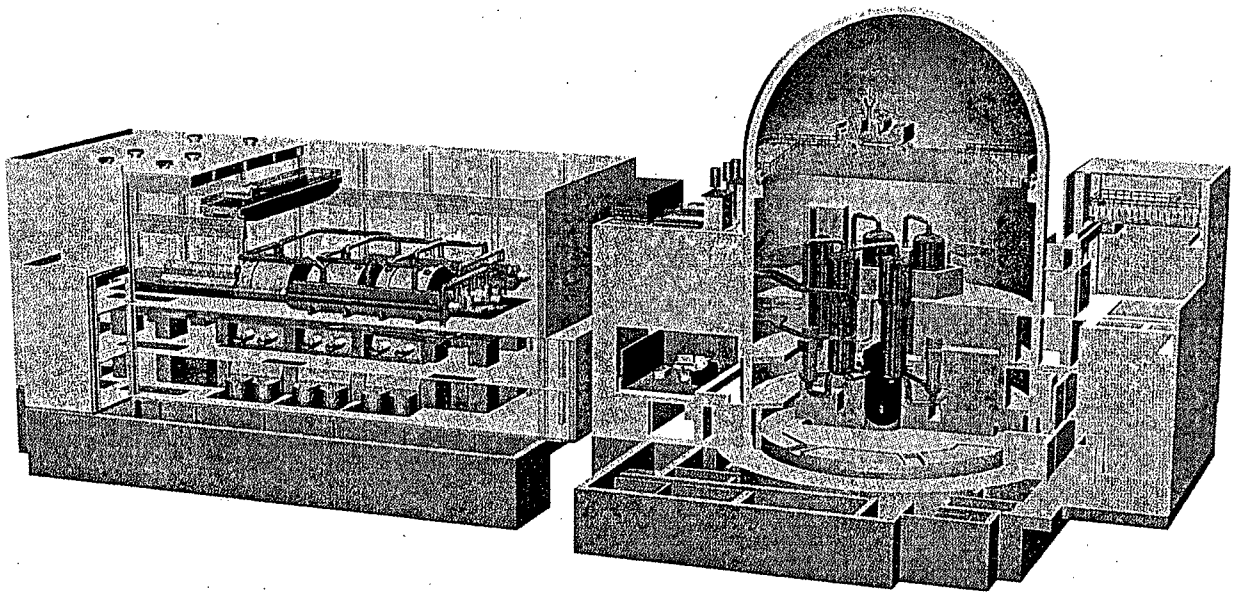
Non-Proprietary

US-APWR Topical Report

HSI System Description and HFE Process



Doc. Number :
MUAP-07007-NP R1

July 2007

MITSUBISHI HEAVY INDUSTRIES, LTD.

HSI System Description and HFE Process

Non Proprietary Version

July 2007

Revision History

Revision	Date	Page (Section)	Description
0	April 2007	All	Original issued
1	July 2007		The following items are revised based on NRC comments or correcting erratum.
		All	Pictures were replaced to color version.
		8 (3.4)	Descriptions were corrected.
		15 (4.1)	A description about the operational VDU qualification was added.
		19 (4.2.2)	A description about RSC was added.
		21-22 (4.3.1 b.)	A reason applying noise level "raised" was added.
		41 (4.5.3)	Physical tag descriptions were added.
		76 (4.10.3)	Further notes of the minimum inventory HSI were added.
		82 (4.11.4)	Descriptions were corrected.
		85 (4.12)	A Minimum Inventory HSI process was added.
		87 (5.0)	Descriptions about HFE process were added.
		100 (5.3.2.1)	Further notes of the automation rule were added.
		135 (5.10.2.1)	Descriptions that accidents are including CCF condition were added.

Mitsubishi Heavy Industries, Ltd.
16-5, Konan 2-chome, Minato-ku
Tokyo 108-8215 Japan

Abstract

This topical report describes the functional design of the MHI Human System Interface (HSI) System and the Human Factors Engineering (HFE) process used to create this system and apply it to specific nuclear power plants. The hardware and the software used to implement the HSI System's functional design are described in other topical reports. MHI seeks NRC approval of the HSI System design and its design process for application to the HSI System of the US-APWR and replacement of current HSI systems in operating plants. The HSI System is essentially the same as the HSI System developed by MHI and MELCO for nuclear power plants in Japan. For applications in the US, this report demonstrates conformance of the HSI System design and design process with all applicable US Codes and Standards. These include the applicable provisions of:

- Code of Federal Regulations
- Regulatory Guides
- Branch Technical Positions
- NUREG-Series Publications
- IEEE-Standards
- Other Industry Standards

MHI, MELCO and Japanese PWR Owner Group utilities have developed an advanced HSI System that reflects past human factors studies and employs state of the art electronics technology. The HSI System includes of an operator console, a supervisor console and a Large Display Panel (LDP). It features soft controls for the manipulation through Visual Display Unit (VDUs) with touch panels. The HSI System has been evaluated by Japanese utility operators using a prototype main control board driven by a plant simulator. The facility for this evaluation was prepared by MELCO.

Most of the HSI System is fully computerized, although there are some portions that utilize conventional switches and indicators. The fully computerized portion of the HSI System provides significant benefits to the safety of nuclear power, such as the reduction in operations and maintenance work load, which reduces the potential for human error. Based on the experience in Japan, MHI and MELCO's computerized digital HSI System improves the operability, reliability and availability of plant operations.

This topical report describes the functional design of MHI and MELCO's HSI System, which includes:

- Non-safety HSI based on Video Display Units which allow monitoring and control of both non-safety and safety functions
- A non-safety Large Display Panel which provides spatially dedicated continuously visible (SDCV) HSI for information important to plant operability and safety
- Safety related HSI based on Video Display Units which allow monitoring and control of safety functions
- Safety related HSI based on spatially dedicated continuously visible conventional controls for system level actuation of Reactor Trip and Engineered Safety Feature Actuation Systems
- The ability to monitor and control critical safety functions through systems that are diverse from the HSI and supporting systems described above.

In addition, this topical report describes the HFE design process which considers all elements of NUREG-0711, as follows:

- Human Factors Engineering Program
- Operating Experience Review (OER)
- Functional Requirements Analysis and Function Allocation
- Task Analysis
- Staffing and Qualification
- Human Reliability Analysis (HRA)
- HSI Design
- Operating Procedure Development Plan
- Procedures for Normal Operation
- Procedures for Accident Operation
- Training Program Development Plan
- Human Factors Verification and Validation
- Design Implementation Plan
- Human Performance Monitoring Plan

The HSI System takes advantage of digital technology capabilities that were not available for analog systems. Some of the design aspects of the system may not be readily familiar to those acquainted with previous analog designs. Therefore this document puts special emphasis on the explanation of the technical aspects of the HSI System design and its conformance to codes and standards. The following are key areas in which the design presents significant innovations:

- Multi-channel operator stations
- HSI System's ability to accommodate reduced operator staffing
- Operation under degraded conditions
- Common cause failure modes for Defense-in-Depth and Diversity (D3) analysis
- Minimum inventory of HSI
- Computer based procedures

MHI specifically seeks NRC approval of the HSI System design in these areas.

This report distinguishes between the descriptions applicable to the US-APWR and those relevant to operating plants, where there is a clear need for such a distinction. Where there are no distinctions, the description is generically applicable to the US-APWR and a broad range of operating plants, although not necessarily all operating plants. When this topical report is referenced in a plant-specific Licensing Amendment Request, the Plant Licensing Documentation will identify any areas of this topical report that are not applicable.

The complete MHI digital instrumentation and control (I&C) design is described in four Topical Reports:

- Safety I&C System Description and Design Process
- Safety System Digital Platform - MELTAC -
- HSI System Description and HFE Process(Human Factor Engineering) Process (this report)
- Defense in Depth and Diversity

This document identifies the additional HSI and HFE related information to be submitted for NRC approval in future Plant Licensing Documentation. This Plant Licensing Documentation, in combination with the contents of this Topical Report and the contents of the other Topical Reports identified above, is expected to be sufficient to allow the NRC to make a final safety determination. Other documentation generated during the design process is available for NRC audit, as may be needed to allow the NRC to fully review the HSI System design and the HFE design process.

Table of Contents

List of Tables

List of Figures

List of Acronyms

AOO	Anticipated Operational Occurrences
ARP	Alarm Response Procedure
ATWS	Anticipated Transient Without Scram
BHEP	Basic Human Error Probability
BISI	Bypassed or Inoperable Status Indication
CCF	Common Cause Failure
CCW	Component Cooling Water
C/C	Control Center
COL	Combined License
CBP	Computer-based Operating Procedure
COTS	Commercial-Off-The-Shelf
CPU	Central Processing Unit
CV	Containment Vessel
D3	Defense-in-Depth and Diversity
DAC	Design Acceptance Criteria
DAS	Diverse Actuation System
DBA	Design Basis Accident
DC	Design Certification
DCD	Design Control Document
DF	Dependency Factor
DHP	Diverse HSI Panel
DMC	Date Management Console
DTM	Design Team Manager
ECCS	Emergency Core Cooling System
EF	Error Factor
EFC	Error-Forcing Contexts
EFW	Emergency Feed Water
ELM	Engineering Line Manager
EOF	Emergency Operations Facility
EP	Back Feed Electric Power
EPM	Engineering Project Manager
ESF	Engineered Safety Feature
ESFAS	Engineered Safety Feature Actuation System
FMEA	Failure Modes and Effects Analyses
FC	Fail to Close
FC	First Concrete
FO	Fail to Open
F.O.	First Out
FTA	Fault Tree Analysis
GOMS	Goals, Operators, Methods, and Selection rules
GUI	Graphical User Interfaces
HA	Human Action

