk-informed methods that are alternatives to the method described in BTP 7-19.)

BTP 7-19 reiterates NRC's four-point position on defense-in-depth and diversity. Points 1-3 apply to modifications to operating plants and call for the D3 evaluation discussed above. Such evaluations typically lead to identification of a small number of specific manual actions that operators should take to cope with postulated common cause failures of digital safety systems.

Point 4 indicates that "A set of displays and controls located in the main control room should be provided for manual system-level actuation of critical safety functions and monitoring of parameters that support safety functions. The displays and controls should be independent and diverse from the computer-based safety systems identified in Points 1 and 3." Acceptance criteria are provided, including specific capabilities that should be provided, how they should be implemented in order to ensure they are not subject to common cause failures of the protection systems, and the need for HFE principles and criteria to be applied in their design.

The latest revision of BTP 7-19 (Rev. 5) indicates that all four points of this position on D3 apply to both advanced plants and digital system modifications to operating plants.

## **2.2 Industry Standards**

This section briefly summarizes important provisions of two industry standards that relate to safety monitoring and control.

*IEEE 603 – IEEE Standard Criteria for Safety Systems for Nuclear Power Plants (1998) [6]*

This document includes the following requirements on control room indication and manual control (IEEE 603 section indicated in Parentheses):

- Displays needed for manual protective actions for which no automatic control is provided must be part of the safety systems (thus qualified) and must meet requirements of IEEE 497-1981 (5.8.1) Although the standard refers only to displays, it is reasonable to expect that the controls for these manual actions also should be considered part of the safety systems. Note that the scope of manual actions to which this paragraph applies is not very

clear. This report provides guidance for determining what requirements should be applied to various manual actions and the associated HSIs.

- Safety system status indication must be provided, but need not be part of the safety system (5.8.2)
- Continued indication of bypasses must be provided but need not be part of the safety system; requires automatic activation of this display under certain circumstances, and requires capability to manually activate the indication at any time (5.8.3)
- Requires that information displays be accessible to the operator, and displays for manually controlled protective actions be visible from the location of the controls used to effect the actions (5.8.4)
- “Human factors shall be considered at the initial stages and throughout the design process to assure that the functions allocated in whole or in part to the human operator(s) and maintainer(s) can be successfully accomplished to meet the safety system design goals, in accordance with IEEE Std 1023-1988.” (5.14)
- Requires capability in the control room to implement manual initiation at the division level of the automatically initiated protective actions; minimize the number of discrete operator manipulations required consistent with redundancy requirements (6.2 paragraph a)
- Requires capability in the control room to manually initiate and control protective actions not selected for automatic control (6.2 paragraph b)
- Requires capability to implement manual actions necessary to “maintain safe conditions” after the protective actions are completed, with the associated displays and controls located in areas that are accessible, in a suitable environment, and suitably arranged for operator surveillance and action (6.2 paragraph c).

The 1991 version of IEEE 603, which contained similar requirements, was endorsed by the NRC in Regulatory Guide 1.153 Rev. 1 [16]. Later, the standard was incorporated in 10 CFR 50.55a(h) along with its predecessor, IEEE 279 [4]. That regulation states that protection systems constructed after January 1, 1971, but before May 13, 1999, must meet the requirements in either IEEE 279 or IEEE 603. New plants should meet the requirements of IEEE 603.

It should also be noted that NUREG-0800 [10] Chapter 7, Appendix 7.1-C, *Guidance for Evaluation of Conformance to IEEE Std 603*, item 13 states that: “The review of information displays should...confirm that the information displayed and the characteristics of the displays (e.g., location, range, type, and resolution) support operator awareness of system and plant status and will allow plant operators to make appropriate decisions.”

*IEEE 497 - IEEE Standard Criteria for Accident Monitoring Instrumentation for Nuclear Power Generating Stations (2002) [5]*

This revision of the standard was intended to provide a consolidated source of post-accident monitoring requirements and bases for the new generation of advanced nuclear plant designs. In addition, the standard provides guidance allowing a flexible basis (less prescriptive than the

versions of Reg. Guide 1.97 that were in use at the time) for making changes to such systems in older plants. It also was specifically intended to provide criteria for advanced instrumentation systems designs, and for design modifications based on modern digital technology.

This IEEE standard was endorsed, subject to some specific regulatory positions stated by NRC, in the latest revision (Rev. 4) of Regulatory Guide 1.97 [15], discussed above.

DRAFT



# 3

## PROCESS FOR IDENTIFYING AND IMPLEMENTING THE MINIMUM INVENTORY

---

This section describes a process for identifying and implementing the minimum inventory of HSIs that are needed in addition to computer-based workstations with selectable displays and controls normally used by the operators. First, an overview is provided outlining the key elements of the approach. Then the process for new plants and a process for modernization of operating plants are described.

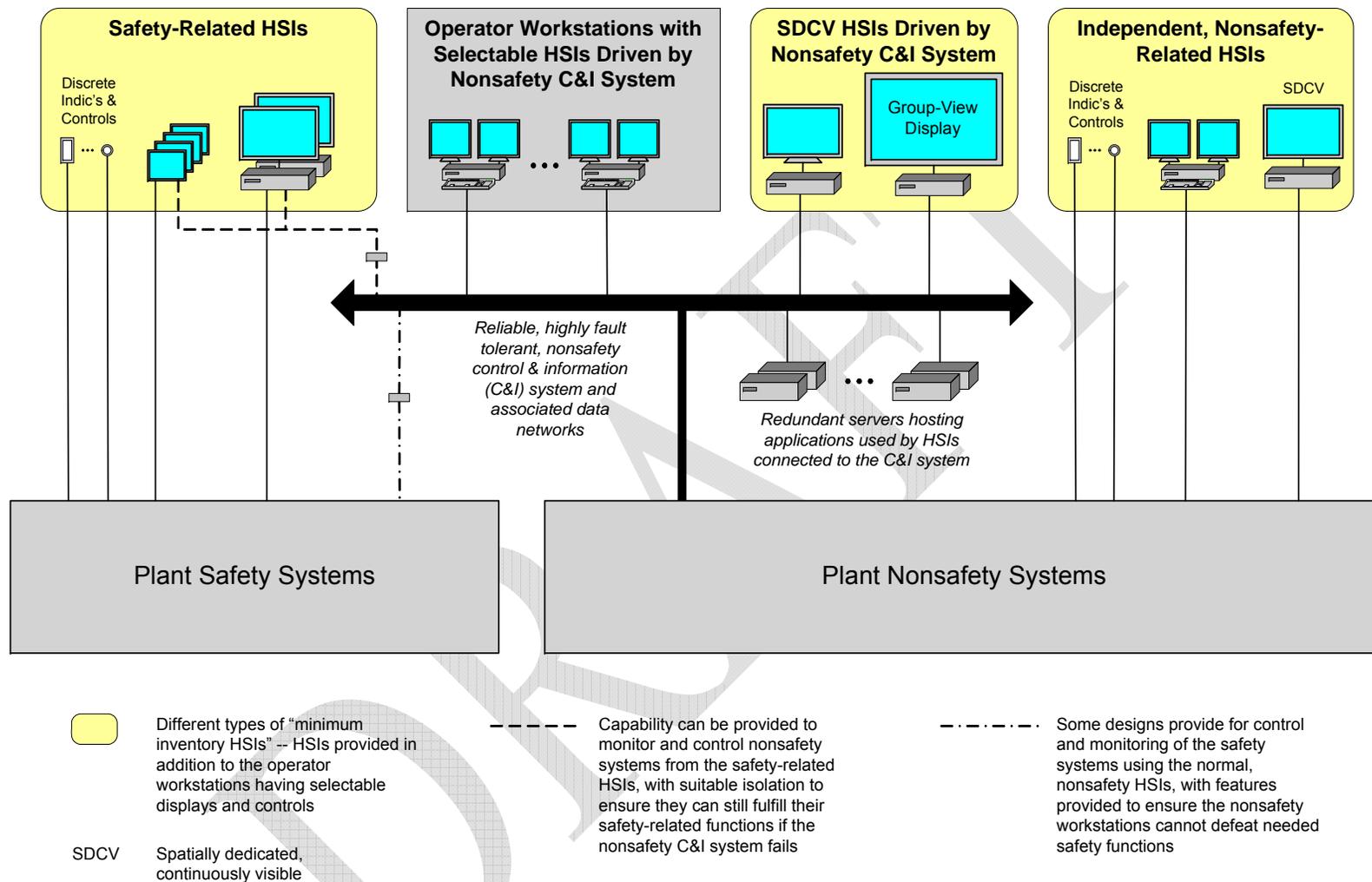
It is important to note that the determination of what minimum inventory of HSIs will be required and how they should be implemented interacts heavily with decisions on the I&C and HSI platforms to be used, the overall I&C and information systems architecture, and the plant's concept of operations. It is important to consider the I&C architecture and the HSI architecture together to assess failure modes of the integrated systems, identify coping strategies, and implement the minimum inventory HSIs as part of the overall design.

### 3.1 Overview

Figure 3-1 shows a generic, simplified architecture diagram, depicting a hypothetical digital control and information system driving workstations that provide the primary HSIs used by the operators during normal operation. These typically include selectable displays and soft controls presented on one or more video display units.

The figure also shows additional HSIs that provide capabilities not supported by the operator workstations, and which may be needed in a modern control room design. These include:

- Spatially dedicated, continuously visible (SDCV) displays driven by the nonsafety control and information system – for example, a flat panel display that shows alarms in fixed positions, such as a tile-replica display; large group-view displays, visible to the entire operating crew, also may be provided
- Safety-related HSIs – these may be qualified discrete digital or analog/hard-wired controls and indicators, or qualified computer-based HSIs; these may include SDCV computer-based displays.
- Nonsafety-related HSIs that are independent of the main control and information system that drives the operator workstations – again, these may include discrete controls and indicators and/or computer-based HSIs, and may include SDCV HSIs



**Figure 3-1**  
**Different Types of Minimum Inventory HSIs**

Note that the safety-related HSIs are (by regulation) independent of the nonsafety control and information system and associated operator workstations, and both the safety-related HSIs and independent, nonsafety-related HSIs achieve high reliability through redundancy (redundancy within themselves or redundancy to the functionality within the control and information system, or both). Note also that not all of these HSI types will be needed or desired. In fact, it is desirable to minimize the number of different types of HSIs. The intent of the figure is to show the possibilities that should be considered. This report provides guidance on determining what design requirements apply to HSIs that support safety and nonsafety functions and, based on those requirements, making design choices regarding what minimum inventory of HSIs should be provided in addition to the nonsafety operator workstations.

In order to determine what minimum inventory HSIs will be needed and how they will be implemented in the control room, it is necessary to:

- Determine what functions and tasks need to be supported by the HSIs
- Identify specific HSI resources (e.g., alarms, controls, displays, and procedures) required to support those tasks
- Determine what design requirements apply to the HSIs including those imposed by regulatory requirements, and particularly addressing requirements related to safety classification, independence, and accessibility.

An important input to this is the design of the control and information system architecture, 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.

Each of these items is discussed further below.

### **3.1.1 Categories of Functions and Tasks**

The minimum inventory HSIs and their design requirements should be identified based on what is needed to support the functions and tasks the operators must perform, and the applicable regulatory requirements. Many of the relevant functions and tasks are described in the emergency procedure guidelines (EPGs) or plant-specific emergency operating procedures (EOPs). The procedures typically identify multiple ways of accomplishing safety functions, or multiple success paths for recovering from abnormal events or accidents. Some of these use safety systems ("safety success paths") to accomplish the function, while others make use of non-safety systems ("non-safety success paths"). When multiple success paths are identified, the first one specified is typically the "preferred success path." The operators will choose this success path first if it is available. This may be a non-safety success path.

Another source of information on important functions and tasks is the plant's probabilistic risk assessment (PRA). The PRA should be consulted to ensure that all risk-significant operator actions and tasks have been identified. Section 5.2.6 of EPRI 1010042 [2] provides guidance on use of the PRA to support HSI design and licensing.

The following categories of functions and tasks should be addressed when identifying the minimum inventory HSIs:

Emergency Operations

1. Manual operator actions that are credited in the SAR safety analyses, for which no automated actions are provided
2. Monitoring and, when necessary, backing up automatic protective actions or automated success paths called out in the EOPs; this includes manual system-level actuations and use of manual component-level controls when necessary
3. Manual actions that are needed to accomplish the preferred manual safety success paths called out in the EOPs (including event-specific as well as symptom-oriented or functional procedures) for which there are no automated success paths. This does not include manual actions credited in the safety analysis, which are covered in the first category above.
4. Manual actions needed to accomplish preferred manual non-safety success paths called out in the EOPs (including event-specific as well as symptom-oriented or functional procedures)
5. Additional post-accident monitoring – use of Reg. Guide 1.97 [14,15] instrumentation for additional functions beyond the credited manual actions and backing up of the automatic systems covered in 1 and 2 above

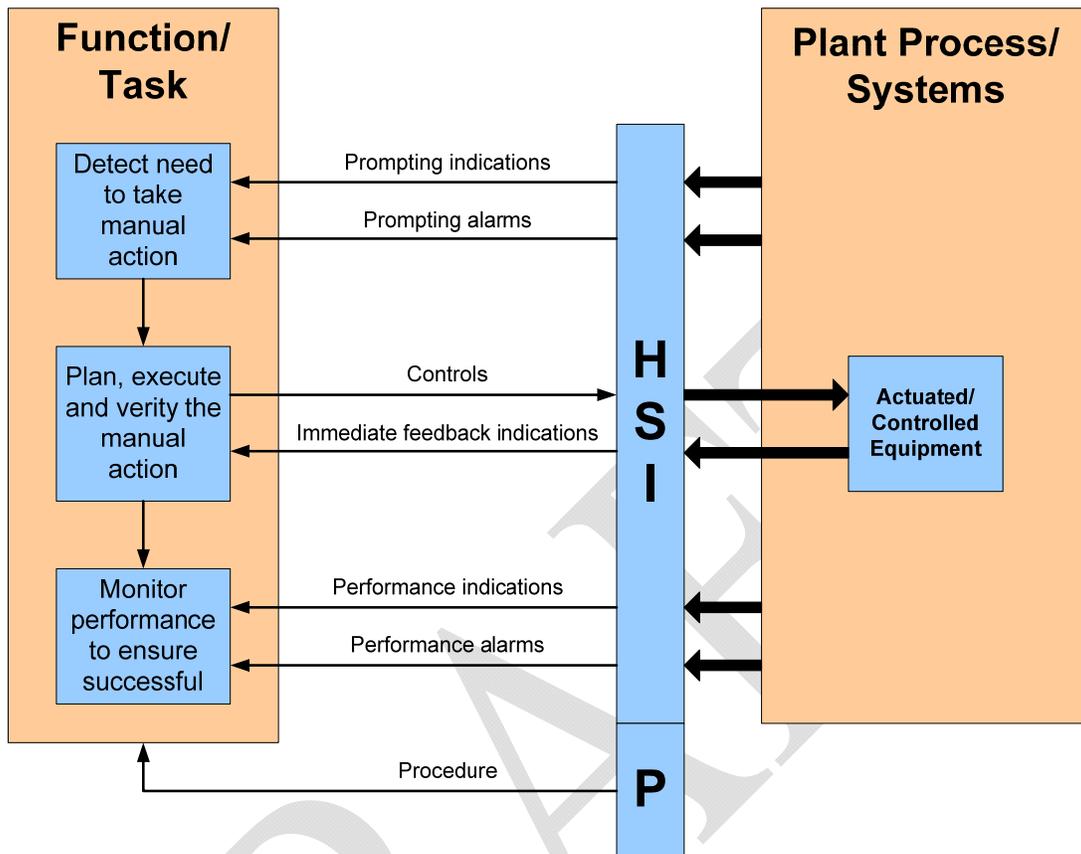
Normal (Non-Emergency) Operation

6. Monitoring safety system availability
7. Monitoring plant safety parameters (includes monitoring conditions that could lead to safety system actuation, and potentially taking pre-emptive action prior to actuation)
8. Functions and tasks other than the above that are needed to support continued operation under conditions in which the normally-used HSIs are failed or degraded – the extent of the functions and tasks that need to be performed depends on the plant's concept of operations for these conditions
9. Other important functions and tasks needed during normal operation, with all HSIs available, which may require HSI capabilities or characteristics not provided by the operator workstations (e.g., display of parameters important to maintaining situation awareness on a spatially dedicated display that is visible to the entire crew).

### **3.1.2 HSI Resources Needed**

For each task, typically there are multiple HSI resources needed to support the operator in performing the task. Figure 3-2 illustrates this for the example of a manual operator action. The needed HSI resources include:

- Indications and alarms used to detect the need to take the action (called prompting indications and alarms, typically indicating a threat to a critical safety function)
- Controls used to perform the action and indications that provide immediate feedback confirming that the action has been taken (e.g., pump status lights showing a pump has been turned on)
- Indications and alarms used to monitor performance of the actuated component or system to confirm that the manual action has been achieved (note this is different from confirming that the action has been taken (item above) and different from confirming that the end goal has been accomplished, which is ultimately restoring the critical safety function), and
- A procedure that prescribes how the task is to be performed and aids the operator in performing and confirming the necessary actions – the procedure may be in hardcopy form or provided as part of the HSI in a computerized implementation.



**Figure 3-2**  
**Examples Showing Types of HSI Resources Needed to Support a Manual Control Task**

Note that this is a simplified illustration only; a full task analysis would evaluate the function/task in more detail and identify detailed requirements for task support.

The HSI resources needed to support the tasks discussed in Section 3.1.1 should be identified. This may be done on a preliminary basis initially as design concepts are being developed to support control room conceptual design for a new plant or, for an operating plant modernization, to support definition of control room endpoint concepts. For a conceptual design an initial determination can be made of what controls, displays and alarms are likely to be needed for each type of minimum inventory HSI, and approximately how many of these there will be. This information can then be used to scope out early design concepts for implementing these HSIs. At this conceptual design stage detailed task analyses are not required. Task analyses would be needed later during detailed design to define specific HFE requirements related to the minimum inventory functions and tasks. Section 3.4 of EPRI 1010042 [2] and Section 5 of NUREG 0711 [8] provide guidance on performing task analysis.

### **3.1.3 HSI Design Requirements**

HSI design requirements should be determined for each category of functions and tasks, based on the applicable regulatory requirements and guidelines and the plant's concept of operations. The following types of design requirements should be addressed:

- Safety classification and associated requirements for HSI qualification
- Requirements for diversity and independence
- Requirements for hardware/software simplicity
- Accessibility requirements

These design requirements capture the primary design characteristics that are imposed by regulatory requirements and guidance and are important in determining the overall architecture of the HSIs in the main control room.

Each of these types of design requirements is discussed briefly below. Section 4 provides detailed guidance for determining the specific design requirements of each type that are applicable to the minimum inventory HSIs.

#### ***Safety Classification and Qualification Requirements***

Regulatory requirements dictate whether the HSIs for a particular function or task need to be safety-related. In some cases the existing regulatory requirements are very clear, but in others they are not so clear and are thus subject to some interpretation. Section 4 provides detailed guidance intended to help clarify the requirements and identify the minimum set of HSIs needed to support the different categories of functions and tasks.

It may be appropriate to apply a graded approach to qualification of HSIs performing functions with different levels of criticality or importance to safety. The design organization may already have established a graded approach for digital systems qualification, and this might be used to set appropriate criteria for qualification of different HSIs or HSI components. Full "1E" qualification of safety-related hardware and software will be required for HSIs that have the highest safety significance or impact on plant risk. However, other HSIs are of lower safety significance and may not require the same level of rigor in qualifying them for their specific safety-related purposes. The guidance in Section 4 identifies specific types of HSIs that may be candidates for applying a graded approach.

It should be noted that there is precedence for use of a graded approach to determining qualification requirements for HSIs. A graded approach to qualification was accepted for certain HSIs during the design certification of ALWRs. Also, Reg. Guide 1.97 Revision 3 [14] used a graded approach for setting design and qualification criteria for instrumentation and displays provided for post-accident monitoring. Use of a graded approach can be particularly important for software, where the level of software quality assurance can be graded depending on safety significance and complexity. Early interaction with NRC is recommended when applying graded approaches to digital system qualification.

### ***Independence and Diversity Requirements***

Regulatory requirements dictate that the safety-related HSIs be independent of the plant's nonsafety systems, including the control and information system. However, additional HSIs beyond the safety-related HSIs may be needed to provide operators with the capability to deal with failures of the operator workstations as discussed in Section 3.1.4. These must be independent of the normally-used workstations in the sense that they must not be subject to the same failures that are postulated for the workstations.

Branch Technical Position BTP 7-19 in Chapter 7 of the NUREG 0800 [10] calls for the capability to cope with potential common cause failures of the automatic protection systems, when those systems are implemented using digital technology. BTP 7-19 describes the NRC's expectations for a defense-in-depth and diversity (D3) evaluation to identify potential common cause failures (CCFs) and demonstrate that the plant has adequate coping capability to deal with them according to acceptance criteria specified in the branch technical position (points 1-3 of the NRC's 4-point position on defense-in-depth and diversity). Manual operator actions are often credited in these D3 evaluations. Thus any control room HSIs that are credited in the D3 evaluation must be diverse from the protection systems credited in the safety analysis for which the CCF is postulated, i.e., they must not be subject to the same common cause failure.

### ***Hardware/Software Simplicity Requirements***

Some of the minimum inventory HSIs may be subject to requirements for simplicity in the way they are implemented, in order to ensure that they are highly reliable and can be counted on to provide needed backup capabilities. For example, IEEE 603 (paragraph 6.2a) [6] states that:

*Means shall be provided in the control room to “implement manual initiation at the division level of the automatically initiated protective actions. The means provided shall minimize the number of discrete operator manipulations and shall depend on the operation of a minimum of equipment [emphasis added] consistent with the constraints of...” the redundancy and independence requirements contained in paragraph 5.6.1 of the standard.*

Regulatory Guide 1.62 [13] also includes a provision that manual system-level actuation should depend on a minimum of equipment.

Branch Technical Position BTP 7-19 of NUREG 0800 Chapter 7 [10] states in Point 4 of the four-point position on D3:

*“A set of displays and controls located in the main control room should be provided for manual system-level actuation of critical safety functions and for monitoring of parameters that support safety functions. The displays and controls should be independent and diverse from the computer-based safety systems...”*

In discussing the criteria for implementation of these displays and controls, BTP 7-19 further states that:

*“Displays and manual controls provided for compliance with Point 4 of the NRC position on D3 should be sufficient both for monitoring the plant state and to enable control room operators to actuate the systems that will place the plant in a hot shutdown condition. In addition, the displays and controls should be sufficient for the operator to monitor and control the following critical safety functions: reactivity level, core heat removal, reactor coolant inventory, containment isolation, and containment integrity. This additional manual capability is necessary in new reactors because all of the protection and control systems are digital-computer-based and thus vulnerable to common-cause failure. These controls provide plant operators with information and control capabilities that are not subject to common-cause failures due to software errors in the plant's automatic digital I&C safety system because they are independent and diverse from that system.*

*The point at which the manual controls are connected to safety equipment should be downstream of the plant's digital I&C safety system outputs. These connections should not compromise the integrity of interconnecting cables and interfaces between local electrical or electronic cabinets and the plant's electromechanical equipment. To achieve system-level actuation at the lowest possible level in the safety system architecture, the controls may be connected either to discrete hardwired components or to simple (e.g., the component function can be completely demonstrated by test), dedicated, and diverse, software-based digital equipment [emphasis added] that performs the coordinated actuation logic.*

Revision 5 of BTP 7-19 states that Point 4 applies to new plants and digital system modifications to operating plants.

### ***Accessibility Requirements***

As used here, accessibility refers to how easily and quickly an operator can access and use an HSI resource. Controls, displays and alarms that are accessed by navigating through a display hierarchy on a workstation, and making appropriate selections to bring up the needed information display or control, are considered less “accessible” than the discrete controls and displays provided on conventional control boards. However, use of conventional devices is not the only way to achieve good accessibility. Spatially dedicated displays can be driven by computer-based systems such that selected information is continuously visible to the operators (these are referred to as spatially dedicated, continuously visible or SDCV HSIs). Similarly, soft controls can be continuously displayed on dedicated screens located at fixed positions in the control room.

There are also intermediate levels of accessibility that can be provided, such as displays or controls that are selectable but require only one action to access them. These are not quite as accessible as SDCV HSIs, but they are more accessible than those that require navigation through a series of menus or other multi-step selection process to reach the desired control or display.

### **3.1.4 HSI Failure Modes and Backup Operational Capabilities**

Designers and plant owners should consider the possibility for control and information system failures during normal operation, when no accident has occurred. If operators in the control room rely primarily on HSIs driven from the control and information system for monitoring and controlling the plant, potential failures or degradation of this capability need to be considered<sup>4</sup>. The nature and extent of failures that can occur, how often they may occur over the life of the plant, and their potential duration when they do occur, will drive decisions on what alternate or backup capability should be provided beyond the safety-related HSIs already required by regulation. Also, the extent of backup HSI capability that will be needed will depend on the chosen 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. These choices can have a major impact on the control room design.

#### **3.1.4.1 Control and Information System and HSI Failure Modes**

Credible failure modes of the control and information system and the associated HSIs should be identified, and the designer and/or plant owner should determine what failures will be addressed as part of overall control room design. The failure analysis should consider single failures and potential common cause failures, including those that may result from software or digital system design flaws and maintenance errors, including software maintenance. This needs to be a realistic evaluation of possible failures, asking questions such as:

- Could the failure occur during the lifetime of the plant<sup>5</sup>?
- If so, how frequently might it occur?
- How will it be detected and how long will this take (including consideration of possible “silent” failures)?
- How long might it take to diagnose the problem once it is detected, identify and correct the fault, return the system to operation, and verify it is operating correctly and can be relied upon for continued operation?

This is far from an exact science, and relies heavily on informed judgment. The intent is not to come up with precise numbers for any of these. Rather, the objective is to determine what could happen and what the operational consequences would be, and then to set some design basis

---

<sup>4</sup> The first step in protecting against failures of the control and information systems is employing highly reliable hardware and software in an architecture that provides defense against large-scale failures. Also, suitable quality assurance measures should be taken when developing applications on the chosen platform. Special scrutiny should be applied for critical applications important to plant availability and investment protection and those important to safety such as SPDS, ATWS, and computerized emergency procedures. This should ensure that the control and information system is highly reliable and has very high availability. However, even when these measures have been taken, the potential for system failures still should be considered, and their potential impact should be examined as discussed in this section.

<sup>5</sup> It is important to remember that even if the answer to this question is no, regulatory requirements dictate that safety-related HSIs be provided independent of the nonsafety control and information systems to support accident mitigation and safe shutdown.

assumptions about the postulated failure modes that can be used in designing (or retaining) suitable backup capabilities.

Two additional important questions are:

- What defensive design measures might be taken in the design and configuration of the control and information systems to prevent or minimize the likelihood or duration of troublesome failures?
- What is the basis for concluding that a particular failure will not occur during the remaining plant life?

Again, this will involve using judgment as well as data that may be available from the equipment vendor.

For commercial systems, there may be a large installed base with extensive experience that can be examined to evaluate the potential for failures. However, it will be important to examine the applicability of this experience to the planned installation, preferably by talking to actual end users as well as the vendor. Questions that should be asked here include:

- What are the differences between the majority of installations whose experience is to be considered and the installation to be done at this plant?
- Are those installations using the same architecture?
- Are they using the same software versions, including operating systems and application software?
- Are they using the same hardware versions?
- If not, are they using hardware or software versions that are sufficiently similar that the comparison is valid?
- Are the power supply arrangements the same or similar, including a comparably reliable source of power?

EPRI TR-106439 [3] provides guidance on evaluating the dependability of commercial digital equipment, including guidance on use of operating history in the evaluation. EPRI 1002835 [1] provides guidance on identifying and evaluating defensive measures that may have been taken in the design of the equipment/system that influence the likelihood of failures, particularly common cause failures due to software or digital system design faults. Although both of these documents focus primarily on other issues, the guidance they contain can and should be used for evaluation of nonsafety-related digital systems including the control and information systems and associated HSIs.

The failure analysis should consider as a minimum the following types of failures<sup>6</sup>:

---

<sup>6</sup> The discussion here addresses only failures that impact the HSIs. Control system failure analysis should address other failures such as loss of automatic control functions, and the associated impact on the operators. Such failures are not within the scope of this report as it deals only with HSI failures and the need for backup HSIs.

- Loss of one or more operator workstations, such that displays go dark or freeze or are impaired in some way. Consider in particular failures that can affect multiple or all workstations in the control room, degrading some or all alarm and information display and/or soft control capabilities. Consider loss of critical operator prompts that continue to be sent from automation that remains functional, but the prompts are not displayed because of HSI failure.
- 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. This should include wireless as well as wired networks. While redundancy within communication networks can reduce the frequency of these types of failures, this redundancy is typically not coupled with physical separation and there may still be single points of failure. Thus redundancy alone may not completely preclude such failures. (Also see the discussion below about potential loss of automatic control functions.)
- 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 – for example, servers that provide graphical displays to the workstations, databases containing needed real-time or static (e.g., configuration) data, calculations or algorithms providing data needed in displays, or which provide advanced control capabilities, alarm processing, or computer-based procedures
- Loss of power causing failure or degradation of the HSIs – the nonsafety workstations may not be powered from vital buses backed by station batteries. Loss of offsite power and other major power loss events such as station blackout should be examined to determine whether and how long the HSIs and their data sources will continue to operate, and whether loss of these HSIs could complicate a loss of offsite power or station blackout event.

The analysis should examine the overall system architecture and its design basis, the data sources and communication networks used, the assignment of applications to processors, and where redundancy or other defensive measures have been incorporated to prevent or significantly reduce the likelihood of failures. Modern data communications and switching technologies (e.g., reconfigurable networks), which are more fault tolerant than simple dual redundant buses, may significantly reduce the likelihood of some large-scale failures. Careful assignment or distribution of applications and functions within the system can have a significant impact on the determination of what failures need to be considered. Design decisions on power supply arrangements and the use of battery backups also can have a major impact on potential for large-scale failures.