HAZOP	Hazards and Operability Analysis
HDSR	Historical Data Storage and Retrieval
H.E	Human Error
HED	Human Engineering Descriptions
HEP	Human Error Probability
HEPA	High-Efficiency Particulate Air
HFE	Human Factors Engineering
HFEVTM	HFE V&V Team Manager
HRA	Human Reliability Analysis
HSI	Human System Interface
HSIS	Human System Interface System
HVAC	Heating, Ventilation, and Air Conditioning
I&C	Instrumentation and Control
ITAAC	Inspections, Tests, Analyses, and Acceptance Criteria
ITV	Industrial Television
LBB	Leak Before Break
LBLOCA	Large Break Loss Of Coolant Accident
LC	Locked to Close
LCO	Limiting Condition for Operation
LDP	Large Display Panel
LER	Licensee Event Report
LERF	Large Early Release Frequency
LO	Locked to Open
LOCA	Loss Of Coolant Accident
MCB	Main Control Board
MCR	Main Control Room
M/C	Metal Clad Geer
MELCO	Mitsubishi Electric Corporation
MELTAC	Mitsubishi Electric Total Advanced Controller
MHI	Mitsubishi Heavy Industries
MSLB	Main Steam Line Break
NIS	Nuclear Instrumentation System
NPP	Nuclear Power Plant
OER	Operation Experience Review
OSD	Operational Sequence Diagram
PAM	Post Accident Monitor
PCMS	Plant Control and Monitoring System
PM	Project Manager
PRA	Probabilistic Risk Assessment
PRC	Process Recording Computer
PSF	Performance Shaping Factor
PSMS	Protection and Safety Monitoring System
QA	Quality Assurance

RCS	Reactor Coolant System
R.G.	Regulatory Guide
RHR	Residual Heat Removal
RMS	Radiation Monitoring System
RO	Reactor Operator
RPS	Reactor Protection System
RSC	Remote Shutdown Console
RSR	Remote Shutdown Room
RSS	Remote Shutdown Station
RT	Reactor Trip
RTB	Reactor Trip Breaker
RWSP	Refueling Water Storage Pit
SAR	Safety Analysis Report
SAT	Systematic Approach to Training
SDCV	Spatially Dedicated Continuously Visible
SER	Safety Evaluation Report
SFP	Spent Fuel Pit
SG	Steam Generator
SGTR	Steam Generator Tube Rupture
SLS	Safety Logic System
SBO	Station Black Out
SPDS	Safety Parameter Display System
SRO	Senior Reactor Operator
SS	Shift Supervisor
STA	Shift Technical Advisor
Tcold	Reactor Coolant Inlet Temperature
T/C	Thermocouple
Thot	Reactor Coolant Outlet Temperature
THERP	Technique for Human Error Rate Prediction method
TMI	Three Mile Island
TR	Topical Report
TSC	Technical Support Center
UMC	Unit Management Computer
UPS	Uninterruptible Power Supply
UV	Under Voltage
V&V	Verification and Validation
VDU	Visual Display Unit
VTM	V&V Team Manager

1.0 PURPOSE

The purpose of this Topical Report is to describe the Mitsubishi Heavy Industries (MHI) Human System Interface (HSI) System (HSIS) design and the Human Factors Engineering (HFE) design process used by MHI for that system. MHI seeks approval from the US Nuclear Regulatory Commission for the use of the MHI HSI System for new nuclear plants and for operating nuclear plants.

The design process described in this report is applicable to the MHI Human System Interface designs for both new and existing operating plants. The system descriptions are directly applicable to the MHI US-APWR. For operating plants the basic design features that ensure regulatory compliance are maintained, as described in this report. However, due to plant differences, specific changes in implementation detail will be described in Plant Licensing Documentation (e.g., License Amendment Request or Final Safety Analysis Report).

2.0 SCOPE

In this report the complete set of safety and non-safety HSI components is referred to as the HSI System. The safety-related HSI elements described in this report are part of the Protection and Safety Monitoring System (PSMS). The PSMS includes the Reactor Protection System, the Engineering Safety Feature Actuation System, the Safety Logic System and the Safety-Grade HSI System. The non-safety HSI elements described in this report are part of the Plant Control and Monitoring System (PCMS) or the Diverse Actuation System (DAS). The PCMS includes reactor and turbine control systems. The DAS provides backup monitoring and control for critical safety functions.

The HSI for the PSMS is built on the MELTAC Platform, which is described in a separate Digital Platform Topical Report. In addition, the MELTAC Platform is applied to portions of the HSI for the Plant Control and Monitoring System. The MELCO computer used for non-safety applications is a different design than that used for safety-related applications. There are also differences in Quality Assurance processes for the design and manufacturing of both. The DAS, including its HSI, is diverse from the PCMS and the PSMS. These safety and non-safety systems are described in this report only to the extent necessary to understand their HSI. Other topical reports describe the design of the hardware and software of these systems and the design process used to create that hardware and software.

This report consists of two parts. The first part, Section 4, describes the HSI System design. The second part, Section 5, describes the design process used in creating that design.

3.0 APPLICABLE CODES, STANDARDS AND REGULATORY GUIDANCE

This section identifies the HSI System's compliance with applicable codes and standards. Unless specifically noted, the latest version of the codes and standards issued as of the date of this document is the applicable one. The following terminology is used in this section:

Plant Licensing Documentation – This refers to plant level documentation that is specific to a group of plants or a single plant, such as the Design Control Document (DCD), Combined Operating Licensing (COL) Application, Final Safety Analysis Report, or License Amendment Request.

HSI System - This refers to the functional design of the safety and non-safety HSI components that are the subject of this Topical Report. The "HSI System" includes the MHI safety related and non-safety related HSI. The terms "PSMS HSI", "PCMS HSI" and "DAS HSI" refer to different elements of the overall HSI System.

The codes and standards applicable to MHI's complete digital I&C system are described in other topical reports. The codes and standards identified below are those that directly affect the functional design of the HSI System.

3.1 Code of Federal Regulations

1. 10 CFR 50 Appendix A: General Design Criteria for Nuclear Power Plants

GDC 1 :Quality Standards and Records
The Quality Assurance program for the MHI System meets the requirements of 10 CFR 50 Appendix B.

GDC 5 : haring of Structures, Systems, and Components
In general, there is no sharing of this Equipment among nuclear power units. Any sharing is discussed in specific Plant Licensing Documentation.

GDC 12 : Suppression of Reactor Power Oscillations
HSI for specific reactor trip functions is described in Plant Licensing Documentation.

GDC 13 : Instrumentation and Control
HSI for specific instrumentation and control functions are described in Plant Licensing Documentation.

GDC 19 : Control Room
The HSI System provides the safety-related and non-safety related Human System Interface for the control room. The Human Factors Engineering design aspects of the HSI and the control room design are described in this report.

GDC 20 : Protection System Functions
HSI for specific protection system functions is described in Plant Licensing Documentation.

GDC 21 : Protection System Reliability and Testability
The HSI for manual test features for the areas that are not covered by automated

tests are described in this report. Most manual tests may be conducted with the plant on line, and with the protection functions bypassed or out of service. Equipment that cannot be tested with the plant on line can be tested with the plant shut down.

GDC 22 : Protection System Independence
The HSI used to monitor interlocks between redundant divisions during maintenance operations is performed on one division at a time, as described in this report.

GDC 23 : Protection System Failure Modes
All detected failures are alarmed. The HSI for failure detection and alarms are described in this report.

GDC 24 : Separation of Protection and Control Systems
Where safety sensors are shared between control and protection systems, signal selection logic in the control system prevents erroneous control actions due to single sensor failures. The HSI used for sensor monitoring and failure alarms is described in this report.

GDC 25 : Protection System Requirements for Reactivity Control Malfunctions
HSI features to monitor and alarm reactivity control malfunctions are described in this report.

2. Applicable 10 CFR 50.34 (f)(2) Post-TMI Requirements

- (iii) Control room design
  The Human Factors design aspects of the HSI and the control room are described in this document.

- (iv) Safety Parameter Display Console
  The PCMS HSI described in this report provides safety parameter displays in the control room.

- (v) Bypassed and inoperable safety system status indication
  This indication is provided by the PCMS HSI.

- (xi) Relief and safety valve position Indication
- (xii) Auxiliary feedwater system initiation and flow indication
- (xiii) Pressurizer heater control
- (xiv) Containment isolation systems
- (xvii) Accident monitoring instrumentation
- (xviii) Inadequate core cooling monitoring
- (xix) Instruments for monitoring plant conditions following core damage
- (xx) Pressurizer level indication and controls for pressurizer relief and block valves
  The HSI for items xi thru xiv and xvii through xx above are generally described in this topical report. Specific display designs are described in Plant Licensing Documentation.

3. 10 CFR 50.36 Technical specifications
1) Safety limits, limiting safety system settings, and limiting control settings.
The HSI System is used to monitor safety limits and control limits.

3) Surveillance requirements
The HSI System provides extensive automatic testing, as discussed above with respect to with GDC 21. It is used for periodic surveillances to confirm the operability of the automatic test features and to manually test features of the system that are not tested automatically. Most manual tests may be conducted with the plant on line. Functions that cannot be tested with the plant on line are tested during plant shutdown.

4. 10 CFR 50.55.a
(a)(1) Quality Standards for Systems Important to Safety
The HSI System was originally developed under a Japanese nuclear quality program that is equivalent to 10 CFR 50 Appendix B. Other licensing documents describe this equivalence. An approved 10 CFR 50 Appendix B quality program is now in effect for all the equipment comprising the System.

(h) Invokes IEEE Std. 603-1991
See compliance with IEEE 603-1991

5. 10 CFR 50.62 ATWS Rule
The Diverse Actuation System is used to actuate plant systems for Anticipated Transient Without Scram (ATWS) mitigation. The DAS HSI is described briefly in this Topical Report and in more depth in the Topical Report for Defense in Depth and Diversity.

6. 10 CFR 50.54(m)(2)(iii)
Section 5.4 of the Topical Report describes how the HSI System supports the following minimum Main Control Room staffing requirements:
(iii) When a nuclear power unit is in an operational mode other than cold shutdown or refueling, as defined by the unit's technical specifications, each licensee shall have a person holding a senior operator license for the nuclear power unit in the control room at all times. In addition to this senior operator, for each fueled nuclear power unit, a licensed operator or senior operator shall be present at the controls at all times. That section of the report also describes how this HSI supports higher staffing levels. Actual staffing levels are described in Plant Licensing Documentation.

7. 10 CFR 52.47
(a)(2) Level of Detail
The information provided in this Topical Report, together with the additional information described in other digital system Topical Reports and DCD, are sufficient to allow the NRC staff to reach a final conclusion on all safety questions associated with the design before certification of the US-APWR design is granted. The information includes performance requirements and design information sufficiently detailed to permit the preparation of acceptance and inspection requirements by the NRC, and procurement specifications and construction and installation specifications by an applicant.

(b)(2)(i) Innovative Means of Accomplishing Safety Functions
In the near term, the HSI System is expected to be applied to conventional I&C safety and non-safety functions typical of current operating plants and new evolutionary plants. In the longer term, the HSI System is expected to be applied to such innovative safety functions as may be typical of new passive plants. All specific plant safety functions are described in the Plant Licensing Documentation.

8. 10 CFR 52.79(c) ITAAC in Combined Operating License Applications
   The inspections, tests, analyses and acceptance criteria that demonstrate that the HSI System has been constructed and will operate in conformity with the Commission's regulations will be provided in the Plant Licensing Documentation.

3.2 Staff Requirements Memoranda

9. SRM to SECY 93-087
   Item II.Q: Defense Against Common-Mode Failures in Digital Instrumentation and Control Systems
   Diverse monitoring and diverse manual control functions are provided by this HSI.

   Item II.T Control Room Annunciator (Alarm) Reliability
   Alarm annunciators are generally provided by the PCMS HSI. For Advanced Light Water Reactors there are no manual actions required for the safety systems to accomplish their safety functions, therefore there are no Class 1E annunciators. Any exceptions to this are described in the Plant Licensing Documentation.

3.3 NRC Regulatory Guides

10. R.G. 1.8 Personnel Selection and Training
    The HSI system copes with operating staffs and training system for operator staffs. The Reg. Guide endorses ANSI/ANS-3.1-1993 and ANSI/ASME NQA-1-1983. See with these ANSI Standards.

11. R.G. 1.22 Periodic Testing of Protection System Actuation Functions
    See GDC 21. Protection actuation functions are completely testable through a combination of overlapping automatic and manual tests. Manual tests can only be conducted when a division is bypassed. Divisions are interlocked to prevent concurrent bypassing of redundant functions in more than one redundant division. The HSI System supports manual tests, and displays and alarms for interlocks and automatic test results.

12. R.G. 1.47 Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems
    See compliance with 10 CFR 50.34 (f)(2)(v). The PCMS HSI provides alarms for all bypassed or inoperable safety functions; these alarms are provided on selectable displays. Spatially dedicated, continuously visible alarm displays are provided for any bypassed or inoperable condition that prevents actuation of the safety function at the division level. The ability to manually actuate bypassed or inoperable alarms at the division level is provided for conditions that are not automatically detected.

13. R.G. 1.62 Manual Initiation of Protective Actions
    The PSMS HSI provides manual initiation at the system level for all reactor protection system (RPS) and engineered safety feature actuation system (ESFAS) safety functions by conventional Spatially Dedicated Continuously Visible (SDCV) switches located in the main control room. Additional system level manual initiation switches may also be located at the Remote Shutdown panel, depending on the specific plant design; these are described in the Plant Licensing Documentation.

14. R.G. 1.97 Instrumentation for Light Water Cooled Nuclear Power Plants to Assess Plant Conditions During and Following an Accident (endorses IEEE Std. 497-2002)

The PCMS HSI displays signals from accident monitoring instrumentation of all variable Types. In addition, the PSMS HSI displays signals for Type A and B variables and meets all applicable Class 1E requirements. Display designs for specific accident monitoring instrumentation are described in the Plant Licensing Documentation.

15. R.G. 1.105 Setpoints for Safety-Related Instrumentation (endorses ISA-S67.04-1994 and ANS-10.4-1987)
    The uncertainties associated with the PSMS and PCMS are described in the Safety System and Digital Platform Topical Reports. They include uncertainties for signal conditioning modules, signal splitters, instrument loop power suppliers and analog to digital converters. The displays and alarms from the PSMS HSI and PCMS HSI are generated from the digital values within the controllers of these systems. Therefore, there are no additional uncertainties associated with the HSI for these systems. The uncertainties associated with the DAS HSI are negligible in meeting the acceptance criteria of BTP-19.

16. R.G. 1.114 Guidance to Operators at the Controls and to Senior Operators in the Control Room of a Nuclear Power Unit.
    See compliance with 10 CFR 55.54

17. R.G. 1.118 Periodic Testing of Electric Power and Protection Systems (endorses IEEE 338-1987)
    See compliance with GDC 21, 10 CFR 50.36 and R.G. 1.22. All safety functions are tested either automatically or manually. Manual tests do not require any system reconfiguration, such as jumpers or fuse removals, which have a potential for human performance errors.

18. R.G. 1.149, Rev.3 Nuclear Power Plant Simulators for Use in Operator Training (endorses ANSI/ANS-3.5-1998)
    The HFE program plans to develop operator training program.

19. R.G. 1.152 Criteria for Programmable Digital Computers in Safety Systems of Nuclear Power Plants (endorses IEEE 7-4.3.2-2003)
    The methods used for specifying, designing, verifying, validating and maintaining software for the PSMS HSI complies with these Regulatory Guide requirements. The life cycle process for the digital platform software is described in the Digital Platform Topical Report. The life cycle process for the system application software is described in the Safety I&C System Description and Design Process Topical Report. The methods used for controlling cyber threats throughout the life cycle are described in these documents.

20. R.G. 1.153 1996 Criteria for Safety Systems (endorses IEEE Std 603-1991)
    Compliance with the General Design Criterion identified in this Regulatory Guide is discussed above. Compliance with IEEE 603-1991 is discussed below.

21. R.G. 1.168 Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants (endorses IEEE Std 1012-1998 and IEEE Std 1028-1997)
    The PSMS HSI uses processes for verification, validation, reviews and audits that comply with this Regulatory Guide. The design processes for the digital platform are described in the Digital Platform Topical Report. The design processes for plant systems are described in the Safety I&C System Description and Design Process Topical Report.

22. R.G. 1.174 An approach for using probabilistic risk assessment in risk-informed decisions on plant specific changes to the licensing basis
The HFE program approaches risk-informed view of points in task analysis, HRA, etc.

23. R.G. 1.177 An Approach for Plant-Specific, Risk-Informed Decisionmaking: Technical Specifications
The HFE program approaches risk-informed view of points in task analysis, HRA, etc.

24. R.G. 1.187 Guidance for Implementation of 10 CFR 50.59, Changes, Tests, and Experiments R.G. 1.196 Revision 02 Control Room Habitability at Light-water Nuclear Power Reactors
Control Room Habitability systems ensure the main control room (MCR) environment is adequate to allow operators to maintain plant control limits during normal operation and to maintain plant safety limits during and after anticipated transients or design basis accidents. The systems to ensure Control Room Habitability are described in Plant Licensing Documentation.

3.4 NRC Branch Technical Positions

25. BTP HICB-1 Guidance on Isolation of Low-Pressure Systems from the High-Pressure Reactor Coolant System
26. BTP HICB-2 Guidance on Requirements of Motor-Operated Valves in the Emergency Core Cooling System Accumulator Lines
27. BTP HICB-3 Guidance on Protection System Trip Point Changes for Operation with Reactor Coolant Pumps out of Service
28. BTP HICB-4 Guidance on Design Criteria for Auxiliary Feedwater Systems
29. BTP HICB-5. Guidance on Spurious Withdrawals of Single Control Rods in Pressurized Water Reactors
30. BTP HICB-6 Guidance on Design of Instrumentation and Controls Provided to Accomplish Changeover from Injection to Recirculation Mode

    The HSI System provides displays, alarms and controls for the plant components that address BTP HICB 1 thru 6, above. Specific HSI designs are described in Plant Licensing Documentation.

31. BTP HICB-8 Guidance for Application of Regulatory Guide 1.22
All functions of the protection system are testable at power. The HSI System supports this testing.

32. BTP HICB-9 Guidance on Requirements for Reactor Protection System Anticipatory Trips
There are no non-safety anticipatory trips used in the reactor protection system. Any exception to this will be described in Plant Licensing Documentation. If any non-safety trips are used in the protection system the HSI System would support such trips. .

33. BTP HICB-10 Guidance on Application of Regulatory Guide 1.97
The HSI System complies with this BTP for displays and alarms for all instrumentation signals. However, R.G. 1.97 Revision 4 has superseded Revisions 2 and 3, for which this BTP was written. Therefore, where there are conflicts, the HSI System meets the requirements of R.G. 1.97 Revision 4.

34. BTP HICB-12 Guidance on Establishing and Maintaining Instrument Setpoints
See compliance with R.G. 1.105.

35. BTP HICB-16 Guidance on the Level of Detail Required for Design Certification Applications Under 10 CFR Part 52
See compliance with 10 CFR 52.47. This Design Acceptance Criterion applies only to HSI System final display designs and HFE validation. The level of detail needed for the NRC staff to make a final safety determination is described in Plant Licensing Documentation.

36. BTP HICB-17 Guidance on Self-Test and Surveillance Test Provisions
See compliance with GDC 21, 10 CFR 50.36, R.G. 1.22 and R.G. 1.15. Surveillance testing, taken together with automatic self-testing, provides a mechanism for detecting all failures. The HSI System supports both functions.