#### 3.1.4.2 Concept of Operations for Failed/Degraded Conditions

Beyond the regulatory requirement for safety-related HSIs for accident mitigation and safe shutdown, the extent of the additional HSI capability that is needed to handle HSI failures depends to a great extent on how the plant wants to respond to the identified HSI failure modes, i.e., the concept of operations for these degraded conditions. A number of options are possible,

including but not limited to the following. Note that these all assume that the reactor is at power and no secondary event or accident has occurred. They are listed in order of increasing capability of the backup HSIs that would be needed:

**Trip.** Immediately trip the plant and use the qualified controls and displays already provided in the MCR to meet regulatory requirements, plus local controls and indications as necessary to reach a safe shutdown condition. This approach requires no additional HSI capability, because the main control room must include safety-related HSIs sufficient to achieve safe shutdown independent of the nonsafety HSIs. However, it may not be the lowest-risk approach, from either a safety or economic standpoint. Other options should be considered if it is expected that large-scale HSI failures may occur multiple times during the plant life. Also, the plant designer or owner should consider whether the intent is to reach hot or cold shutdown. Some operating plants' licensing basis for the safety-related controls and indications in the main control room is based on achieving hot shutdown, while others are based on reaching cold shutdown. The concept of operations for HSI failure should be based on one or the other.

**Safely shut down using preferred means.** 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 to 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 (i.e., an administrative limit) or a Limiting Condition of Operation (LCO) associated with the HSI failure.

**Hold for a finite but not pre-determined time.** Continue operating the plant 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 pre-determined length of time. (An LCO might, however, specify restrictions on operation intended to prevent transients or upsets from being triggered.) There is precedent for this type of situation, where the safest route is to continue operating the plant at power rather than attempting to shut it down, because of the reduced capability to handle problems that may arise as the plant goes through the transients and state changes associated with shutdown. This option requires the greatest amount of backup HSI capability in the control room, potentially including indication of pre-trip conditions so the control room operators can quickly determine whether conditions are present that may require pre-emptive action to shut down. It may also require stationing additional personnel at locations in the plant for monitoring of local indications, and/or setting up temporary instrumentation either inside or outside the main control room.

For some of the functions and tasks required by the chosen concept of operations, local controls and indications may be used to accomplish the functions. However, the number of auxiliary

operators available to perform these functions and the time frame in which they must be accomplished will need to be considered. Also, the degree to which local control stations rely on the same control and information systems or networks can have an impact here. If some local controls and indications are affected by the same failures, then local actions at those stations cannot be counted on for situations in which the control room HSIs have failed.

In all cases, there should be an intensive effort to restore the normally-used HSIs to service. For the last option, continued operation for a finite but not pre-determined time, the plant's safety review committee, or plant operations review committee, should monitor the situation on an ongoing basis and determine whether operation could continue while repair efforts are being made, or if the plant should be shut down. The plant's emergency action plan should specify, for the anticipated HSI failure conditions, what notifications would be required (e.g., what conditions would require declaration of an Unusual Event) and the time limits for making the required notifications.

#### 3.1.4.3 Implementing the Backup HSIs

Backup HSIs for coping with failure of the normally-used HSIs can be implemented using a conventional or computer-based design, and safety-related or nonsafety-related HSIs, as long as the equipment is not subject to the same failure modes for which it is intended to provide backup. Section 5 discusses options for implementation of the needed backup HSI capabilities as part of the minimum inventory.

### 3.2 New Plant Designs

For a new plant, the minimum inventory HSIs should be identified and implemented as part of the overall control room design. As discussed in Section 3.1, this includes:

- Identifying the specific functions and tasks that need to be supported by the minimum inventory HSIs – Section 3.1.1 gives the categories of functions and tasks that should be considered
- Identifying the specific HSI resources (e.g., alarms, controls, displays and procedures) required to support those tasks – Section 3.1.2 provides examples of the types of HSIs resources that should be considered
- Determining what design requirements apply to the HSIs – important types of design requirements are discussed in Section 3.1.3
- Identifying and evaluating design options and selecting a final design concept for implementation of the minimum inventory HSIs

Inputs to the process include the following:

- Plant design basis
- Overall concept of operations for the plant including staffing goals
- Initial concepts for the overall I&C and information systems architecture

- Emergency procedure guidelines (EPGs) or plant-specific emergency operating procedures (EOPs), including event-specific as well as symptom-oriented or functional procedures
- Plant probabilistic risk assessment (PRA)
- Industry and regulatory standards and guides applicable to the plant design
- Diversity and defense-in-depth (D3) evaluation results
- Results of failure modes analysis for the control and information systems including credible failures, their frequency, effects, and duration and the concept of operations chosen for the identified failure modes – Section 3.1.4 provides guidance here

As discussed earlier, this activity is dependent on and interacts with decisions on the architecture of the I&C and information systems. Iteration between these activities may be needed to arrive at a final integrated solution that satisfies all the applicable requirements and design constraints.

Also, as part of the control room design process, appropriate HFE principles and analyses should be applied in developing and validating the design of the minimum inventory HSIs in concert with the rest of the control room, integrating the minimum inventory HSIs into the overall control room design.

### **3.3 Modernization of Operating Plants**

For an operating plant that plans to modernize its control room, the process is somewhat more complicated. The plant typically does not start over with a clean sheet of paper to design the new control room, but rather determines how the control room can be changed over time to approach a desired endpoint. The process illustrated in Figure 3-3 can be used for identification and implementation of the minimum inventory HSIs as part of the modernization design effort.

As shown in the figure, an initial identification of minimum inventory HSIs and their design requirements is made as part of the effort to define a design concept for the control room endpoint – the target design concept for the control room at the end of the modernization program. Detailed design and implementation of the minimum inventory HSIs occurs in one or more modifications depending on how the plant decides to stage the modernization. The figure identifies some of the important inputs or sources of information that can be used at each step in the conceptual design effort, including the Minimum Inventory HSI Design Requirements Matrix discussed above. The same inputs will be used to support the final design of the control room modifications. The design changes should be validated as part of the overall HFE design and evaluation process.

Two types of reviews can be performed to identify the minimum inventory HSIs – a “top-down” review and a “bottom-up” review. At a minimum, a top-down review should be performed. The top-down review starts with the tasks (see Section 3.1.1) and identifies the HSI resources needed to support them (see Section 3.1.2). The top-down review should include the following activities:

**Review EOPs.** A key part of the top-down review is an examination of the plant's emergency operating procedures (EOPs) for mitigating accidents and achieving safe shutdown. This should include event-specific procedures as well as symptom-oriented or functional procedures not tied to any specific event. Only the procedures and procedure steps that address the functions and tasks identified in Section 3.1.1, for which minimum inventory HSIs may be needed, will require review. For example, once the preferred automatic or manual safety success path has been reviewed for a given event, and (depending on the concept of operations for HSI failure) the preferred non-safety success path, no further review may be needed for that event. Additional alternate or contingency paths need not be reviewed. Also, some procedures address events in which multiple failures of safety systems or functions occur, for which it is not reasonable to also postulate failure of the HSIs. Judgment should be used in determining which events and failure scenarios need to be reviewed for identifying minimum inventory HSIs.

When conducting this EOP review it is important to identify which actions are to be taken out in the plant as well as inside the control room. Availability of auxiliary operators to perform actions outside the main control room should be considered.

**Identify Reg. Guide 1.97 Variables and Associated Displays.** The plant's safety analysis report (SAR) or other documents should be reviewed to identify Reg. Guide 1.97 [14,15] variables. The specific HSI devices that are credited for display of these variables should be identified.

**Identify Manual System-Level Actuation Controls.** Identify the specific manual system-level actuation controls provided in accordance with Reg. Guide 1.62 [13].

**Review Credited Manual Operator Actions.** Review the plant SAR or other documents to identify the specific manual operator actions credited in the SAR safety analysis for design basis events, for which no automatic action is provided. For each of these, identify the required HSI resources including prompting indications, alarms, controls, immediate feedback indications, and performance indications and alarms.

**Review PRA for Risk-Significant Operator Actions.** A review of the plant's probabilistic risk analysis (PRA) can help identify any additional operator actions or tasks that are risk significant and should be addressed when defining what additional HSIs may be needed. Identify which of these, if any, should be supported during the postulated HSI failure conditions, and have not already been identified from the reviews above.

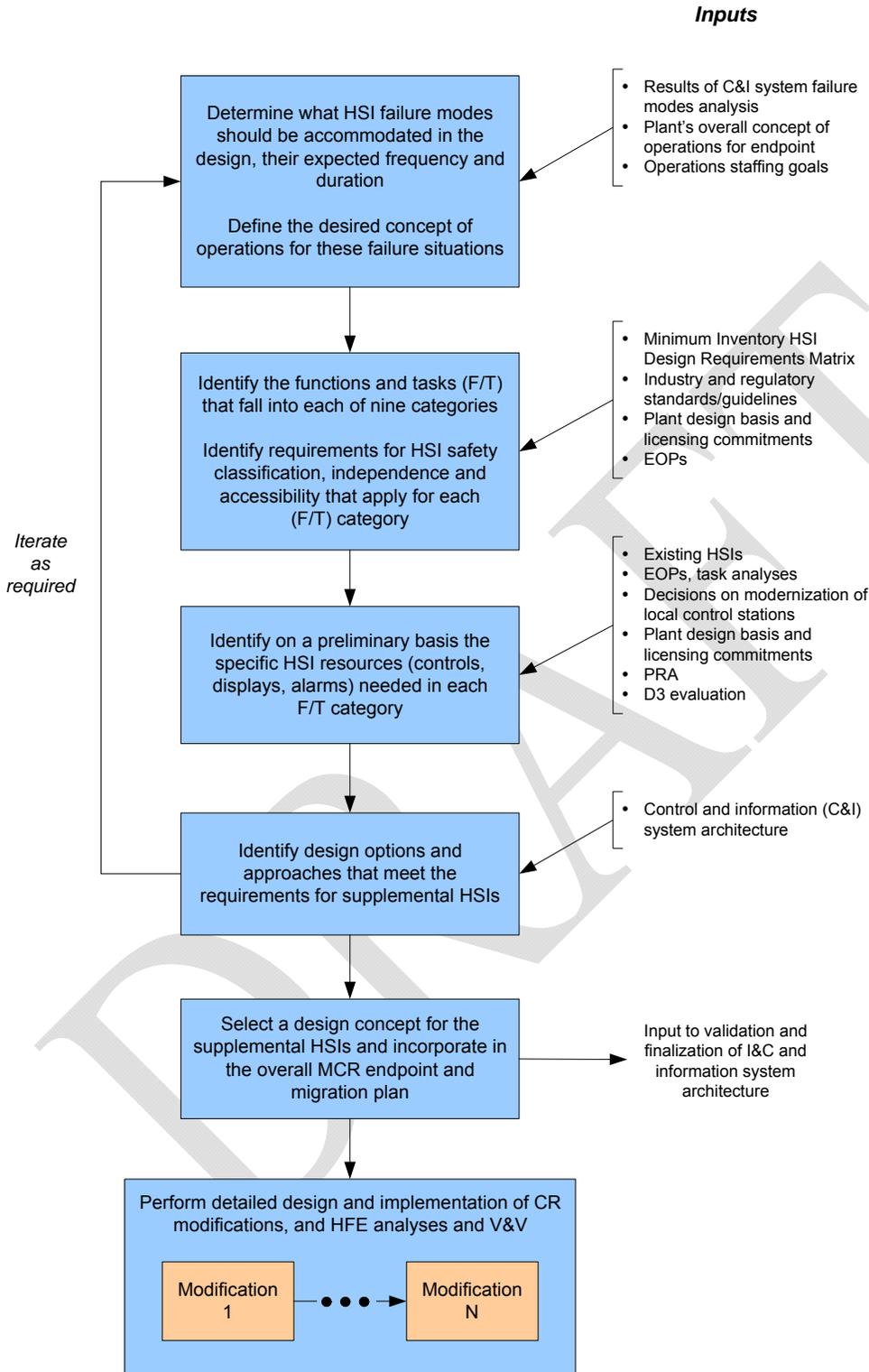
**Review D3 Evaluation.** Review the results of the D3 evaluation performed in accordance with BTP 7-19, or perform an initial scoping evaluation if the full evaluation has not yet been performed. Identify specific manual operator actions credited for coping with software/digital common cause failures of the RTS and ESFAS. Determine what specific HSI resources are required to support these actions. Also, examine the position taken on Point 4 of BTP 7-19 [10], and the manual controls and supporting indications (if any) credited for compliance with Point 4. Note that, depending on the system architecture and implementation of the qualified, manual system-level actuations used to meet Reg. Guide

1.62 [13], the same controls may be sufficient to meet the Point 4 requirements (they must be shown not to be vulnerable to potential software/digital common cause failures in RTS/ESFAS). The required safety function indications also may overlap with those required to meet Reg. Guide 1.97 (Type B variables) [14,15].

***Identify HSI Resources Needed for Remaining Tasks.*** Evaluate all other functions and tasks addressed in Section 3.1.1 to determine what additional HSI resources are needed for each category. This includes HSIs needed to support continued operation on failure of the normally-used HSIs, if this is part of the chosen concept of operations.

The bottom-up review examines the existing controls, indicators, and alarms provided in the current control room to ensure that all those needed to support the functions and tasks have been identified. This review also can be used to capture the current HSI components in an inventory or database for use in identifying an appropriate disposition for each of them in the final endpoint design (e.g., retain, move, transfer to the new digital system, implement as part of a minimum inventory HSI, etc.).

Some HSI resources will support multiple functions/tasks, each having a different set of HSI design requirements. In this case, the most stringent requirements should be determined for each HSI resource (see Section 3.1.3 for guidance on identifying the HSI design requirements).



**Figure 3-3**  
**Process for Identifying and Implementing Minimum Inventory HSIs as Part of Control Room Modernization**

# 4

## DESIGN REQUIREMENTS

---

The sub-sections below provide guidance for determining design requirements for each category of functions/tasks. These are presented roughly in order of decreasing safety significance. Minimum requirements based on the regulations, or on regulatory guides to which most plants are committed, are specified. Additional guidance is provided in areas where the regulatory requirements are not clear or are absent.

It is important to note that the same HSIs may support multiple functions or tasks. Each sub-section addresses HSIs that have not already been covered in an earlier sub-section. So, for example, if an EOP success path makes use of system-level actuation controls discussed in the earlier sub-section related to backing up automated success paths, they are not discussed again. Each HSI should meet the most stringent requirements that apply.

For each function/task, the applicable HSI resources (e.g., prompting indications, alarms, controls, procedures, etc.) are addressed separately. See Figure 3-2 for an illustration of the different types of HSI resources.

The guidance is summarized in Table 4-1. The table lists the categories of functions/tasks identified in Section 3.1.1 and the HSIs that pertain to each. The columns of the table correspond to the types of HSI design requirements noted in Section 3.1.3. Applicable regulatory and industry requirements and guidance documents are also identified in the table.