37. BTP HICB 19 Guidance on Evaluation of Defense in Depth and Diversity in Digital Computer Based I&C Systems
The Defense-in-Depth and Diversity (D3) Topical Report describes the diversity within the safety and non-safety I&C systems, including the diversity between the PSMS HSI, PCMS HSI and DAS HSI. That report also describes the methodology for coping with an Anticipated Operation Occurrence (AOO) or Postulate Accident (PA) concurrent with a common cause failure (CCF) of the PSMS and PCMS. The D3 Coping Analysis method includes justification for credited manual operator actions which is evaluated through the HFE Program described in this report. Coping for all Anticipated Operation Occurrences and Postulate Accidents is described in Plant Licensing Documentation. This report describes the functional design of the PSMS HSI, PCMS HSI and DAS HSI.

38. BTP HICB 21 Guidance on Digital Computer Real Time Performance
The real-time performance for the HSI System complies with this BTP. The method for determining response time performance for the PSMS HSI is described in the Safety I&C System Description and Design Process Topical Report. The response time performance for digital platform components is described in the Digital Platform Topical Report.

3.5 NUREG-Series Publications (NRC Reports)

39. NUREG-0654, Criteria for Preparation and Evaluation of Radiological Emergency
The HSI System is used for monitoring and managing radiological emergencies.

40. NUREG-0696 Functional Criteria for Emergency Response Facilities
The PCMS HSI provides plant information at the Emergency Response Facilities such as Technical Support Center, Emergency Operating Facilities, etc.

41. NUREG-0700, Human-System Interface Design Review Guidelines
The HSI System design complies with these guidelines.

42. NUREG-0711, Human Factors Engineering Program Review Model
The design process used for the development of the HSI System and the training of personnel in the use of this system to operate the plant comply with the guidelines in this NUREG.

43. NUREG-0737, Supplement 1 Clarification of TMI Action Plan Requirements
The HSI System is used to comply with the following TMI Action Plan Requirements:

- Plant Safety Parameter Display – The HSI System provides safety parameter displays for the control room and for emergency support facilities.
- Indication and Control for Safety Components (e.g., relief valves, pressurizer heaters, containment isolation valves).

Inadequate Core Cooling Monitoring and Instrumentation for Accident Monitoring: -- The HSI System provides non-safety related and safety related displays for monitoring safety related instruments and non-safety related and safety related controls for safety related plant components.

44. NUREG-0800 Chapter 7 of the USNRC Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants, Rev.4
The HSI System fulfills all safety related requirements of this NUREG for monitoring safety related plant instrumentation and controlling safety related plant components. Descriptions of specific plant systems are provided in the Plant Licensing Documentation.

45. NUREG-0800 Chapter 18 of the USNRC Standard Review Plan for the Review of Human Factors Engineering for Nuclear Power Plants, Rev.1
The requirements of this NUREG for Human Factors Engineering Design Process are met by the HSI System. Descriptions of specific plant display screens and validation activities are described in the Plant Licensing Documentation.

46. NUREG-0899 Guidelines for the Preparation of Emergency Operating Procedures
The HSI System is used to display and execute Emergency Operating Procedures.

47. NUREG-1220 Training Review Criteria and Procedures
The training phase of the HFE Program complies with these requirements.

48. NUREG-1358 Lessons Learned From the Special Inspection Program for Emergency Operating Procedures
The procedure development phase of the HFE Program complies with these requirements.

49. NUREG-1560 Individual Plant Examination Program: Perspectives on Reactor Safety and Plant Performance
The performance monitoring phase of the HFE Program complies with these requirements.

50. NUREG-1764 Guidance for the Review of Changes to Human Actions
The performance monitoring phase of the HFE Program complies with these requirements.

3.6 IEEE Standards

51. IEEE 7-4.3.2 2003 Criteria for Programmable Digital Computer Systems in Safety Systems of Nuclear Power Generating Stations
The PSMS HSI conforms to all requirements of this standard, as augmented by R.G. 1.152, including key requirements for:
- Software quality and life cycle processes
- Independent Verification and Validation
- Communications independence

The HSI functional designs described in this Topical Report provide input to the software design process.

52. IEEE 338 1987 Periodic Surveillance Testing of Nuclear Power Generating Station Safety Systems
    The HSI System supports compliance with this standard, as augmented by R.G. 1.22.

53. IEEE 494 1974 Method for identification of Documents Related to 1E Equipment
    The documentation for the PSMS HSI conforms to this standard by having the term "Nuclear Safety Related" applied on the face of each document and drawing that is provided to the licensee. Generic documents and drawings used only for internal use by MHI do not contain this designation.

54. IEEE 497 2002 Accident Monitoring Instrumentation for Nuclear Power Generating Stations
    See compliance with R.G. 1.97.

55. IEEE 603 1991 Safety Systems for Nuclear Power Generating Stations
    (1998 version is currently not endorsed by NRC)
    The HSI System conforms to this standard, as augmented by R.G. 1.153, including key requirements for:
    - Quality
    - Testability
    - Monitoring and Information
    - Bypasses

3.7 Other Industry Standards

56. ANSI/ANS 3.1 Rev.1 -1999 Selection, Qualification, and Training of Personnel for Nuclear Power Plants
    See compliance with R.G. 1.8.

4.0 DESIGN DESCRIPTION

This section describes the main design features of the MHI HSI System. This HSI System has been designed in a joint project between MHI, MELCO and Japanese PWR Owner Group utilities (See Appendix A).

Figure 4.0-1 shows the design process for the MHI HSI System and the relationship between the design steps and the twelve Human Factor Engineering (HFE) elements presented in NUREG-0711, rev.2. HFE elements E01, E02, E03, E04, E05, E06, E07, E08, E10 and E11 were included in the design process with Japanese utilities, Elements E09 and E12 were not part of the design process in Japan. This topical report describes the HFE elements that were encompassed in the development program in Japan, the prepared a plan for the remaining two HFE elements (E09 and E12), and the plan for a more refined Human Reliability Analysis (HRA) methodology.

Table 4.0-1 compares the NUREG0711 HFE program elements to the elements in the HFE program implemented for Japanese PWRs. This table also identifies additional program plan activities conducted for US applications. A description of the HFE Program Plan is in the next section of this topical report.

Figure 4.0-1 shows the typical milestone of HSI design for US-APWR.

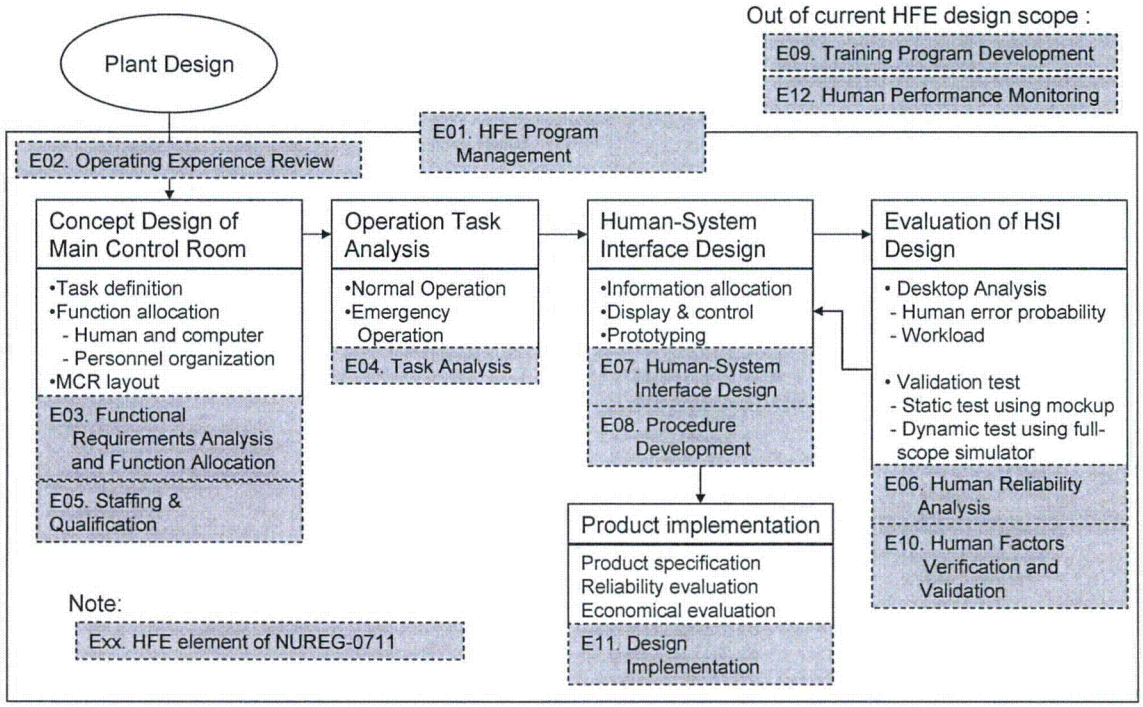


Figure 4.0-1 HFE Design Process of Past Mitsubishi PWR HSI

Table 4.0-1 Comparison of NUREG0711 HFE Program Elements to HFE Program Plan for Japanese PWRs and Additional HFE Program Plan Activities for US Applications

HFE element	Program Plan for US Applications	Experience in past development of Japanese PWR main control room
E01. HFE Program Management	MHI's design process conforms to NUREG-0711 normally. Additional documentation is required.	NUREG-0711 HFE elements, E01, E02, E03, E04, E05, E06, E07, E08, E10 and E11were executed in the design process. E09 and E12 were out of scope (activity of power utility). (See Figure A.1 Figure A.1 HFE Design Process of Mitsubishi PWR)
E02. Operating Experience Review	Approach is same as Japanese PWR	Operation Experience is input information of the concept design phase.
E03. Functional Requirements Analysis and Function Allocation	Approach is same as Japanese PWR	Functional requirements analysis and function allocation is considered in the concept design phase.
E04. Task Analysis	Approach is same as Japanese PWR	OSD was used in a gross and narrative task analysis, and Card's human information processing model was used in detail task analysis.
E05. Staffing and Qualifications	MHI proposes operation with one SRO and one RO in the MCR for compliance with 10CFR50.54	Design goal of operation with one RO
E06. Human Reliability Analysis	Approach is same as Japanese PWR	Omission and select errors were mainly analyzed. Human error probabilities were calculated using THERP for selected scenarios.
E07.Human-System Interface Design	Approach is same as Japanese PWR	Design plan was improved through iterative design process (design, prototyping , desktop evaluation, validation test).
E08.Procedure Development	Approach is same as Japanese PWR	Operation Procedure was developed for dynamic validation test.
E09. Training Program Development	Implementation plan is added	Out of scope from HSI development
E10. Human Factors Verification and Validation	Approach is same as Japanese PWR	Two type of test was executed. One is static test using HSI mockups. The other is dynamic test using prototype HSI system and full-scope plant simulator.
E11. Design Implementation	Implementation plan is added	Out of scope from HSI development
E12. Human Performance Monitoring	Implementation plan is added	Out of scope from HSI development