For convenience, Table 4-2 provides a summary list, drawn from Table 4-1 and the accompanying text, of (1) the minimum set of HSIs that need to be safety-related, and (2) the minimum inventory of HSIs that should be spatially dedicated and continuously visible (SDCV), based on the guidance in this section. The section number where applicable guidance is provided is indicated for each item.

Note that this guidance identifies the **minimum** set of HSIs that should be safety-related, and the **minimum** set that should be SDCV. This is not meant to imply that the design cannot or should not provide additional HSIs in either of these two categories. The design process for a new control room or modernization of an existing control room may identify additional HSIs that should be safety-related or others that should be SDCV. For example, the evaluation of failure modes and development of accident mitigation strategies may conclude that HSIs beyond the minimum set identified here should be implemented on a safety-related platform. The HFE design process or simulator testing and validation may identify additional HSIs that could benefit from SDCV implementation.

DRAFT

**Table 4-1  
Minimum Inventory HSI Design Requirements Matrix**

Functions/Tasks and Associated HSIs	HSI Design Requirements <sup>1</sup>		Applicable Regulatory and Industry Requirements and Guidance <sup>4</sup>
	Safety Classification <sup>2</sup>	Accessibility <sup>3</sup>	
<b>1. Perform Credited Manual Actions (Section 4.1)</b>			
Prompting indications	SR  See text for discussion of trend display vs. primary indicator	SDCV for at least one channel  The SR HSI can be selectable if a NSR HSI is provided that is highly reliable and SDCV	IEEE 603 (§5.8.1, §5.8.4)  Reg. Guide 1.97 Rev. 3 (Type A; Category 1)  Reg. Guide 1.97 Rev. 4 (Type A)
Prompting alarms	Operating plants: NSR <sup>5</sup>  New plants: SR if needed to prompt credited manual action <sup>6</sup>	SDCV	None <sup>6</sup>
Controls & immediate feedback indications	SR	SDCV  One-step accessible is acceptable if supported by appropriate HFE analyses	IEEE 603 (§6.2)
Performance indications	SR* for primary indications  Secondary indications can be NSR	SDCV for primary indications  Secondary indications can be selectable	None
Performance alarms	NSR <sup>5</sup>	Selectable	None
Procedures	SR* or paper (procedures can be provided on a NSR platform, but then backups should be provided as SR* or paper)	Selectable	None
<b>2. Monitor Safety Functions and Back Up Automatic Success Paths (Section 4.2)</b>			
Indications of the status of critical safety functions	SR*	SDCV for one of the redundant indications  The SR HSI can be selectable if a NSR HSI is provided that is highly reliable and SDCV	Reg. Guide 1.97 Rev. 3 (Type B; Category 1)  Reg. Guide 1.97 Rev. 4 (Type B)
Alarms indicating challenges to critical safety functions	NSR <sup>5</sup>	SDCV	NUREG 0700

Functions/Tasks and Associated HSIs	HSI Design Requirements <sup>1</sup>		Applicable Regulatory and Industry Requirements and Guidance <sup>4</sup>
	Safety Classification <sup>2</sup>	Accessibility <sup>3</sup>	
<p>Indications of the status of fission product barriers:</p> <p>If following Reg. Guide 1.97 Rev. 3</p> <p>If following Reg. Guide 1.97 Rev. 4</p>	<p>SR*</p> <p>SR*</p>	<p>SDCV for one of the redundant indications if Category 1 per Reg. Guide 1.97 Rev. 3</p> <p>The SR HSI can be selectable if a NSR HSI is provided that is highly reliable and SDCV</p> <p>Selectable</p>	<p>Reg. Guide 1.97 Rev. 3 (Type C, Category 1)</p> <p>Reg. Guide 1.97 Rev. 4 (Type C)</p>
<p>Indications related to safety system operation:</p> <p>If following Reg. Guide 1.97 Rev. 3</p> <p>If following Reg. Guide 1.97 Rev. 4</p>	<p>SR* if Category 1 per Reg. Guide 1.97 Rev. 3</p> <p>NSR</p>	<p>SDCV for one of the redundant indications if Category 1 per Reg. Guide 1.97 Rev. 3</p> <p>The SR HSI can be selectable if a NSR HSI is provided that is highly reliable and SDCV</p> <p>Selectable</p>	<p>Reg. Guide 1.97 Rev. 3 (Type D, Category 1)</p> <p>Reg. Guide 1.97 Rev. 4 (Type D)</p>
Alarms on fission product barriers and safety system operation	NSR	Selectable	None
Indications of safety system actuation status	NSR	<p>SDCV display for high-level summary indications</p> <p>Component-level details can be on selectable displays</p>	IEEE 603 (§5.8.2)
Alarms on safety system actuation failures	NSR	<p>SDCV display for high-level summary alarms</p> <p>Component-level details can be on selectable displays</p>	None
Manual system-level actuation controls	<p>SR</p> <p>Dependent on a minimum amount of equipment</p>	SDCV	<p>Reg. Guide 1.62</p> <p>IEEE 603 (§6.2a)</p>

Functions/Tasks and Associated HSIs		HSI Design Requirements <sup>1</sup>		Applicable Regulatory and Industry Requirements and Guidance <sup>4</sup>
		Safety Classification <sup>2</sup>	Accessibility <sup>3</sup>	
	Manual component-level controls	No specific requirements if not used for credited manual actions (item 1 above), or for preferred manual safety and non-safety success paths identified in EOPs (items 3 and 4 below).		None
	Procedures for monitoring safety functions and backing up automated success paths	SR* or paper (procedures can be provided on a NSR platform, but then backups should be provided as SR* or paper)	Selectable	None
D3 Points 1-3 – HSIs needed for specific manual actions credited in the D3 evaluation for coping with CCFs:				
	Prompting indications	NSR	As determined by appropriate HFE analyses	BTP 7-19, Points 1-3
	Prompting alarms	Independent of the protection system common cause failures (CCFs) they are intended to address	SDCV	No specific guidance
	Manual controls		As determined by appropriate HFE analyses	BTP 7-19, Points 1-3
D3 Point 4 – HSIs needed for monitoring safety functions and for system-level actuations for D3:				
	Safety function indications	NSR	SDCV	BTP 7-19, Point 4
	Safety function alarms	Independent of the computer-based safety systems	As determined by appropriate HFE analyses	No specific guidance
	Controls for system-level actuations		SDCV	BTP 7-19, Point 4
D3 coping procedures:				
	Procedures needed for D3 coping	NSR or paper Independent of the protection system common cause failures (CCFs) they are intended to address	Selectable	BTP 7-19 addresses D3 coping but gives no specific guidance on procedures
<b>3. Carry Out Preferred Manual Safety Success Paths (Section 4.3)</b>				
	Prompting indications	SR*	Selectable	IEEE 603 (§6.2c) Reg. Guide 1.97 Rev. 4 (Type D)
	Prompting alarms	Prompting alarms are not required as actions are prompted by EOP execution		None
	Controls & immediate feedback indications	SR*	Selectable	IEEE 603 (§6.2c)
	Performance indications	SR*	Selectable	None
	Performance alarms	NSR <sup>5</sup>	SDCV	None

Functions/Tasks and Associated HSIs		HSI Design Requirements <sup>1</sup>		Applicable Regulatory and Industry Requirements and Guidance <sup>4</sup>
		Safety Classification <sup>2</sup>	Accessibility <sup>3</sup>	
Procedures needed for accident mitigation and achieving safe shutdown		SR* or paper (procedures can be provided on a NSR platform, but then backups should be provided as SR* or paper – see text for discussion of minimum set of procedures required)	Selectable	None
<b>4. Carry Out Preferred Manual Non-Safety Success Paths (Section 4.4)</b>				
	Prompting indications	NSR	Selectable	None
	Prompting alarms			
	Controls & immediate feedback indications			
	Performance indications			
	Performance alarms		SDCV	
	Procedures	NSR or paper	Selectable	
<b>5. Perform Additional Post-Accident Monitoring (Section 4.5)</b>				
	Indications	SR* if Category 1 in Reg. Guide 1.97 Rev. 3  No qualification requirement if following Reg. Guide 1.97 Rev. 4	SDCV if Category 1 in Reg. Guide 1.97 Rev. 3	Reg. Guide 1.97 (Type E)
	Alarms	NSR <sup>5</sup>	SDCV	None
	Procedures	SR* or paper (procedures can be provided on a NSR platform, but then backups should be provided as SR* or paper)	Selectable	None
<b>6. Monitor Safety System Availability (Section 4.6)</b>				
	System-level indications	NSR	SDCV	10 CFR 50.34(f)(2)(v)  Reg. Guide 1.47  IEEE 603 (§5.8.3)
	System-level alarms		SDCV	
	Component-level indications		Selectable	None
	Component-level alarms		Selectable	

Functions/Tasks and Associated HSIs	HSI Design Requirements <sup>1</sup>		Applicable Regulatory and Industry Requirements and Guidance <sup>4</sup>
	Safety Classification <sup>2</sup>	Accessibility <sup>3</sup>	
<b>7. Monitor Plant Safety Parameters (Section 4.7)</b>			
Safety parameter indications	NSR	SDCV or one-step accessible display prompted by SDCV alarms (see next row)	10 CFR 50.34(f)(2)(iv) NUREG 1342 NUREG 0700
Safety parameter alarms		SDCV	NUREG 0700
Other prompting indications for pre-emptive safety actions		Selectable	None
Other prompting alarms for pre-emptive safety actions		SDCV	
Controls for pre-emptive safety actions	No additional requirements. Manual system-level actuation controls (in item 2 above) can be used to take pre-emptive actions.		
<b>8. Continue Operation Under Conditions of Failed/Degraded HSIs (Section 4.8)</b>			
<b>Note: The chosen concept of operations will determine which of the following operations need to be supported by additional, independent HSIs</b>			
Safely shut down the plant using preferred non-safety success paths:			
Indications, alarms, and controls for preferred non-safety success paths	NSR, independent of the normally-used HSIs  Or implement on same platform as safety-related HSIs	Determine based on appropriate HFE analyses	None
Procedures for use of preferred non-safety success paths	NSR, independent of the normally-used HSIs; or on paper	Selectable	
Maintain stable plant operation for a pre-determined time (governed by Tech Spec LCO or administrative limit):			
Additional HSI resources desired to support maintaining operation (e.g., alarms for investment protection)	NSR, independent of the normally-used HSIs	Determine based on appropriate HFE analyses	None
Procedures for maintaining stable operation for a pre-determined time	NSR, independent of the normally-used HSIs; or on paper	Selectable	
Continue operation for a finite but not pre-determined time (not governed by Tech Spec LCO):			
Safety parameter alarms	NSR, independent of the normally-used HSIs	Determine based on appropriate HFE analyses	None
Other prompting indications and alarms for pre-emptive safety actions			

Functions/Tasks and Associated HSIs	HSI Design Requirements <sup>1</sup>		Applicable Regulatory and Industry Requirements and Guidance <sup>4</sup>
	Safety Classification <sup>2</sup>	Accessibility <sup>3</sup>	
HSI resources needed to perform required Tech Spec surveillances Alarms desired for investment protection Procedures for continuing operation for a finite but not pre-determined time (including tech spec surveillance procedures)	NSR, independent of the normally-used HSIs	Determine based on appropriate HFE analyses	None
<b>9. Perform Other Important Tasks During Normal Operation With All HSIs Functioning (Section 4.9)</b>			
HSI resources needing enhanced accessibility – for example, key indications, alarms or controls supporting plant power production or investment protection; alarms requiring prompt operator action; indications important to maintaining situation awareness	NSR	Consider SDCV or one-step accessible for these, based on appropriate HFE analyses	None
<b>Notes:</b> <p><sup>1</sup> Minimum requirements that are either explicitly stated in the regulatory documents or can be clearly inferred from them, are provided where applicable. In cases where the regulatory requirements or guidance documents are not very clear, subject to interpretation, or non-existent, additional guidance is provided as appropriate.</p> <p><sup>2</sup> This column identifies those HSIs that should be implemented using safety-related equipment. Those designated SR should be implemented as safety-related HSIs. Those designated SR* should also be safety-related, but are good candidates for application of a graded approach to qualification, particularly software qualification, due to their lower level of safety significance. Those designated NSR are not required to be safety-related, i.e., they may be implemented using nonsafety-related equipment.</p> <p>All of the safety related HSIs must, per regulation, be independent of the nonsafety HSIs. However, some HSIs have additional requirements for independence, diversity or simplicity – these requirements are included where applicable in the Safety Classification column.</p> <p><sup>3</sup> Accessibility relates to the amount of effort required by the user to access a specific HSI resource. The most accessible HSIs are those that are spatially dedicated and continuously visible (SDCV), requiring no action on the part of the user in order to access and use the HSI resource. The next most accessible are those that require only one action in order to access the control or information display, referred to here as “one-step accessible.” The least accessible are those that require multiple actions (e.g., navigating through a hierarchy of screens or a menu system) to access the needed resource. These are referred to as “selectable.”</p> <p><sup>4</sup> This column identifies regulatory and industry guidance documents, where available, that provide related guidance. In some cases there is no guidance, or the guidance that is available is not clear and requires interpretation. The table and accompanying text provide guidance to fill these gaps.</p> <p><sup>5</sup> Although there is no requirement that these alarms be safety related, consider providing alarm capability on the same safety related display that is used for the associated indications.</p> <p><sup>6</sup> The SRM to SECY-93-087 [18] 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.O) [10] has similar provisions.</p>			

**Table 4-2**  
**Summary List of Safety-Related and SDCV or One-Step Accessible HSIs**

<b>Minimum Inventory HSIs</b>	<b>Guidance Section</b>
<b>Minimum set of HSIs that should be safety-related (designated SR in Table 4-1):</b>	
Prompting indications (Reg. Guide 1.97 Type A), controls and immediate feedback indications for credited manual actions	4.1
Controls for manual system-level actuation of safety systems	4.2
<b>Minimum set of HSIs that should be safety-related but are candidates for a graded approach to qualification, particularly regarding software QA/V&amp;V (designated SR* in Table 4-1):</b>	
Primary indications of performance for credited manual actions	4.1
Procedures needed for credited manual actions, if not provided in paper form (if these procedures are provided on a nonsafety-related computer-based platform, then backup procedures should be provided as SR* or paper)	4.1
Indications of the status of critical safety functions and fission product barriers, and safety system operation (Reg. Guide 1.97 Types B and C)	4.2
Indications related to safety system operation (Reg. Guide 1.97 Rev. 3 Type D, Category 1)	4.2
Procedures for monitoring safety functions and backing up automated success paths, if not provided in paper form (if these procedures are provided on a nonsafety-related computer-based platform, then backup procedures should be provided as SR* or paper)	4.2
Prompting indications, controls and immediate feedback indications, and performance indications for carrying out preferred manual safety success paths	4.3
Procedures needed for accident mitigation and achieving safe shutdown, if not provided in paper form (if these procedures are provided on a nonsafety-related computer-based platform, then backup procedures should be provided as SR* or paper) – Section 4.3 discusses the minimum set of procedures required	4.3
Other post-accident monitoring indications (Reg. Guide 1.97 Rev. 3 Type E, Cat. 1)	4.5
Procedures for post-accident monitoring, if not provided in paper form (if these procedures are provided on a nonsafety-related computer-based platform, then backup procedures should be provided as SR* or paper) – Section 4.3 discusses the minimum set of procedures required	4.5
<b>Minimum set of HSIs that should be spatially dedicated, continuously visible (SDCV):</b>	
Prompting indications (at least one channel – Reg. Guide 1.97 Type A), prompting alarms, controls and immediate feedback indications, and primary performance indications for credited manual actions	4.1
At least one of the redundant indications of the status of critical safety functions (Reg. Guide 1.97 Type B)	4.2
At least one of the redundant indications of the status of fission product barriers and safety system operation (Reg. Guide 1.97 Rev. 3 Types C and D, Category 1)	4.2
Alarms indicating challenges to critical safety functions	4.2
High-level summary indications and alarms for safety system actuation status	4.2
Controls for manual system-level actuation of safety systems	4.2
Prompting alarms for manual actions credited in the D3 evaluations per BTP 7-19 Points 1-3	4.2
Safety function indications and controls for system-level actuations credited for satisfying Point 4 of BTP 7-19	4.2
Performance alarms for preferred manual safety success paths	4.3

Minimum Inventory HSIs	Guidance Section
Performance alarms for preferred manual non-safety success paths	4.4
Other post-accident monitoring indications and associated alarms (Reg. Guide 1.97 Rev. 3 Type E, Cat. 1)	4.5
System-level indications and alarms on safety system availability	4.6
Alarms on safety parameters and other alarms for prompting pre-emptive safety actions (SPDS)	4.7
<b>Minimum set of HSIs that should be one-step accessible or SDCV:</b>	
Safety parameter indications (SPDS)	4.7

#### 4.1 Perform Manual Credited Actions

These are actions that are specifically credited in the SAR safety analyses for accident mitigation, for which no automatic control is provided. These are typically very limited in number, and some plants may have none. Because of their importance to mitigation of design basis events, the HSIs that support these actions have the most stringent requirements.

The discussion here pertains to manual actions that are time critical. For actions that are longer term (e.g., actions needed to achieve safe shutdown after completing event mitigation actions or a mitigation action required several hours after the initiating event) less stringent HSI design requirements may be appropriate. If required, these actions should fall under one of the other categories of functions and tasks, such as carrying out preferred manual safety or non-safety success paths per the station’s EOPs.

Credited manual actions may be system-level actuations or control of individual components such as pumps or valves. Manual actuation or control of auxiliary equipment (e.g., cooling water, ventilation, lubrication), needed in the short term to support the primary equipment being controlled, also should be included.

##### *Prompting Indications*

Prompting indications are the process parameters that lead the operator to take the credited manual action. As stated in IEEE 603 [6], the indications needed to prompt the action are considered “part of the safety systems” and thus should be on qualified displays. Reg. Guide 1.97 refers to these indications as Type A variables. Revision 3 of the Reg. Guide [14] classifies them as Category 1 in terms of design criteria, which again indicates that they should be qualified as safety-related instrumentation. Revision 4 of the Reg. Guide [15] also specifies criteria for design and qualification of these indications. Since they are safety-related, these indications must be independent of the nonsafety-related HSIs normally used by the operators.

Reg. Guide 1.97 Revision 3 specifies that “continuous real-time display” should be provided for these variables. Revision 4 of the Reg. Guide indicates that at least one redundant display of each Type A variable should have continuous real-time display. These criteria can be interpreted as meaning that the indications (at least one channel for each variable) should be provided on

spatially dedicated, continuously visible (SDCV) displays, which is consistent with their importance to accident mitigation. This requirement can be met by a highly reliable, nonsafety-related SDCV display, in which case the safety-related display could be selectable.

If plant procedures require that parameter trends be used to support taking a credited manual action, then design requirements applicable to trend displays should be determined. If the trend can be deduced directly from the indicator, then a separate trend display would not be required. On the other hand, if the trend cannot be deduced from the indicator and is needed to support the action, then a qualified trend display may be required.

If the trend display is separate from the primary indicator, a graded approach for qualification of the trend display should be considered. As long as it is reasonable to expect that failures of the system providing the trend display would be detected, then additional operator surveillance of the indicators that remain functional could be used to detect the trend and ensure that the proper action is taken.

IEEE Std 497-2002 [5], endorsed by Reg. Guide 1.97 Revision 4, requires that if “direct or immediate trend or rate information is essential for operator action, the trend information shall be continuously available on dedicated trend displays...and selectively available on another redundant trend display.” This again implies SDCV implementation for at least one of a redundant set of such trend displays.

### ***Prompting Alarms***

Traditionally, alarms have been provided using highly reliable, nonsafety related alarm systems. For operating plants there is no specific requirement that alarms be provided on safety-related displays, and operator surveillance and monitoring of key indications can be used to ensure that credited manual actions are taken when required. However, alarms also can play an important role in prompting the required actions. Use of modern HSI technology presents opportunities to provide alarm features as well as display of key indications. Therefore, if a digital solution is used to implement alarms prompting credited actions for an operating plant, placing those alarms on the same safety-related displays that present the prompting indications should be considered as part of the design.

The Staff Requirements Memorandum (SRM) to SECY-93-087 [18] states that the alarm system for Advanced Light Water Reactors (ALWRs) should incorporate redundancy. It goes further to state that alarms for manual actions required for the safety systems to accomplish their safety functions should meet IE requirements. NUREG-0800 (SRP) Section 7.5 (III.1.O) [10] has similar provisions. Therefore, alarms that are needed to prompt credited manual actions in new plant designs should be implemented using safety-related equipment.

Because of their importance and the need for prompt action, SDCV display should be used for these alarms to ensure that they are quickly recognized by the operators in the midst of other alarms that may be occurring.

### ***Controls and Immediate Feedback Indications***

The credited manual control actions are necessary to support the conclusions of the safety analyses contained in the plant's SAR. Therefore, the controls needed to perform the actions must be qualified as safety-related equipment. IEEE 603 [6] discusses the need for these controls, and, although it is not explicitly stated, it can be inferred that the controls should be considered part of the safety systems and thus subject to the same design requirements. Immediate feedback indications (e.g., pump run/stop status indications, valve open/closed indications) should be treated in the same way as the controls themselves, as they are necessary for verifying the required actions have taken place.

Regarding accessibility, implementing the controls and immediate feedback indications in a spatially dedicated, continuously visible (SDCV) form will provide the most rapid access for the operator. It is desirable to automate safety functions to the extent practical to minimize the need for credited manual actions. For a limited number of manual actions, it is then practical to use SDCV conventional devices. However, if there are many controls required to support manual actions, there is precedence for regulatory acceptance of soft controls for credited manual actions for which the operator must perform only one action to access the needed control. This is referred to here as "one-step accessible." This type of design solution has been accepted by the NRC previously as part of the design certification reviews for ALWRs. When supported by appropriate task analysis, and HFE verification and validation, this should be acceptable for modernized control rooms as well as new designs.

Note that because the prompting indications are continuously displayed (SDCV – see discussion above), the operator will be able to recognize quickly the conditions that require the manual action. Most actions do not (and likely should not) require such rapid action that the operator would not then have time to take a single action to access the needed control. If the time frame is so short that this is in question, then automation should be considered for that control action.

### ***Performance Indications***

There are no specific regulatory requirements regarding the design of process performance indications (e.g., flow, level, etc.) and alarms needed for continued monitoring of the equipment or function that is the subject of the manual action, unless these indications are also called out in Reg. Guide 1.97 [14,15] for post-accident monitoring. The design requirements should be based on the importance of these indications to fulfilling the intended functions based on the safety analysis. Primary indications needed to verify that the function has been performed may need to be safety-related; however, a graded approach to qualification should be considered for these. Secondary indications (e.g., performance of sub-systems or components that contribute to the overall function) can be nonsafety-related.

Primary indications should be placed on SDCV displays, so that they are immediately available to the operators. Secondary indications can be on selectable displays.

## *Performance Alarms*

Alarms can be important in alerting operators to problems related to the functions initiated by credited manual actions. There is no requirement that the alarms be implemented using safety-related equipment. However, if computer-based solutions are chosen, presenting these alarms on the same displays used to present the performance indications may be appropriate. These can be selectable.

## *Procedures*

If procedures needed by the operator to perform the credited manual actions are implemented on a nonsafety-related system, then backup procedures will be required. These can be implemented in hardcopy form or on a safety-related computer-based system that is independent of the nonsafety system normally used to present the procedures. EPRI 1015313 [17] provides guidance on implementation of computerized procedures on nonsafety-related platforms, including guidance on quality assurance and other digital system requirements that may apply, the need for backups, and making the transition to backup procedures.

## **4.2 Monitor Safety Functions and Back Up Automatic Success Paths**

There are no specific operator actions credited for automated success paths, because the automatic systems that carry out these success paths take the protective actions to completion and meet all qualification and redundancy requirements. (Manual actions that are credited, for which no automatic control is provided, are addressed in Section 4.1 above.) However, monitoring the performance of the automatic systems and associated safety equipment, and backing them up as necessary, is an important operator task. This includes manual actuation of the safety systems when necessary.

There are a number of regulatory requirements and guidance statements that apply to monitoring critical safety functions and backing up the automatic protection systems:

**IEEE 603 [6] and Reg. Guide 1.62 [13]** contain requirements for manual system-level actuation controls. Here we address the use of these controls to back up the automatic actuations. The controls also can be used to take discretionary, pre-emptive actions before automatic actuation occurs – that use is addressed in Section 4.7.

**Reg. Guide 1.97 [14,15]** gives criteria for instrumentation and displays to monitor critical safety functions (Type B variables), the potential or actual breach of fission product barriers (Type C variables), and the operation of the safety systems and other systems important to safety (Type D variables). It provides design criteria for the instrumentation and associated displays.

**Branch Technical Position BTP 7-19 [10]** calls for a defense-in-depth and diversity (D3) evaluation to identify potential common cause failures of protection systems (RTS and/or ESFAS) that use digital technology, and demonstration of adequate coping capability to deal with such failures. Manual operator actions may be credited as part of

the D3 coping capability. In addition, BTP 7-19 Rev. 5 states in Point 4 that “a set of displays and controls located in the main control room should be provided for manual system-level actuation of critical safety functions and for monitoring of parameters that support safety functions.” These must be independent of the computers used in the automatic actuation systems. See Section 3.1.3 for further discussion.

### ***Indications and Alarms***

There are several types of indications that may be used by the operators to monitor safety functions and back up the automatic safety systems. These indications and associated alarms are discussed below:

#### Status of Critical Safety Functions, Fission Product Barriers, and Operation of Safety Systems (Reg. Guide 1.97)

Reg. Guide 1.97 [14,15] gives requirements on indication of variables indicating whether critical safety functions are being performed properly (denoted as Type B variables). The regulatory guide also has requirements on indications related to the potential or actual breach of fission product barriers (Type C variables) and indications related to the operation of the safety systems (Type D variables). For key variables of these three types, Revision 3 of the regulatory guide imposes its Category 1 design and qualification criteria. Other variables of less importance fall into Category 2, which has more relaxed criteria regarding seismic qualification, redundancy, and standby power sources. Still others are placed in Category 3, which accepts high-quality commercial, non-qualified equipment. Revision 4 of Reg. Guide 1.97 [15], which is based on IEEE Std 497-2002 [5], also addresses Types B, C and D variables and associated design criteria. However, it provides a less prescriptive and more flexible approach for identifying the specific variables of each type. It also provides a somewhat more standardized set of design and qualification criteria based on the variable type. See Section 2.1 and Table 2-1.

As discussed in Section 4.1, indications of Type A variables needed to support credited manual operator actions should be implemented using qualified, safety-related equipment. HSIs for Type B, C and D variables also should be safety-related if Category 1 per Reg. Guide 1.97. If following Rev. 4 of the Reg. Guide, only Types B and C are required to be safety-related. However, note that there is precedence in operating plants and ALWR designs for regulatory acceptance of a graded approach to qualification for Type B, C and D variables.

Reg. Guide 1.97 Revision 3 [14] states that variables falling into Category 1 (which includes selected Type B, C and D variables) need to have “continuous real-time display.” This implies that the indications for these variables should be spatially dedicated and continuously visible (SDCV). Revision 4 of Reg. Guide 1.97 [15] states that at least one redundant indication for each Type B variable must have continuous real-time display, again implying that those indications should be SDCV. This requirement can be met by a highly reliable, nonsafety-related SDCV display, in which case the safety-related display could be selectable.

Reg. Guide 1.97 requirements regarding other variables needed for post-accident monitoring, classified as Type E variables, are addressed in Section 4.5.

#### Alarms on Challenges to Critical Safety Functions

Alarms on critical safety functions are important in alerting operators to plant safety challenges. There is no requirement that these alarms be presented on safety-related HSIs. However, if the Reg. Guide 1.97 indications discussed above are presented on safety-related HSIs, then providing alarm functionality for these indications would ensure that the alarms are available to assist the operators in detecting problems and backing up the automatic systems when needed. Also, NUREG 0700 (paragraph 4.1.2-1) [7] states that “The alarm processing system should ensure that alarms that...indicate a threat to plant critical safety functions are presented in a manner that supports rapid detection and understanding under all alarm loading conditions.” This implies that these alarms should be spatially dedicated and continuously visible (SDCV).

#### Alarms on Fission Product Barriers and Safety System Operation

There is no requirement that these alarms be presented on safety-related HSIs, and no requirements for accessibility. These alarms can be on nonsafety-related, selectable displays.

#### Actuation Status Indications

In order to back up the automatic actuation systems, the operators must be able to determine the status of the actuations. IEEE 603 [6] requires that the operators be provided with “accurate, complete, and timely information pertinent to safety system status.” It states that safety system status indications need not be considered part of the safety systems, implying that there is no requirement for these indications to use qualified equipment.

No specific requirements regarding accessibility of these indications are stated. However, because of their importance to the plant’s emergency operating procedures and the operator’s ability to back up the automatic systems, high-level summary indications of status (e.g., at the division level for each major system or function) should be provided on SDCV displays to ensure rapid access to these key indications. Detailed or component-level actuation status indications can be made available on selectable displays.

#### Alarms on Safety System Actuation Failures

There is no requirement that these alarms be presented on safety-related HSIs, and no specific regulatory requirement regarding their accessibility. However, consistent with the actuation status indications discussed above, high-level alarms on actuation failures (e.g., at the division level for each major system or function) should be provided on SDCV displays to ensure rapid assimilation of these alarms. Detailed or component-level alarms can be provided on selectable displays.

### ***Manual System-Level Actuation Controls***

IEEE 603 [6] and Reg. Guide 1.62 [13] require manual, system-level actuation controls in the main control room. IEEE 603 states that these manual actuations “shall depend on the operation of a minimum of equipment” consistent with requirements for redundancy. Reg. Guide 1.62 has a similar provision. Although there are no explicit requirements stated regarding the need for these controls to be safety-related, there is considerable industry precedence for this in both operating plants and ALWR designs. Given the need for simplicity (reliance on a minimum of equipment, which becomes difficult if one attempts to implement these in non-qualified equipment and then interface it to the safety systems) and the precedence of existing designs, it should be expected that these controls will need to be safety-related.