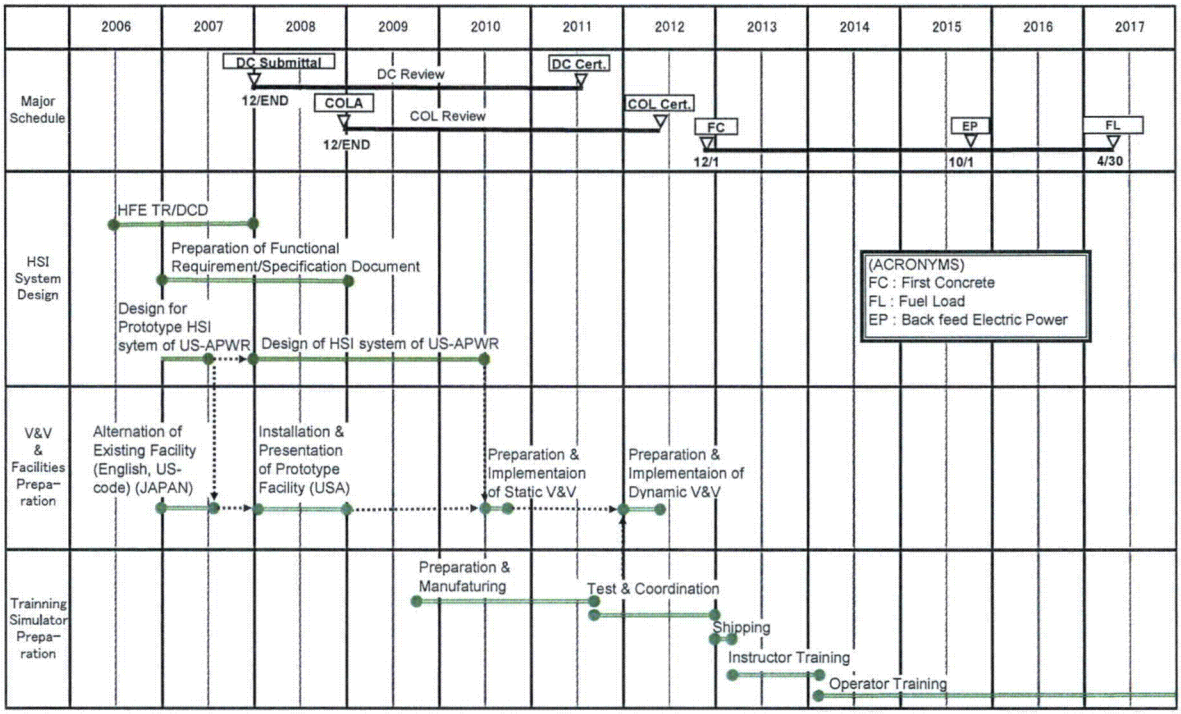


Figure 4.0-2 Typical Schedule of HSI Design for the US-APWR

4.1 Design Basis

The HSI System introduces the use of soft (touch or click based) operation utilizing the computer-based HSI. (See section 4.5) Soft operations are performed by requesting an Operational visual display unit (VDU) screen on an Operational VDU and then touching or clicking an operation area of a soft switch displayed on the screen. The benefits of the soft operation are to reduce the operator's workload compared with that of the conventional HSI by providing relevant process control information in integrated displays on VDUs and utilizing a compact console that minimizes required operator movement. The HSI System also provides operation support functions that utilize the computer to consolidate large amounts of data into meaningful information displays. These advanced features of the HSI System are expected to improve overall operator performance and reduce the potential for human error.

The HSI System utilizes various visual display devices, color-coding symbol-coding, etc. It is designed for use by plant personnel having average visual ability (i.e., no weaknesses in visual power or color-blindness limitations).

The HSI of the US-APWR utilizes various visual display devices, color-coding symbol-coding, etc. It is designed on the assumption of average visual ability by the plant operators (no weak visual power or color-blindness limitations).

They key features of the HSI System are summarized below, and explained in detail in the sections that follow

a. Integration of monitoring and operation

The main actions of plant operators consist of checking the standby condition of equipment before operation, monitoring the plant parameters (direct and relevant parameters) and identifying plant behavior during operation. In order to improve the operability of the plant, all safety and non-safety soft controls and the relevant information, such as component status and relevant parameters, are integrated onto non-safety multi-channel VDUs. The non-safety multi-channel VDUs are the primary operator interface for all plant conditions, normal and accident. To support this design basis, the Operational VDUs are classified as Important-to-Safety (similar to the Safety Parameter Display System) and they are seismically qualified. Safety VDUs provide backup HSI for failures of the non-safety multi-channel VDUs. The Safety VDUs also provide interlocks and controls to ensure the non-safety multi-channel VDUs cannot create failure conditions that would degrade the safety functions.

The basis for this multi-channel integration is as follows:

- Safety functions are monitored by multiple non-safety and safety instrumentation (e.g., narrow range - wide range, in-cores – ex-cores)
- Multiple safety and non-safety success paths exist for all critical safety functions (e.g., Charging - Safety Injection, Main Feed – Aux Feed, Sprays - Reliefs)
- Integrated safety and non-safety monitoring and control on multi-channel VDUs provides the following benefits:
  - Continuous awareness of critical safety functions while immediate focus may be plant maneuvering and power production.
  - A single operator can execute procedures that historically involve multiple operators to coordinate multiple safety divisions and non-safety systems. This simplifies task coordination for maintaining critical safety functions.

- Operators can execute computer based procedures with integrated information and manual controls (e.g., via hyperlinks).
- Minimizes operator transitions between safety and non-safety VDUs, thereby reducing operator workload during critical plant situations.

These benefits reduce operator task burden and reduce the potential for human error.

b. Automatic verification of component status

When a significant plant operating event occurs such as a plant shut down or an emergency core cooling system (ECCS) actuation in an emergency, the operator's workload and level of stress increase. This stress is caused by the simultaneous operations that need to be performed such as collecting the safety-related information, confirming plant conditions, etc. In the HSI System, the status of components such as valves and breakers and the status associated with plant trip signals, ECCS signals and isolation signals are automatically checked by comparing their status with the expected status defined in the computer archives.

c. Inter-linked screen request

Individual display screens are designed for monitoring specific plant systems or functions. All the related information required for related tasks such as alarm diagnosis, control actions, procedure execution, monitoring auxiliary functions, etc can be requested on the screen. Screens for related tasks are inter-linked in terms of the functional and/or operational relationship.

d. Use of Large Display Panel for situation awareness and information sharing

The primary purpose of the Large Display Panel (LDP) is to provide Spatially Dedicated Continuously Visible (SDCV) information to operation personnel to enhance situation awareness. The LDP helps operators maintain continuous awareness of overall plant status and critical status changes, while they are engaged in operational details on a VDU display for a specific plant system or function. The secondary purpose of the LDP is to help the operations staff coordination and communication by providing a common visualization of plant information.
The following functions are provided by the LDP so that all of operators understand overall plant conditions:

- Display of key parameters and key component status for normal operation and emergency conditions. The selection basis for the information displayed on the LDP is described below.
- Grouped alarm displays and dynamic alarm prioritization to aid operator response decisions.
- Display the computer-checked results of component status verifications which support the operator's confirmation task.
- Integration of all information in a graphic display that allows easy understanding of the plant situation and quick recognition of status changes.

e. Alarm prioritization system

A dynamic prioritized alarm system is provided to avoid information overload and facilitate plant state identification. The alarm function in the Plant Control and Monitoring System

(PCMS) compiles many simultaneous alarms and displays them on the Alarm VDUs and on the LDP, with color coordination categorized in three levels. Moreover, the priority of an individual alarm can be changed depending on the importance of additional alarms, so that when more critical/important alarms are activated, the overall plant status is easily recognized using LDP and Alarm details can be confirmed and acknowledged on the Alarm VDU. Alarms are also shown in graphic displays on the Operational VDU representing the related parameter's numerical value with red color and switch information (i.e., trip, power-off, etc.).

f. Main Control Room Staff

The above-mentioned features make it possible to operate the plant by just one Reactor Operator (RO) and one Senior Reactor Operator (SRO) in the Main Control Room (MCR) during postulated plant operating modes. This Main Control Room staffing meets the regulatory requirements of 10 CFR 50.54(m)(2)(iii). The normal MCR staff is supplemented by one additional SRO and one additional RO that will be at the plant to accommodate unexpected design conditions, such as conditions where the HSI System is degraded. This overall plant staffing meets the regulatory requirements of 10 CFR 50.54(m)(2)(i).
While the HSI System is designed to support the minimum MCR and plant staffing described above, the space and layout of the Main Control Room are designed to accommodate the foreseen maximum number of operating and temporary staff. Accommodations for additional staff are described below.

g. Applicable plant personnel

Plant personnel addressed by the HFE program include licensed control room operators as defined in 10 CFR Part 55 and the following categories of personnel defined by 10 CFR 50.120:

- non-licensed operators,
- shift supervisor,
- shift technical advisor,
- instrument and control technician,
- electrical maintenance personnel,
- mechanical maintenance personnel,
- radiological protection technician,
- chemistry technician,
- engineering support personnel.

In addition, any other plant personnel who perform tasks that are directly related to plant safety are addressed in the HFE program.