Reg. Guide 1.62 states that the “switches for manual initiation of protective actions at the system level should be located in the control room and be easily accessible to the operator so that action can be taken in an expeditious manner.” This implies that the controls should be spatially dedicated and continuously visible (i.e., implemented as hard switches or SDCV soft controls).

### ***Manual Component-Level Controls***

There is no specific regulatory requirement regarding design or qualification criteria for manual component-level controls, other than those used for credited manual actions (see Section 4.1). Requirements for controls that support preferred manual safety and non-safety success paths in the EOPs are addressed in Sections 4.3 and 4.4. Other component-level controls can be implemented using non-safety HSIs.

### ***Procedures***

If procedures needed to support monitoring and backing up the automated safety success paths (typically part of the plant’s emergency procedures) are implemented on a nonsafety-related system, then a minimum set of backup procedures may be needed. These may be in hardcopy form or implemented on a safety-related computer-based system. See Section 4.3 for further discussion of the minimum set of backup procedures needed. EPRI 1015313 [17] provides guidance on implementation of computerized procedures on nonsafety-related platforms, including guidance on quality assurance and other digital system requirements that may apply, the need for backups, and making the transition to backup procedures.

### ***Manual Controls, Indications and Procedures Used for D3 Coping Capability***

As discussed above, the D3 evaluation called for by Points 1-3 of BTP 7-19 [10] may result in crediting specific manual actions for coping with common cause failures (CCFs) of the RTS and/or ESFAS. This will require that prompting indications (displays and/or alarms) and controls (at the system or component level) be provided to accomplish these actions, and that these be implemented such that they are not subject to the same CCF that they are intended to address. They can be implemented using nonsafety-related equipment as long as adequate reliability and availability can be demonstrated. Use of the nonsafety control and information system to provide these capabilities may provide the best solution, because (1) it should have the needed reliability,

and (2) it ensures that the HSIs used for D3 are the same as those normally used by the operators, avoiding issues of unfamiliarity and the need to train on seldom-used backups. However, it will be necessary to ensure that the signals used for this purpose are not affected by the postulated CCF. Signals that are generated within the protection equipment and then passed to the control and information system may not be acceptable.

As discussed in BTP 7-19, HFE principles and criteria should be applied in the design of the displays and controls. Due to the importance of alerting operators to safety system failures that require backup manual actions, alarms prompting those actions should be spatially dedicated and continuously visible (SDCV). Requirements for the indications and controls needed for D3 coping actions should be determined based on appropriate HFE analyses. If such actions are driven by procedures (with procedure entry prompted by SDCV alarms), there may be no need for the indications or controls to be SDCV.

*[This needs to be coordinated with the resolution of credited operator action times being investigated separately.]*

As noted earlier, Point 4 of BTP 7-19 calls for indications and controls to accomplish manual system-level actuation of critical safety functions and monitoring of parameters that support the safety functions. This position originally was applied to advanced plants with digital protection and control systems. However, Rev. 5 of BTP 7-19 now makes Point 4 applicable to both new plants and operating plants that undergo modernization of the control and protection systems. Because Point 4 addresses all critical safety functions, compliance with this requirement would likely lead to the need for additional HSIs beyond those required for the specific manual actions credited in the D3 evaluation. The indications and controls provided for Point 4 need to be independent of potential common cause failures in the computer-based safety systems.

Point 4 HSIs also need to be implemented by connecting them to discrete hardwired devices or simple, dedicated, diverse digital devices per BTP 7-19 (see discussion in Section 3.1.3). This implies an expectation that the indications and controls will be spatially dedicated and continuously visible. BTP 7-19 is silent on alarms. Requirements for alarms on safety functions to meet Point 4, and their accessibility, should be determined by appropriate HFE analyses.

Procedures that are needed for the operators to be able to carry out prescribed actions for coping with common cause failures must be available when they are needed. If manual actions are credited for coping with a CCF, and that same CCF can cause failure of the system that implements computer-based procedures normally used by the operators, then separate backup procedures will be needed sufficient for coping with the identified CCF. These may be implemented in hardcopy form or on a computer-based system that is not affected by the postulated CCF (the computer-based system can be nonsafety-related). Note that if the procedures are implemented on a system that can be shown to be unaffected by the postulated CCF, then the procedures should be available and no backup procedure is required.

### 4.3 Carry Out Preferred Manual Safety Success Paths

The emergency procedure guidelines (EPGs) or plant-specific emergency operating procedures (EOPs) provide multiple ways for the operators to deal with plant emergencies and accident scenarios; these are referred to as success paths. Automated success paths are addressed in Section 4.2. Here we begin to address manual success paths, where there is no automated success path. These may include actions that support the automatic protection systems in mitigating accident conditions, or they may address longer-term actions needed to achieve safe shutdown of the plant.

Some manual success paths may call for performing actions that, although necessary if other means are not available, would be undesirable due to the need for extensive clean-up operations later, or other economic or environmental consequences. Examples are actions that cause atmospheric release, containment flooding or contamination, or safety injection actuation. Typically the operators would first try to use other means that do not have such undesirable consequences. These are referred to as *preferred* success paths.

Some preferred success paths make use of safety systems or equipment, while others use non-safety equipment. This section discusses preferred manual *safety* success paths (those making use of safety equipment to accomplish the needed functions). Preferred manual *non-safety* success paths are addressed in Section 4.4.

There are no explicit regulatory requirements for qualification of HSIs that support preferred manual success paths. IEEE 603 [6] states that “Means shall be provided to implement the manual actions necessary to maintain safe conditions after the protective actions are completed... Such displays and controls shall be located in areas that are accessible, located in an environment suitable for the operator, and suitably arranged for operator surveillance and action.” However, it does not specifically address qualification or independence requirements. Reg. Guide 1.97 Revision 4 [15], which endorses IEEE Std 497-2002 [5], specifies design and qualification requirements for Type D variables, which include variables indicating performance of systems needed for accident mitigation and to achieve and maintain safe shutdown. It specifies that instrument channels monitoring systems that are expected to be operable following a seismic event shall be seismically qualified, but does not specify any independence requirements for these variables.

In operating plants, many of the controls and indications for safety equipment are qualified, but this was not due to a specific regulatory requirement. Therefore, for new plant designs and for modernization of operating plants, decisions must be made regarding what level of qualification should be used for these HSIs.

For preferred manual safety success paths required to achieve and maintain safe shutdown conditions, although the regulatory requirements are not explicit, it can be inferred that the indications and controls needed to accomplish these actions should be qualified. This is addressed in the discussion below.

EPGs/EOPs typically specify alternate safety or non-safety success paths in addition to the preferred success paths. These may be needed when the preferred success path is not available or does not achieve the desired results. Because there are no specific qualification, independence or accessibility requirements for the HSIs to perform these alternate or contingency success paths, they are not addressed further here.

### ***Prompting Indications***

As discussed above, although the regulations do not explicitly state the requirement, it can be inferred that the key indications needed to prompt actions required for carrying out the preferred manual safety success paths should be provided on safety-related HSIs. Actions that are credited in the safety analysis were addressed in Section 4.1 above. Here we are addressing longer-term actions not specifically credited in the safety analysis. Therefore, a graded approach to qualification should be considered for these indications. There is precedence for this in the ALWR designs.

Because the actions are prompted by EOP execution, these indications can be selectable.

### ***Prompting Alarms***

Actions needed to carry out the preferred manual safety success paths typically are prompted by the emergency operating procedures, which are entered due to prompting indications or alarms. Therefore, prompting alarms for individual actions are not required. However, if HFE analyses indicate benefits of providing such alarms within the design, consider providing them on the same safety-related displays used to present the associated indications.

### ***Controls and Immediate Feedback Indications***

Consistent with the discussion above under *Prompting Indications* these should be safety-related, and a graded approach to qualification is suggested. The control actions are prompted by procedure and typically are not time-critical, so making them selectable should be adequate unless a specific control requires time-critical action or frequent adjustment such that one-step access or SDCV implementation is needed.

### ***Performance Indications***

Similar to the prompting indications discussed above, indications on performance of the preferred manual safety success paths should be safety-related but considered for qualification with a graded approach. Because actions are guided by the EOPs, SDCV display is not required.

### ***Performance Alarms***

There is no requirement that these alarms be safety-related. However, consistent with other safety significant alarms, these alarms should be considered for inclusion on the same safety-related display used for the associated indications. Because it is important for an operator to give

prompt attention to problems in preferred success paths that have been deployed, these alarms should be SDCV.

### **Procedures**

Procedures that are necessary for the operators to mitigate accidents and achieve safe shutdown must be available under accident conditions in which they are needed. If the plant's emergency procedures are implemented on a nonsafety-related system, then a minimum set of backup procedures will be needed. These may be in hardcopy form or implemented on a safety-related computer-based system. The minimum set of procedures that must be available in backup form are the function-based (symptom-oriented) or functional recovery procedures needed for the operators to mitigate accident conditions regardless of the specific cause or event. Event-specific or optimal recovery procedures may not be needed as long as the function-based procedures are adequate for accident mitigation and achieving safe shutdown. The minimum set of required backup procedures should be defined and justified.

EPRI 1015313 [17] provides guidance on implementation of computerized procedures on nonsafety-related platforms, including guidance on quality assurance and other digital system requirements that may apply, the need for backups, and making the transition to backup procedures.

## **4.4 Carry Out Preferred Manual Non-Safety Success Paths**

This section addresses success paths called out in the EPGs or plant-specific EOPs that require manual action, make use of non-safety equipment, and are *preferred* in that they would be the first choice for achieving safe shutdown over other alternative paths that may result in undesirable consequences such as containment flooding (see discussion in Section 4.3 regarding different types and consequences of success paths).

The manual actions credited in the safety analysis (Section 4.1), automated success paths (Section 4.2), and preferred manual safety success paths (Section 4.3) provide adequate means for accident mitigation and achieving safe shutdown. Those paths use safety systems and equipment that meet the single-failure criterion and other qualification requirements. Preferred manual non-safety success paths, on the other hand, are not credited for accident mitigation and do not have any specific regulatory requirements governing their design or qualification. Therefore, this category is purely discretionary. However, note that these success paths may receive significant credit in the PRA for mitigation of accident sequences and thus may be risk significant.

None of the HSIs for these paths are required to be safety-related<sup>7</sup>. However, depending on the plant's concept of operations for conditions in which the normally-used HSIs have been lost or

---

<sup>7</sup> In those operating plants that were subject to Unresolved Safety Issue (USI) A-46, certain equipment had been designated for use in reaching safe shutdown following a seismic event. This equipment, which was identified on a safe shutdown equipment list (SSEL), was evaluated for seismic ruggedness. Although in most plants this equipment was safety-related, in some plants some of this equipment may be nonsafety. When modernizing the instrumentation and controls for this equipment, the need to maintain seismic safe shutdown capability should be considered. For

degraded (see Section 3.1.4), there may be a desire to provide capability to achieve safe shutdown using preferred manual non-safety success paths independent of the normally-used HSIs. This is discussed in Section 4.8 below.

### ***Prompting Indications and Alarms***

The prompting indications for deployment of safety or non-safety success paths are typically the same. So for most situations these are already covered above. However, for some events there may be some unique prompting indications for non-safety success paths. There is no requirement that these be safety-related. Because actions associated with the success paths are guided by EOP execution, selectable implementation should be adequate for these.

### ***Controls and Immediate Feedback Indications***

There is no requirement these be safety-related. It is acceptable for these controls and indications to be selectable since they are discretionary, and because again their use is guided by execution of the EOPs.

### ***Performance Indications and Alarms***

There is no requirement that these be safety-related. The indications can be selectable. However, because it is important for an operator to give prompt attention to problems in preferred success paths that have been deployed, the alarms should be SDCV.

### ***Procedures***

Because preferred manual non-safety success paths are not credited for accident mitigation or achieving safe shutdown, there are no specific requirements regarding implementation of the associated procedures – they may be implemented on a nonsafety-related system or in paper form. However, if the plant's concept of operations for failure or degradation of the normally-used HSIs calls for the ability to achieve safe shutdown using preferred non-safety success paths, and the procedures are computerized and impacted by the same failure or degradation, then backup procedures would be required. This is discussed in Section 4.8

## **4.5 Perform Additional Post-Accident Monitoring for Radioactivity Releases**

Reg. Guide 1.97 [14,15] addresses post-accident monitoring instrumentation and associated displays. Type A variables specified in the regulatory guide, which are needed to support manual operator actions credited in the safety analysis, are addressed in Section 4.1. Type B, C and D variables, which are used for monitoring critical safety functions, potential or actual breach of

---

example, if the controls and indications for most nonsafety-related equipment are being migrated to a new digital control system that is not seismically rugged, then special consideration may be needed for those HSIs required to operate equipment that had been identified on the USI A-46 safe shutdown equipment list (e.g., these might be moved to a safety-related platform that is seismically qualified so they can still be relied upon for seismic safe shutdown).

fission product barriers, and operation of the systems needed to mitigate accidents and achieve and maintain safe shutdown (respectively), are addressed in Section 4.2 on monitoring and backing up automated success paths and Section 4.3 on preferred manual safety success paths. Reg. Guide 1.97 also contains requirements for Type E variables, which are used for monitoring and assessing the release of radioactive materials.

Revision 3 of the regulatory guide specifies that indication of containment area radiation should meet Category 1 design and qualification requirements. This means it must be safety-related and spatially dedicated, continuously visible (SDCV). Other Type E variables fall into Category 2 or 3; these can be on nonsafety-related selectable displays. Revision 4 of the regulatory guide indicates that qualification is not required for Type E variables.

There are no specific requirements for alarms on Reg. Guide 1.97 parameters. However, alarms on key variables can be important in alerting the operators to conditions requiring their attention. Implementing these on the same qualified HSIs that are used for the qualified indications should be considered. Also, SDCV display should be provided for these alarms.

Procedures that are necessary for the operators to mitigate accidents, achieve safe shutdown and perform post-accident monitoring must be available under the accident conditions in which they are needed. If the plant's emergency procedures are implemented on a nonsafety-related system, then a minimum set of backup procedures will be needed. These may be in hardcopy form or implemented on a safety-related computer-based system. Section 4.3 discusses the minimum set of backup procedures that are needed. EPRI 1015313 [17] provides guidance on implementation of computerized procedures on nonsafety-related platforms, including guidance on quality assurance and other digital system requirements that may apply, the need for backups, and making the transition to backup procedures.

## **4.6 Monitor Safety System Availability**

Sections 4.1 through 4.5 above dealt with emergency operations. The remaining sections deal with functions and tasks performed during normal or non-emergency operations (though they may be performed under emergency conditions as well). The first of these is monitoring safety system availability.