4.2 HSI System Facilities

Facilities included in the scope of the human factors engineering program are the main control room (MCR), the technical support center (TSC), the remote shutdown room, the emergency operations facility (EOF), and local control stations.

4.2.1 Main Control Room

The MCR is the place for process control and supervision in all plant situations. In addition, it provides the means for communication to others outside the plant. Finally, it is the center to initiate the maintenance of process-related equipment.
The following features are provided in the MCR:

- Within the "process control area"
  - working places for two plant operators,
- Within the "shift supervision area"
  - working place for a MCR operating crew leader,
  - working place for an additional personnel needing timely information on the process state (e.g., shift technical advisor). This can also be used as a spared work place to cope with the unavailability of one of the two work places used by the operators.
- Within the "common control area"
  - Diverse Actuation System HSI Panel (DHP) for accident mitigation and safe shutdown in case of loss of the digital I&C and HSI. This includes also the space to store and to manipulate the appropriate operating documentation and procedures;
  - LDP giving a common understanding of the plant state to the operators;
  - fire alarm board, and control board for centralised fire fighting actions in the MCR or its immediate proximity; this also includes the space to store the appropriate fire alarm sheets and procedures,
- communication board (internal, external),
- working place for temporary personnel,
- working area for reading paper based documentation,
- places for the printers and for the workstations giving access to plant or office applications,
- facilities for the storing paper-based documentation.

The computer-based HSI working places for the additional personnel that are expected at the plant during outages and commissioning are located in the computer room or the switching and tagging room.
The facilities for the shift changes are found in the common control room.
The MCR is designed to remain functional during and after earthquakes. A fire in the MCR may initially effect one division of safety or non-safety equipment. HSI in the MCR will be disabled before the fire propagates to other divisions. When the HSI in the MCR is disabled the HSI at the Remote Shutdown Station is enabled to allow safe shutdown. An accident is not postulated concurrent with a MCR fire.

4.2.2 Remote Shutdown Room

The Remote Shutdown Room (RSR) is located in a different fire zone than the MCR. The Remote Shutdown Console (RSC), which is located in the RSR has capabilities to achieve and maintain cold shutdown.
Operators can monitor and control the plant using the VDUs on the RSC to shutdown the plant, to maintain a hot shutdown condition and also transfer to maintain a cold shutdown condition. VDUs on the RSC provide the same screens as that of the main control room, this reduces the need for additional training and minimizes the potential for human error.
Fire protection and security is adequately considered in the design of the RSR and RSC. The controls on the RSC are normally disabled. They are activated by a switching device that transfers control between the main control room and the RSR. These transfer switching devices are located in separate rooms.
The HSI display design is basically the same as that of the MCR. The RSC consists of following devices:

- Operational VDUs (They also have capability of alarm display and audible signals)
- Safety VDUs

Limiting the use of the RSC for safe shutdown is entirely administratively controlled, since all HSI functions available in the MCR are also available at the RSP.

4.2.3 Technical Support Center

The onsite technical support center (TSC) provides the following functions:

- Provides plant management and technical support to plant operations personnel during emergency conditions.
- Relieves the reactor operators of peripheral monitoring and communications duties not directly related to reactor system manipulations.
- Prevents congestion in the MCR.
- Performs EOF functions for the alert emergency class, for the Site Area Emergency class and the General Emergency class until the EOF is functional.

The TSC has facilities to support the plant management and technical personnel who will be assigned there during an emergency and will be the primary onsite communications center for the plant during the emergency.
The facility consists of a plant data display system using VDUs and a LDP, data communication system, tele-communication system of telephones and facsimiles by multiple methods of transmission including private and public lines, satellite communications and adequate working area.
The TSC is located within the Auxiliary Building. The walking time from the TSC to the control room is less than 2 minutes.
The TSC working space is sized for a minimum of 25 persons, including 20 persons designated by the licensee and five NRC personnel. The minimum size of the working space provided is approximately 75 sq ft/person.
The TSC is not seismic Category I or qualified as an engineered safety feature (ESF). The well-engineered structure of the Auxiliary Building provides an adequate capability to withstand earthquakes.
The TSC ventilation system functions in a manner comparable to the control room ventilation system. The TSC ventilation system is not seismic Category I qualified, redundant,

instrumented in the control room, or automatically activated to fulfill its role. A TSC ventilation system that includes high-efficiency particulate air (HEPA) and charcoal filters is provided. The HSI display design is basically the same as that of the MCR. The TSC is consists of the following devices:

- Operational VDUs (They also have capability of alarm display and audible signals. They are used for monitoring only and no control function is provided.)
- Large Display Panels

4.2.4 Interface with Emergency Operation Facility

The Emergency Operation Facility (EOF) provides coordination and communication between on-site and off site emergency management personnel. The EOF consists of an on-site emergency center and an off site emergency operation facility and the physical space for the physical space for the USNRC Emergency Response Facility.
The EOF receives plant process data from the SPDS function of the PCMS which also provides data for the MCR, the TSC and the RSR. The PCMS provides an adequate fire-wall function to prevent cyber invasions from outside the plant.

4.2.5 Local Control

Manual controls are installed in local control stations (only manned on demand) for functions which:

- Require frequent component manipulation during local equipment maintenance that would excessively burden MCR operators. This typically applies to large components such as RHR pumps. These components also have a manual controls in the MCR. Components which have manual controls in both of the MCR and local area are controlled and managed by a tagging system.
- Require frequent process related monitoring and control actions that are not practical to automate. These manual actions would excessively burden MCR operators and these processes require no or minimal co-ordination with the MCR.
- Process related monitoring and control actions related to manual monitoring or manipulations that must be done in close proximity to the process equipment (e.g., manual batch chemical additions)

Although manual controls are not provided in the MCR for some of these functions, monitoring is provided in the MCR for all local functions.

Local controls are installed in local control stations. Local stations are equipped with either conventional HSI devices (push buttons, light indicators, etc.) or with computer and screen-based equipment. HSI device selection considers technical and economical conditions. Local controls which are credited for degraded HSI conditions in the MCR, such as MCR VDU blackout or software CCF in digital systems, operate independently of the failed HSI devices.

The local HSI is designed with consideration of the information and control needed, and the limits of the functions implemented. This includes HSI device selection as well as layout of conventional controls and/or computer screens.

4.3 Layout Design

4.3.1 Main Control Room Layout

The layout of the HSI System in the MCR is determined by the role assigned to each operator. The supervisor directs the operator in the conduct of plant operations and checks the operator's actions. Accordingly, the supervisor console is located behind the operator console. The shift technical advisor advises the supervisor on safety-relevant operations and also monitors the operator's actions. Therefore, the Shift Technical Advisor Console is located near the Supervisor Console and behind the Operator Console. The LDP provides the shared information to the operation personnel. Therefore, the LDP is located at the location where it is visible to all of the operation staff.
The distance between the Operator Console, the Supervisor Console, and the Shift Technical Advisor Console is defined considering walking passage and their ability to communicate verbally with each other over the ambient noise.
The distance between each console and the LDP and the size of the characters and symbols on the LDP are coordinated considering the visibility of the information displayed on the LDP from each console.

a. Distance between LDP and Operator Console

The LDP is located within the viewing area from each console (i.e., the Operator Console, the Supervisor Console and the Shift Technical Advisor Console). The viewing area is defined as the viewing angle with each operator seated at the console.
The LDP view from the operator console - the LDP is visible in the vertical direction and within the horizontal view of an operator sitting at the operator console.
Considering the upper limit of a view angle is not more than 20 degree for frequent and continuous monitoring on the LDP, according to NUREG-0700 rev.2, the minimum distance is approximately 14 feet (4 meters).
These values were verified by Japanese operators in a static verification and validation (V&V) process. Additional validation activities with operators at utilities in the U.S are described below.

b. Distance between Operational console and Supervisor Console/Shift Technical Advisor Console

In the main control room, each member of the operations crew (the reactor operators, the supervisor and the shift technical advisor) are on duty sitting down at their respective consoles. The distance between the Supervisor Console and the Operator Console is less than 17 feet. The distance is defined primarily by their communication capability in their seated positions under the ambient noise conditions.
The information exchange nature of the oral communications sets the minimum conditions that are acceptable.
NUREG-700 rev.2 was utilized to determine the maximum distance at which voice communication is usually possible.
The ambient noise level of the main control room used is based on the design target value of 55 dB.
A plot of possible distance to maintain a voice communication versus the ambient noise level, taken from NUREG-0700 rev.2, is shown in Figure 4.3-2.

The maximum distance at which voice communication is possible is about 17 feet (5 meter) for an ambient noise level of 55 dB. This distance is based on the fact that the operator speaks at a raised voice when executing operational duties.

c. Distance between Each Console and Large Display Panel

The distance between each console and the LDP is set considering the vertical and horizontal viewing field of the operator, and the visibility of information displayed on the LDP.

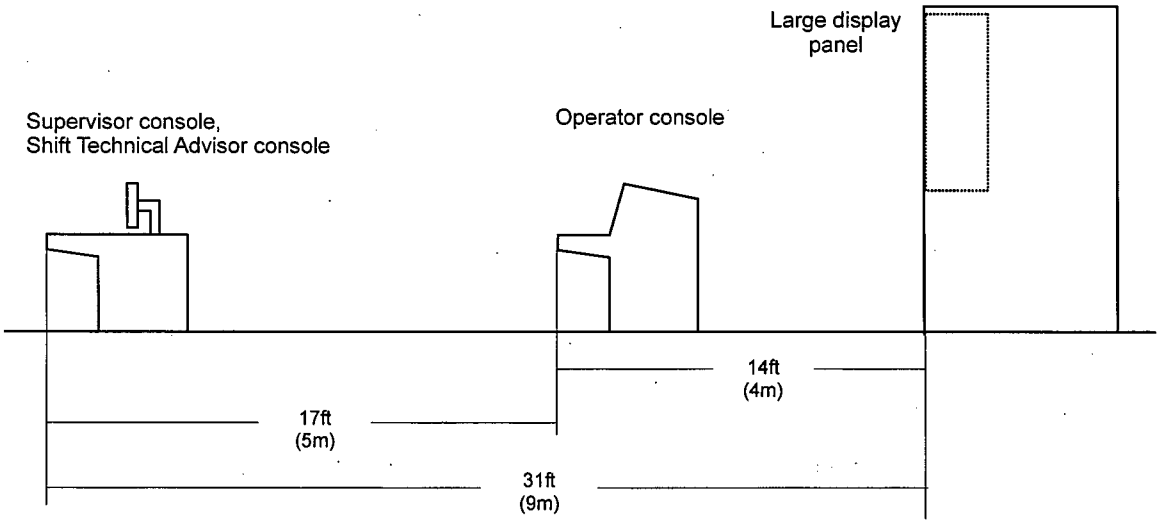


Figure 4.3-1 Distance between Each Console and Large Display Panel

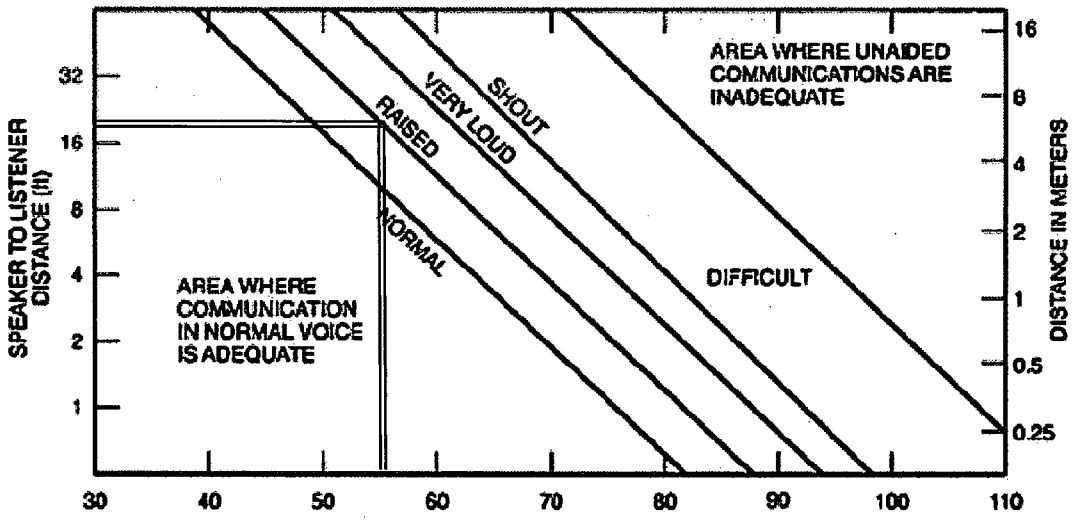


Figure 4.3-2 Voice Level as a Function of Distance and Ambient Noise Level

Figure 4.3-3 shows the typical layout of the main control room. Major HSI equipment in the main control room and other locations relevant to the control of plant operations are presented in Table 4.3-1.

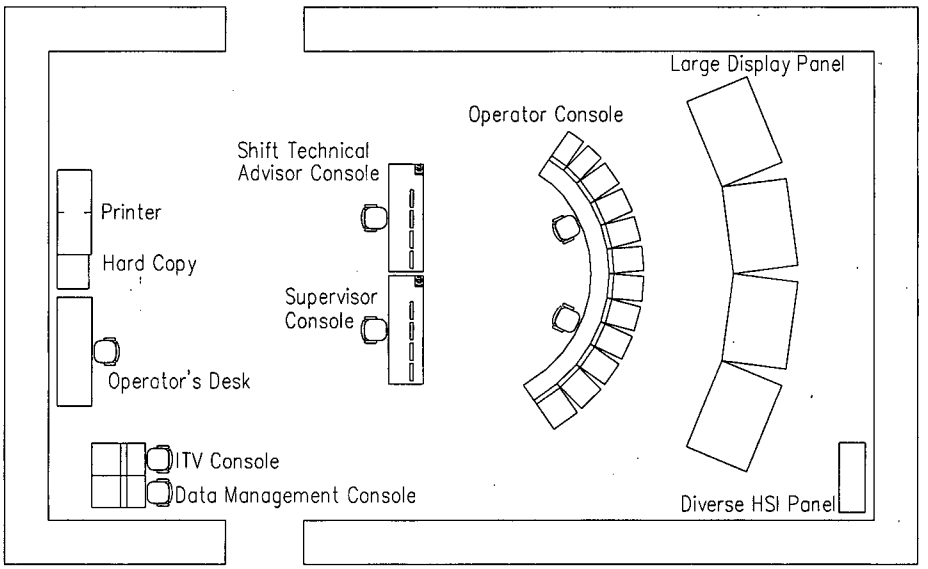


Figure 4.3-3 Typical Layout of the US-APWR Main Control Room

Table 4.3-1 Typical HSI Equipment at Various Locations

Place	Equipment	Function
MCR	Operator Console	Plant operation for any situation of the plant (incl. startup/shutdown, emergency). Can accommodate one or two operators.
	Large Display Panel	Plant status display shared by all the operators in MCR
	Diverse HSI Panel	Conventional switches and indicators for safety operation (for backup in the event of common cause failure)
	Supervisor Console	Plant monitoring by MCR supervisor (monitoring only, no operation)
	Shift Technical Advisor Console	Plant monitoring by Shift Technical Advisor (monitoring only, no operation)
	Data Management Console (DMC)	Data management and reporting from HSI system computers
	ITV Console	Industrial Television console for monitoring local area, spent-fuel pit, etc,
RSR	Remote Shutdown Console	Remote shutdown operation when MCR is not available
TSC	TSC Computer	Plant management and technical support to the reactor operating personnel located in the control room during emergency conditions
EOF	EOF Computer	Management of overall licensee emergency response (including coordination with Federal, State, and local officials), etc.

4.3.2 Operator Console Layout

The arrangement of the equipment at the operator console, supervisor console, Shift Technical Advisor Console and large display unit panel desk areas are illustrated in Figure 4.3-4, 5 and 6.
The shape, dimensions and arrangement of each console meet ergonomic design standards. Hard-wired device selection principles are as follows:

- System level operation switches to be used by operators in the event of an emergency are based on the standards and guidelines (IEEE-603-1991) related to safety systems. Means are provided in the MCR for manual initiation of protective functions at the system level:
  - Reactor trip
  - Actuation of ECCS
  - Containment vessel (CV) isolation phase A
  - Main steam flow isolation
  - Emergency feedwater flow isolation
  - Actuation of emergency feedwater flow
  - Actuation of containment vessel spray and containment vessel isolation phase B
  - Main control room heating, ventilation, and air conditioning (HVAC) isolation
  - Charging water flow isolation

  Note: these are the examples at present state of design and the changes are defined in the Plant Licensing Documentation (e.g., DCD)
- Above functions are realized by conventional hard-wired Class 1E module switches that permit easy and prompt access by the operator.

- The bypass or inoperable state of reactor protection system (RPS) and engineering safety feature actuation system (ESFAS) are displayed on the LDP as SDCV information.

- Means for monitoring and control of safety and non-safety systems at the system and/or component level are realized by the Operational VDUs. Safety VDUs also provide monitoring and component level control for safety functions and satisfy Class 1E requirements.

- Indicators, lamps and switches required for diverse backup as a countermeasure against software common cause failures are provided on a conventional control panel which is independent from the consoles.

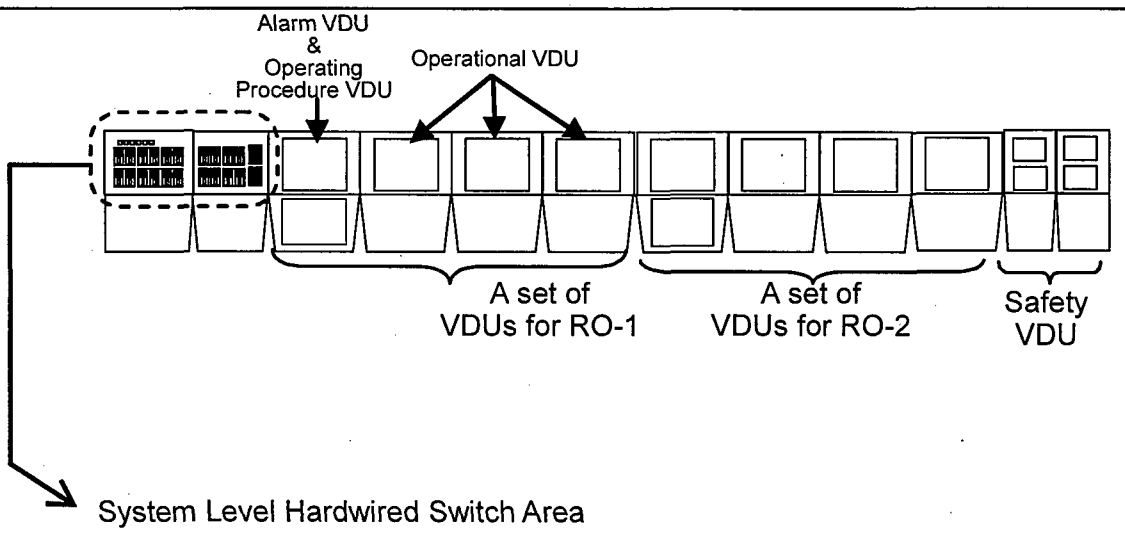


Figure 4.3-4 Equipments Arrangement of Operator Console

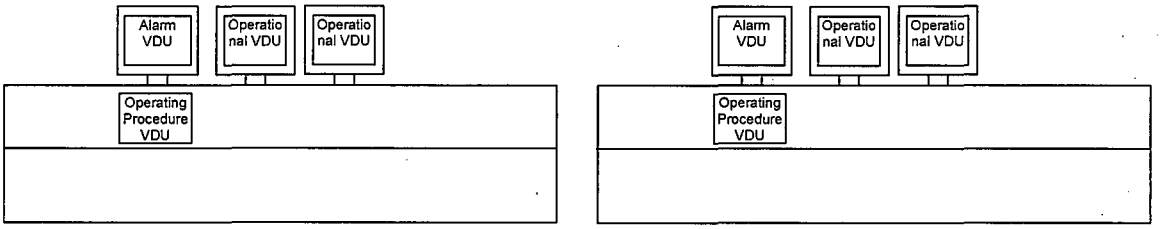


Figure 4.3-5 Equipments Arrangement of Supervisor Console and Shift Technical Advisor Console