Reg. Guide 1.47 [12] requires that bypassed and inoperable status indication be provided for the safety systems at the system level. It does not require that these indications be safety-related. IEEE 603 [6] states that "If the protective actions of some part of a safety system have been bypassed or deliberately rendered inoperative for any purpose other than an operating bypass, continued indication of this fact for each affected safety group shall be provided in the control room... This display instrumentation need not be part of the safety systems."

The text of the regulatory guide implies that the bypassed and inoperable status indications should be continuously displayed. Because of the importance of the operators being able to easily determine safety system status, SDCV display should be considered for system-level or division-level indications. This may be accomplished through use of indicators, alarms, or a combination of the two.

## 4.7 Monitor Plant Safety Parameters

Indications of the status of the plant's critical safety functions, which are Type B variables identified in Reg. Guide 1.97 [14,15], are discussed in Section 4.2 in the context of emergency operations. This section discusses additional requirements for monitoring safety parameters during normal operation, and for taking discretionary, pre-emptive actions when needed to address safety challenges.

### *Safety Parameter Indications*

After the Three Mile Island accident, requirements were established for Safety Parameter Display Systems (SPDS) to improve the ability of plant personnel to monitor critical safety functions and rapidly determine when safety challenges arise. The regulatory requirement for SPDS is contained in 10 CFR 50(f)(2)(iv). Initial guidelines for implementing SPDS were published in NUREG 0800 [10]. Additional guidance was provided in NUREG 0737 [9] and NUREG 1342 [11]. The NRC review criteria for the HFE aspects of SPDS were subsequently moved to NUREG 0700 (Section 5) [7].

Key indications of critical safety function status, provided by Reg. Guide 1.97 [14,15] Type B variables, are displayed on safety-related HSIs (see Section 4.2). There is no requirement that additional indications provided by SPDS be safety-related.

NUREG-1342 [11] notes that SPDS parameters should be continuously displayed. However, the NRC has accepted SPDS systems that provide either a dedicated, single display of plant variables or a hierarchy of display pages on a single display device, with SDCV perceptual cues (e.g., icons that flash) to alert the user to changes in the safety status of the plant (such as when safety functions are challenged). The display showing specific challenged SPDS parameters should be one-step accessible. Some early advanced plant designs have used critical safety function indications on large overview displays to satisfy SPDS requirements.

### *Safety Parameter Alarms*

Alarms on plant critical functions and safety parameters are important in alerting operators to plant safety challenges. NUREG 0700 (paragraph 4.1.2-1) [7] states that "The alarm processing system should ensure that alarms that...indicate a threat to plant critical safety functions are presented in a manner that supports rapid detection and understanding under all alarm loading conditions." This implies that these alarms should be spatially dedicated and continuously visible (SDCV).

### *Other Prompting Indications and Alarms for Pre-Emptive Actions*

Section 4.2 discusses safety-related indications that would indicate the need for RTS or ESFAS actuation. However, there may be other indications that are preferred for indicating the need for pre-emptive action. For example, the safety-related indications may have wide ranges to cover accident conditions, while narrow-range indications may be preferred for detecting imminent challenges to safety functions during normal operation. These indications can be on selectable

displays. However, SDCV display should be used for the alarms to ensure that the operators receive timely prompts for pre-emptive safety actions when needed.

### ***Controls for Pre-Emptive Actions***

Section 4.2 addressed controls for manual system-level actuation of the plant safety systems, focusing on their use to back up the automatic actuations. These controls also may be used to take pre-emptive action when it is deemed necessary by the operators. Such actions are discretionary, and are not credited in the safety analysis for accident mitigation.

## **4.8 Continue Operation Under Conditions of Failed/Degraded HSIs**

As a minimum, plants must provide the capability to manage accidents and achieve safe shutdown using only safety-related control equipment and HSIs. This equipment must be independent of the nonsafety-related HSIs normally used to monitor and control the plant. Other requirements imposed on control equipment and HSIs that are independent of the normally-used HSIs are discretionary. As discussed in Section 3.1.4, the HSI capabilities that will be needed to handle situations in which the normal HSIs have failed depends largely on what failures are postulated, the expected duration of these degraded HSI situations, and how the plant wants to respond to these failure modes. Guidance is provided in Section 3.1.4 on determining a “concept of operations” for these situations, which can range from immediately tripping the plant and making use primarily of the safety-related HSIs available in the control room to reach a safe shutdown condition, to continuing operation indefinitely and providing additional HSIs to allow for selected plant operations and contingencies.

Sections 4.1-4.3 and 4.5 identified a number of HSIs that are required by regulation or are otherwise important to plant safety, and which need to be implemented using safety-related equipment that is independent of the normal HSIs. These include:

- HSIs needed to support manual operator actions credited in the SAR safety analysis
- Manual system-level actuation controls and the indications and alarms that support their use
- HSIs needed to support carrying out preferred manual safety success paths called out in the EPGs or plant-specific EOPs
- Displays of key variables for post-accident monitoring

The chosen concept of operations will dictate whether the following additional capabilities will also need to be supported:

### Use preferred manual non-safety success paths to safely shut down the plant

If a plant shutdown is required or the concept of operations calls for shutting down, the plant may wish to avoid the undesirable consequences of using the non-preferred EOP success paths (e.g., consequences such as atmospheric release or containment flooding). Use of the preferred manual non-safety success paths will require additional HSIs that are independent of the failure or degradation of the normally-used HSIs. These HSIs are not

required to be safety-related; however, they could be implemented on the same platform as the safety-related HSIs. Procedures governing their use can be nonsafety-related, as long as they are independent of the normal HSI failure, or they can be implemented in paper form. Accessibility requirements can be determined based on appropriate HFE analyses – there are no specific requirements on accessibility as these HSIs are discretionary.

Maintain stable plant operation for a pre-determined time

The functions and tasks needed to monitor the status of critical safety functions and to maintain plant safety under normal and accident conditions were addressed in the previous sections. However, functions and tasks needed to maintain power production and ensure investment protection have not been addressed and need to be considered here. This may include indications needed to monitor the status of power production and operating conditions for major plant equipment. It may also include indications and alarms needed to prompt the operator to shut down critical plant equipment when required, as well as the manual controls and feedback indications necessary to carry out these actions. Ability to reduce power may be desired in order to support load reductions, or to respond to equipment failures or plant safety conditions that force a power reduction.

Maintain operation for a finite but not pre-determined time

Maintaining steady-state plant conditions for relatively long periods of time may require enhanced monitoring or alarm capability for plant safety parameters and pre-trip conditions or other conditions indicating the need for pre-emptive action to maintain safety.

Continuing operation for a relatively long period of time also requires consideration of Technical Specification surveillances. Surveillances that are done infrequently (e.g., quarterly) are likely not to be an issue as it could be shown that the normal HSIs could be returned to operability in sufficient time to accomplish these. However, shorter-term surveillances such as 12-hour surveillance tests may need to be supported, depending again on the duration of expected failures and the chosen concept of operations. If so, the HSIs needed to support these surveillances will have to be provided independent of the HSIs that have failed. Note that some of these may already have been identified as being necessary to support other functions and tasks. Also, it should be noted that new plant designs or modernization of operating plants may provide the opportunity to reduce the number of surveillances as compared to current designs, which could in turn reduce the number of HSIs needed to support them.

It should be noted that maintaining stable operation with reduced HSI capability in the control room implies that every effort needs to be made to avoid imposing any transient on the plant (other than a plant shutdown when needed). Associated restrictions on plant operations may need to be specified in suitable administrative operating limits or Limiting Conditions of Operation (LCOs).

The decision to support continued plant operation during HSI failure is a discretionary one, so no specific regulatory requirements apply to the design of these HSIs other than those already discussed. There are no qualification requirements for the minimum inventory HSIs. However, decisions should be made regarding requirements for accessibility of these HSIs, based on the demands of the tasks being performed. Appropriate HFE analyses should be performed to determine these requirements.

Similarly, there are no requirements regarding the form in which procedures should be implemented to support the discretionary capabilities chosen for HSI failure conditions. (Procedures required for accident mitigation and to achieve safe shutdown were addressed earlier in Sections 4.1-4.3.) However, it is recommended that procedures needed by the operators to deal appropriately with HSI failures or degraded conditions be provided in hardcopy form, on qualified HSIs, or on another computer-based system independent of the normally-used HSIs.

#### **4.9 Perform Other Important Tasks During Normal Operation With All HSIs Available**

It is expected that in a modern control room the operators will primarily use the nonsafety-related HSIs, with selectable displays and soft controls, to perform control and monitoring tasks needed during normal operation and to handle anticipated plant transients and upsets. However, some tasks impose requirements on the HSIs that go beyond the capability of a typical operator workstation, particularly in terms of accessibility. A number of tasks have already been identified in Sections 4.1-4.7 – for example, monitoring plant safety parameters and determining when pre-emptive safety actions may be required. Also discussed were requirements for accessibility of displays indicating safety function challenges, top-level SPDS indications and alarms, and narrow-range, non-qualified indications that are determined to be the preferred means of monitoring and detecting the need for pre-emptive safety actions.

There may be additional functions and supporting HSIs that require greater accessibility than would be provided through selectable displays on operator workstations. Examples include:

- Indications, alarms and/or controls that are important in supporting critical functions and tasks related to power production or investment protection, not already addressed in the categories above
- Alarms requiring prompt operator action that have not already been identified in one of the other categories addressed above. SDCV displays should be considered for alarms that require prompt action or that need to be continuously visible to the entire crew (e.g., on a group-view display). See Section 4.4 of EPRI 1010042 [2] and Section 4.2 of NUREG 0700 [7] for guidance on alarm information display.
- Indications important to maintaining situation awareness of the operating crew (e.g., key indications provided on an overview or group-view display visible to the entire crew)

# 5

## IMPLEMENTATION OPTIONS AND SELECTING A DESIGN CONCEPT

---

There is a wide range of options available for implementing the minimum inventory HSIs, ranging from solutions using mostly conventional HSI technology to those employing primarily computer-based solutions using video display units (VDUs) for display and control.

Modern HSI technology provides opportunities to design more effective design solutions for safety monitoring and control than were possible with older analog technologies. This should be considered when selecting a design concept. Additional important considerations in selecting a design concept include:

- Decisions on increasing automation to reduce manual control requirements
- Capabilities and trade-offs of conventional versus computer-based HSI technologies
- The need to minimize the number of different types of HSIs the operators must use

These are addressed in Sections 5.1, 5.2 and 5.3 below.

Additional items that should be considered with respect to implementing the chosen design concept include:

- Impact on Technical Specifications and the site Emergency Plan
- Impact on procedures and training (e.g., impact of multiple diverse HSIs)

These impacts are addressed in Sections 5.4 and 5.5 below.

### 5.1 Automation to Reduce Manual Actions

New plant designs may include automation that reduces the need for manual controls as part of the minimum inventory. Modernization of existing control systems provides an opportunity to increase the level of automation in operating plants as well, including the possibility of automating certain tasks that are now done manually. Automation of some of the manual actions discussed in Section 4 may reduce the number of controls that are needed as part of the minimum inventory. However, note that automating a task does not eliminate the need for operators to monitor and back up the automation.

## 5.2 Capabilities and Trade-Offs of Available HSI Technologies

In choosing among the available design options, it is important to understand the relative advantages and disadvantages of the technologies available.

Table 5-1 compares conventional and modern computer-based HSI technologies and illustrates some of the important tradeoffs involved in selecting the most appropriate technology.

**Table 5-1  
Comparison of Conventional and Newer Computer-Based HSI Technologies**

Characteristic	Advantages and Disadvantages of Each HSI Technology	
	Conventional	Computer-Based
Familiarity (users)	Operators presently have more familiarity with existing, conventional HSIs; however, this is changing as computers become more commonplace in everyday life	Newer operators are more comfortable with computer-based interfaces
Familiarity (maintainers)	Existing maintenance staff are more familiar with conventional technologies, but this also is changing	Newer staff are not as familiar with analog electronic technology as they are with modern computer-based equipment
Familiarity (regulators)	Regulators are most familiar with conventional technologies, although this also is changing	
Maintenance burden		VDUs require no periodic maintenance or calibration, whereas conventional analog electronic devices are subject to drift and require periodic maintenance (e.g., meter calibration, which is in addition to calibration of the instruments).
Flexibility for phased modernization		Once installed, computer-based systems accommodate new HSI functionality more easily than conventional HSIs; migration of the control room HSIs to a modern implementation is easier than relocating conventional meters and switches
Flexibility for future modification		Computer-based HSIs accommodate future changes more easily than do conventional panels
Ease of qualification	Conventional equipment is more easily qualified than is a computer-based system	Use of intermediate qualification levels (particularly with relaxed requirements for software qualification) can help ease this burden
Equipment simplicity	Conventional equipment is less complex; however, interfacing conventional devices as backups to interrupt or override signals from the normal HSIs can be difficult and complex	

Characteristic	Advantages and Disadvantages of Each HSI Technology	
	Conventional	Computer-Based
HSI consistency		Using computer-based technology for supplemental HSIs allows for more consistency between the normal (if computer-based) and backup HSIs, compared to using conventional technology for the backups
Task support		VDUs can provide much better support for operator tasks by bringing together the information specifically needed to support the task, providing higher-level information than is practical with conventional indicators, and providing other operator aids specific to the task
Data accuracy		Digital devices exhibit greater accuracy than analog electronic devices, eliminating their contribution to inaccuracies in displayed data
Data reduction	Analog devices typically can display only a single measurement in a single range, putting the burden on the operators to combine these to determine the actual value.	Computer-based HSIs can monitor multiple redundant signal channels and all ranges, and display the most accurate and validated result for a given variable. Validated results can exclude deviating sensors and automatically switch between narrow and wide range channels. Sensor deviations can be alarmed to prompt required maintenance.
Data consistency		With computer-based implementations, all data (validated results) can be displayed on all HSIs with 100% consistency.
Group-view display capability		VDUs can be used to produce more effective group-view displays more easily than using conventional devices. These can be selectable or SDCV and can provide more effective information presentation with fewer constraints.
Alarm effectiveness		Presentation of alarms on VDUs provides a number of advantages, including the ability to display alarms in fixed positions (similar to conventional tiles) but with greater functionality such as flexible message content, greater ability to apply coding for priority or other purposes, and easier access to supporting details.
Control action support		Soft controls offer a number of advantages over conventional, hard controls.

### **5.3 Minimizing the Number of Different Types of HSIs**

The need for some HSIs to be implemented using qualified equipment, and the need for some HSIs to be independent or diverse from others in order to cope with potential HSI failure modes, can result in the operator having to use a number of different types of HSIs under different circumstances. In order to achieve the highest level of integration and consistency practical, it is important to try to consolidate as much as possible and minimize differences in the functional characteristics of the various HSI resources provided to the operators. Designers should take advantage of opportunities to consolidate HSIs to meet multiple requirements. Examples include:

- If one or more overview displays are to be incorporated into the design to provide high-level information to the entire crew (e.g., via relatively large continuous displays mounted on a wall or vertical panel), it may be possible to take advantage of this feature to meet other requirements as well. For example, using qualified flat panel displays for the overview may allow requirements for Reg. Guide 1.97 [14,15] displays to be met, and also support other safety monitoring requirements that require spatially dedicated and/or qualified displays.
- If the design incorporates the capability to monitor and control safety as well as nonsafety equipment through nonsafety workstations (e.g., some designs are able to accomplish this using a nonsafety control and monitoring system with features that effectively prevent system failures from compromising the safety systems), then these workstations might be used to accomplish other functions. For example, indications and controls needed to support manual actions credited in the D3 evaluation might be accomplished using the nonsafety workstations as opposed to providing separate controls and indicators for D3, as long as the postulated safety system failures they are intended to cope with do not also affect the data sources, control outputs or the workstations themselves.
- If the design incorporates the capability to monitor and control nonsafety-related equipment as well as safety equipment through safety-related (qualified) HSIs, then these qualified HSIs might be used to allow limited continued operation during normal HSI failure conditions (e.g., failure of nonsafety operator workstations).

### **5.4 Impact on Tech Specs and Emergency Plan**

The design solution that is chosen may impact the plant's Technical Specifications. For example, identified HSI failure modes and the concept of operations chosen to deal with them may require modification to the Tech Specs for operating plants – see the discussion in Section 3.1.4. Large-scale failures of control room HSIs also may impact the site Emergency Plan. The need for changes should be considered when developing the design concepts and planning the modernization of an existing control room.

### **5.5 Impact on Procedures and Training**

Procedures should be developed or revised as necessary to reflect use of the minimum inventory or backup HSIs when required. Also, if computer-based procedures are provided for normal use, backup procedures likely will be required for use under conditions in which the computer-based

system (e.g., the operator workstations if they host the procedures) has failed or is degraded. Section 4 identifies the minimum inventory of procedures required for the different categories of functions and tasks. EPRI 1015313 [17] provides additional guidance on computerized procedures, including guidance on making the transition to backup procedures when required.

Differences in the HSIs used by the operators during normal and emergency operations, or in situations when backup HSIs must be used, can lead to errors if these differences are not properly reflected in operator training. These should be addressed specifically in training. Section 6.3 of EPRI 1010042 [2] discusses training issues associated with modernization of operating plants and provides guidance on use of various simulation methods and tools to help familiarize operators with the new HSIs and to conduct training. Procedures also must be addressed along with training to ensure satisfactory operator performance in the modernized control room.

DRAFT



# 6

## REFERENCES

---

*[Note: Full citations will be provided later.]*

1. EPRI 1002835
2. EPRI 1010042
3. EPRI TR-106439
4. IEEE 279
5. IEEE 497-2002
6. IEEE 603
7. NUREG 0700 Rev. 2
8. NUREG 0711 Rev. 2
9. NUREG 0737
10. NUREG 0800
11. NUREG 1342
12. Regulatory Guide 1.47
13. Regulatory Guide 1.62
14. Regulatory Guide 1.97 Revision 3
15. Regulatory Guide 1.97 Revision 4
16. Regulatory Guide 1.153 Revision 1
17. EPRI 1015313
18. SRM to SECY 93-087



# A

## COMPARISON TO REG. GUIDE 1.97 REV. 4

---

The recent revision of Regulatory Guide 1.97 (Rev. 4) [15] provides updated guidance on post-accident monitoring instrumentation that is based primarily on IEEE Std 497-2002 [5]. Because the minimum inventory HSIs identified according to the approach provided in this report include displays of accident monitoring instrumentation covered by Reg. Guide 1.97, during development of this report it was considered important to be consistent with the Reg. Guide, including the previous version (Rev. 3) [14], which many operating plants are still committed to, and the recently updated version (Rev. 4), which may be used to support new plant design or plant modernization.

To support this, a comparison has been made between this industry guidance report and Reg. Guide 1.97, Rev. 4. Detailed results of the comparison are given in the table below. In summary, the comparison shows that:

1. The approaches taken in the two documents are similar, in that they are process-oriented rather than prescriptive, and they rely heavily on the plant emergency operating procedures (EOPs) or emergency procedure guidelines (EPGs) to identify the pertinent HSIs.
2. Although there is overlap, the two documents differ in scope and coverage. In particular:
  - a. The scope of the Reg. Guide is limited to accident monitoring instrumentation for use following a postulated accident
  - b. The industry guidance report addresses HSIs that are needed in addition to the normally-used workstations with selectable displays and controls – as a result:
    - It covers functions and tasks that go beyond just post-accident monitoring – for example, it addresses system-level actuation of safety systems and use of minimum inventory HSIs to maintain power operation under conditions in which the normally-used HSIs are lost or degraded
    - It covers the full range of HSIs needed to support the identified functions and tasks – for example, in addition to displays, it addresses alarms and controls
3. Where the two documents have overlapping coverage, they are consistent in their treatment of the corresponding HSIs.

The conclusion is that the approach provided in this report can be applied in a manner that is consistent with either Rev. 3 or Rev. 4 of Reg. Guide 1.97.

**Table A-1  
Comparison of Industry Guidance Report to Reg. Guide 1.97 Rev. 4 and IEEE Std 497-2002**

HSIs	Industry Guidance Report	IEEE Std 497-2002 and Reg. Guide 1.97 Rev. 4
<p>1. HSIs needed to perform credited manual actions:</p> <ul style="list-style-type: none"> <li>• Prompting indications</li> <li>• Prompting alarms</li> <li>• Controls &amp; immediate feedback indications</li> <li>• Performance indications</li> <li>• Performance alarms</li> </ul> <p><i>The two treatments are consistent for indications supporting the credited manual actions; however, the Reg. Guide does not address the controls needed to take the actions or the other supporting HSIs listed above.</i></p>	<p>Actions specifically credited in the SAR safety analyses for accident mitigation, and for which no automatic control is provided. This category addresses time-critical actions; longer-term actions (e.g., actions needed to achieve safe shutdown after completing event mitigation actions, or mitigation actions required several hours after an initiating event) are not addressed here but likely will be covered by other categories below. Credited manual actions may be system-level actuations or control of individual components such as pumps or valves. Manual actuation or control of auxiliary equipment needed in the short term to support the primary equipment being controlled also is included here.</p>	<p><b>Type A Variables</b> – Those variables that provide the primary information required to permit CR operating staff to take specific planned manually-controlled actions for which no automatic control is provided and that are required for safety systems to perform their safety-related functions as assumed in the accident analysis or are required to mitigate the consequences of an AOO.</p> <p>IEEE 497 indicates that Type A variables do not include those associated with “contingency actions” (alternative actions taken to address unexpected responses of the plant or conditions beyond its licensing basis – for example, actions taken for multiple equipment failures). However, Reg. Guide 1.97 Rev. 4 modifies the wording in the standard such that “Type A variables include those variables that are associated with contingency actions that are within the plant licensing basis and may be identified in written procedures.”</p>

HSIs	Industry Guidance Report	IEEE Std 497-2002 and Reg. Guide 1.97 Rev. 4
<p>2. Monitor safety functions and back up automatic success paths</p> <ul style="list-style-type: none"> <li>• Indications                             <ul style="list-style-type: none"> <li>- Status of critical safety functions, fission product barriers, and safety system performance</li> <li>- Safety system actuation status</li> </ul> </li> <li>• Alarms</li> <li>• Manual system-level actuation controls</li> <li>• Manual component-level controls</li> <li>• Prompting indications and manual controls used for D3 coping capability:                             <ul style="list-style-type: none"> <li>- Specific manual actions credited in the D3 evaluation for BTP 7-19 Points 1 thru 3</li> <li>- System-level monitoring and actuations called for in Point 4 of BTP 7-19</li> </ul> </li> </ul> <p><i>Partial overlap – the Reg. Guide addresses monitoring of safety functions, fission product barriers, and safety system performance; however, it does not address alarms, controls, or D3 coping capability.</i></p>	<p>This covers HSIs needed for monitoring the performance of the automatic systems and associated safety equipment, and backing them up as necessary. It includes monitoring critical safety functions, and manual actuation of safety systems when necessary.</p>	<p><b>Type B Variables</b> – Those variables that provide primary information to the control room operators to assess the plant critical safety functions. Sources: plant functional restoration EPGs, plant-specific EOPs, and plant critical safety function status trees, as applicable.</p> <p><b>Type C Variables</b> – Those variables that provide primary information to the control room operators to indicate the potential for breach or the actual breach of the three fission product barriers (extended range): fuel cladding, reactor coolant system pressure boundary, and containment pressure boundary. These variables represent a minimum set of plant variables that provide the most direct indication of the integrity of the three fission product barriers and provide the capability for monitoring beyond the normal operating range.</p> <p><b>Type D Variables</b> – Those variables that are required in procedures and licensing basis documentation to: a) indicate the performance of those safety systems and auxiliary supporting features necessary for the mitigation of design basis events, b) indicate the performance of other systems necessary to achieve and maintain a safe shutdown condition, and c) verify safety system status. These variables shall be based on the plant accident analysis licensing basis and the following procedures as applicable: a) event-specific EPGs or plant-specific EOPs, b) functional restoration EPGs or plant-specific EOPs, and c) plant AOPs.</p>

HSIs	Industry Guidance Report	IEEE Std 497-2002 and Reg. Guide 1.97 Rev. 4
<p>3. Carry out preferred manual safety success paths</p> <ul style="list-style-type: none"> <li>• Prompting indications</li> <li>• Prompting alarms</li> <li>• Controls and immediate feedback indications</li> <li>• Performance indications</li> <li>• Performance alarms</li> </ul> <p><i>Partially addressed by the Reg. Guide – specifically, indications supporting achieving and maintaining safe shutdown. However, alarms and controls are not addressed in the Reg. Guide.</i></p>	<p>The EPGs or the plant-specific EOPs provide multiple ways for operators to deal with plant emergencies and accident scenarios; these are referred to as “success paths.” This category addresses manual success paths (not including credited manual actions covered in item 1 above) for which there is no automated success path. These may be actions that support the automatic protection systems in mitigating accident conditions, or longer-term actions needed to achieve safe shutdown. When multiple success paths are available, this category specifically addresses those manual success paths that are the preferred paths (those the operators would choose first if available). Also, this category is restricted to “safety success paths” – success paths that make use of safety equipment to accomplish the needed actions.</p>	<p>Partially addressed by <b>Type D Variables</b> – Those variables that are required in procedures and licensing basis documentation to: a) indicate the performance of those safety systems and auxiliary supporting features necessary for the mitigation of design basis events, b) indicate the performance of other systems necessary to achieve and maintain a safe shutdown condition, and c) verify safety system status.</p> <p>Items a) and b) in this definition imply that indications needed per the EPGs or EOPs to mitigate design basis events and achieve and maintain a safe shutdown condition would be included as part of the Type D variables.</p>
<p>4. Preferred manual non-safety success paths</p> <ul style="list-style-type: none"> <li>• Prompting indications and alarms</li> <li>• Controls and immediate feedback indications</li> <li>• Performance indications and alarms</li> </ul> <p><i>Partially addressed by the Reg. Guide – specifically, indications</i></p>	<p>This addresses success paths called out in the EPGs or plant-specific EOPs that require manual action, make use of non-safety equipment, and are preferred in that they would be the first choice for achieving safe shutdown over other alternative paths that may result in undesirable consequences.</p>	<p>Partially addressed by <b>Type D Variables</b> – Those variables that are required in procedures and licensing basis documentation to: a) indicate the performance of those safety systems and auxiliary supporting features necessary for the mitigation of design basis events, b) indicate the performance of other systems necessary to achieve and maintain a safe shutdown condition, and c) verify safety system status.</p> <p>Items a) and b) in this definition imply that indications needed per the EPGs or EOPs to mitigate design basis events and achieve and maintain a safe shutdown condition would be included as part of the Type D variables. In particular, because item b) addresses</p>

HSIs	Industry Guidance Report	IEEE Std 497-2002 and Reg. Guide 1.97 Rev. 4
<p><i>supporting achieving and maintaining safe shutdown. However, alarms and controls are not addressed in the Reg. Guide.</i></p>		<p>“other systems” beyond the safety systems, it can be concluded that indications associated with non-safety success paths would be included in the Type D variables.</p>
<p>5. Additional post-accident monitoring for radioactivity releases</p> <ul style="list-style-type: none"> <li>• Indications</li> <li>• Alarms</li> </ul> <p><i>Consistent for indications, but the Reg. Guide does not address alarms</i></p>	<p>This specifically addresses the Type E variables specified in Reg. Guide 1.97 for monitoring releases of radioactivity.</p>	<p><b>Type E Variables</b> – Those variables required for use in determining the magnitude of the release of radioactive materials and continually assessing such releases. Alarms are not addressed in Reg. Guide 1.97 Rev.4.</p>
<p>6. Monitor safety system availability</p> <ul style="list-style-type: none"> <li>• Indications and alarms</li> </ul> <p><i>Not addressed by Reg. Guide 1.97 Rev. 4</i></p>	<p>This addresses monitoring of safety system availability during normal plant operation, as well as in emergencies – in particular, it addresses HSI needed to monitor bypassed and inoperable status of the safety systems (Reg. Guide 1.47).</p>	<p><i>Not addressed in Reg. Guide 1.97 Rev. 4 or IEEE Std 497</i></p>
<p>7. Monitor safety parameters</p> <ul style="list-style-type: none"> <li>• Safety parameter indications</li> <li>• Safety parameter alarms</li> <li>• Other prompting indications for pre-emptive safety actions</li> <li>• Controls for pre-emptive safety actions</li> </ul> <p><i>Not addressed by the Reg. Guide</i></p>	<p>This addresses additional monitoring of safety parameters during normal plant operation beyond the critical safety function monitoring required by Reg. Guide 1.97 (see item 2 above), and taking discretionary, pre-emptive actions when needed to address safety challenges</p>	<p><i>Reg. Guide 1.97 Rev. 4 requirements for monitoring of critical safety functions (Type B variables) are discussed under item 2 above. The reg. guide does not address additional indications of safety parameter status such as those provided by SPDS.</i></p>

HSIs	Industry Guidance Report	IEEE Std 497-2002 and Reg. Guide 1.97 Rev. 4
<p>8. Continue operation under conditions in which normally-used HSIs have failed or are degraded</p> <ul style="list-style-type: none"> <li>• Indications, alarms and controls needed to support desired capabilities</li> </ul> <p><i>Not addressed by the Reg. Guide</i></p>	<p>This addresses additional, discretionary capabilities for continued operation in situations involving failure or degradation of the normally-used control room HSIs – beyond the capabilities for accident mitigation and safe shutdown already required by regulation.</p>	<p><i>Not addressed in Reg. Guide 1.97 Rev 4 or IEEE Std 497</i></p>
<p>9. Perform other important tasks during normal operation with all HSIs functioning</p> <ul style="list-style-type: none"> <li>• Indications, alarms and/or controls needing enhanced accessibility</li> </ul> <p><i>Not addressed by the Reg. Guide</i></p>	<p>This addresses functions and tasks during normal operations that have not been covered by the items above, and which benefit from greater accessibility of the associated HSIs (i.e., more accessible than a typical workstation involving selectable displays, controls and alarms).</p>	<p><i>Not addressed in Reg. Guide 1.97 Rev. 4 or IEEE Std 497</i></p>