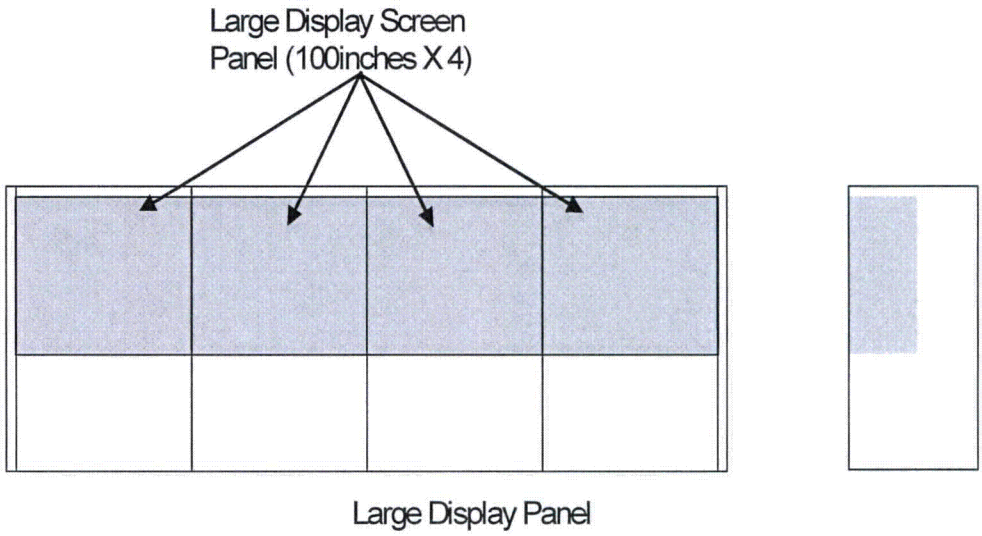


Figure 4.3-6 Screen Arrangement of Large Display Panel

4.4 Display Overview and Navigation

4.4.1 Display Overview

The following types of VDUs are installed in the operator console, the supervisor console and the technical advisor's console. The main purpose of the each VDU is summarized in Table 4.4-1.

Table 4.4-1 Main Purpose of VDUs

Item	Main Purpose
Operational VDU	To execute all of the plant control and monitoring functions, including control of the safety systems.
Safety VDU	To execute the safety-related control and monitoring functions as a backup for the Operational VDU. It can control operation signals from the Operational VDU.
Alarm VDU	To acknowledge and display individual alarms using prioritization color codes. Alarm VDU also provides the alarm confirmation/non-confirmation information to the operator.
Operating procedure VDU	To provide computer-based operation procedure displays near the Operational VDU and the Alarm VDU in order to facilitate and simplify the performance of operation procedure.

The group of Operational VDU display formats also provides the safety parameter display system (SPDS) functions.
Each VDU display design and function is explained in the following sections. (See section 4.5, 4.6. 4.7 and 4.8)

4.4.2 Display Navigation System

To make access to each display easy and simple, a navigation system has been developed for each VDU.

a. Operational VDU

There are multiple paths of calling up displays in the operational VDU. Figure 4.4-1 illustrates the navigation system for calling up the displays.

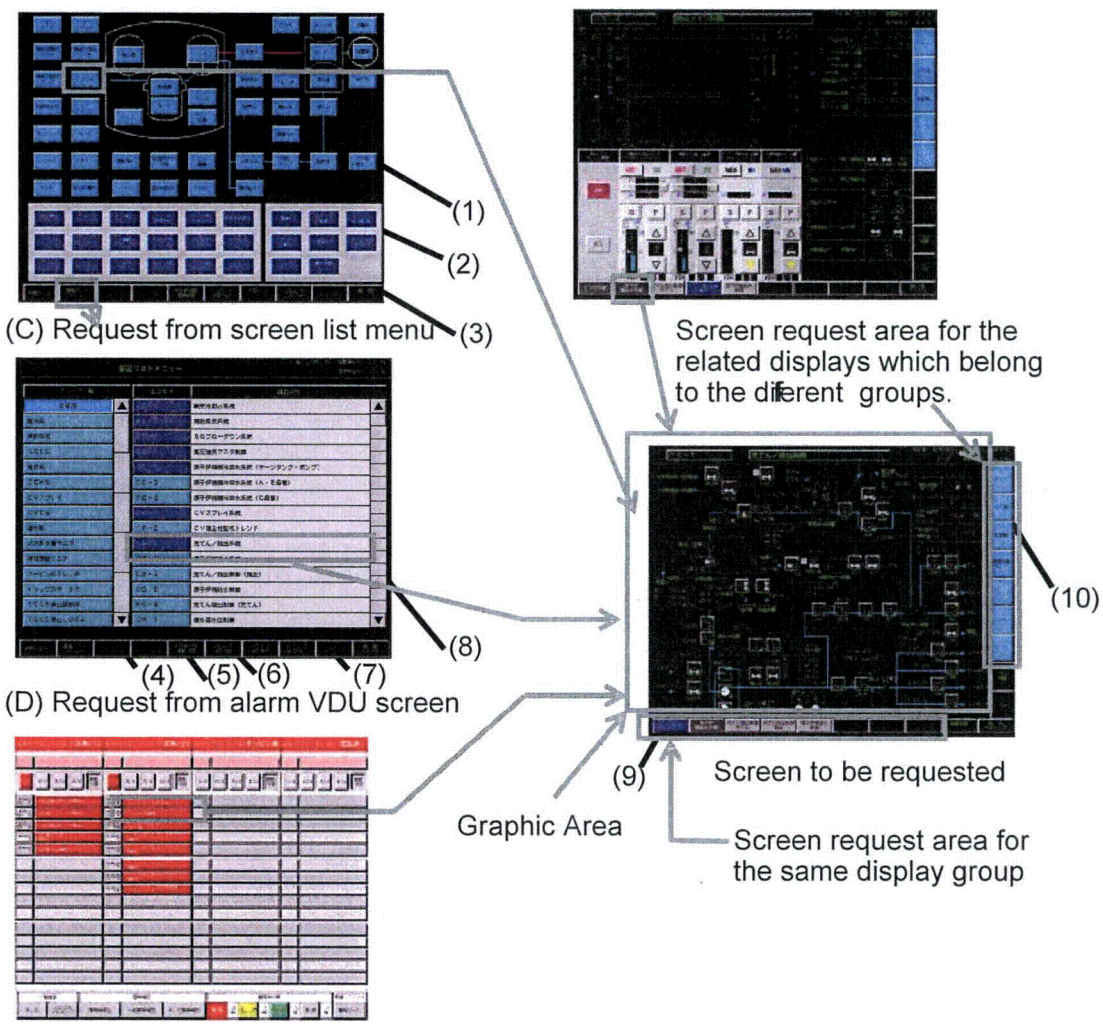
The top navigation display (item (A) in the figure) is commonly used for navigating the operational VDU display information. Using the top navigation display, any operational displays can be selected within two display selection steps. This is based on the following display navigation design:

- All operational displays are grouped system by system by a number. The number is defined by the assignment capacity for the same group display request area (the bottom area in the operational VDU screen).

- The representative display (the system display is normally chosen) is selected directly from the top navigation display.
- The other operational displays are selected from the representative display using the same group display request function located on the bottom area of each operational VDU displays.

In addition, a related display which belongs to another system can be selected directly from each operational VDU screen.

Any operational displays can be also requested from a screen list menu display. (item (2) in the figure)
The screen list menu display can be selected from the top navigation display.
The related operational display can be also selected from the Alarm VDUs. (See section 4.8.3)



Note: See table 4.4-2 for specifications of operational VDU navigation icons, (1)-(10).
See table 4.4-3 for specifications of Alarm VDU icons.

Figure 4.4-1 Screen Request Methods for Operational VDU

Table 4.4-2 Specifications of Operational VDU icons

No	Type	Color/icon Color/letter	Shape	Function
(1)	System display request area	Light blue Black	Rectangle	Top menu of system or component displays grouped by each system (e.g., CVCS,PZR)
(2)	Emergency display request area	Blue White	Rectangle	Directly screen selectable area concerning emergency related screens. (e.g., TRIP STATUS, ECCS VALVE STATUS)
(3)	Function menu area	Black Green	Rectangle	Generic display selection function (e.g., change the screen list menu, move to the previous screen)
(4)	Group list	Same as (1)(2)	Rectangle	Group names are listed here. Grouping is equal to (1)(2).
(5)	Scroll bar	Light gray	Rectangle	Scroll bar to select (4).
(6)	Screen number	Same as (1)(2)	Rectangle	Screen number of each screen. (e.g., CS-1 for CVCS screen-1)
(7)	Screen name	Light gray Black	Rectangle	Individual screen names are listed here.
(8)	Scroll bar	Light gray	Rectangle	Scroll bar to select (6)(7).
9)	Screen request area (same group)	Light gray Black	Rectangle	Select screens included in the same group from the current screen.
(10)	Screen request area (other group)	Light blue Black	Rectangle	Select screens not included in the same group from the current screen.

b. Safety VDU

The safety VDU also has navigation displays. (See Figure 4.4-2) The top navigation displays are divided between operation and monitoring, respectively but they are hyper-linked by a navigation support toolbar which is located and continuously visible on the left side of the each display, in each top navigation displays, the hyper-link buttons are assigned system by system. The navigation system also has a hierarchical structure but enables simple and easy display access avoiding a deep hierarchy and adopting a navigation support tool.

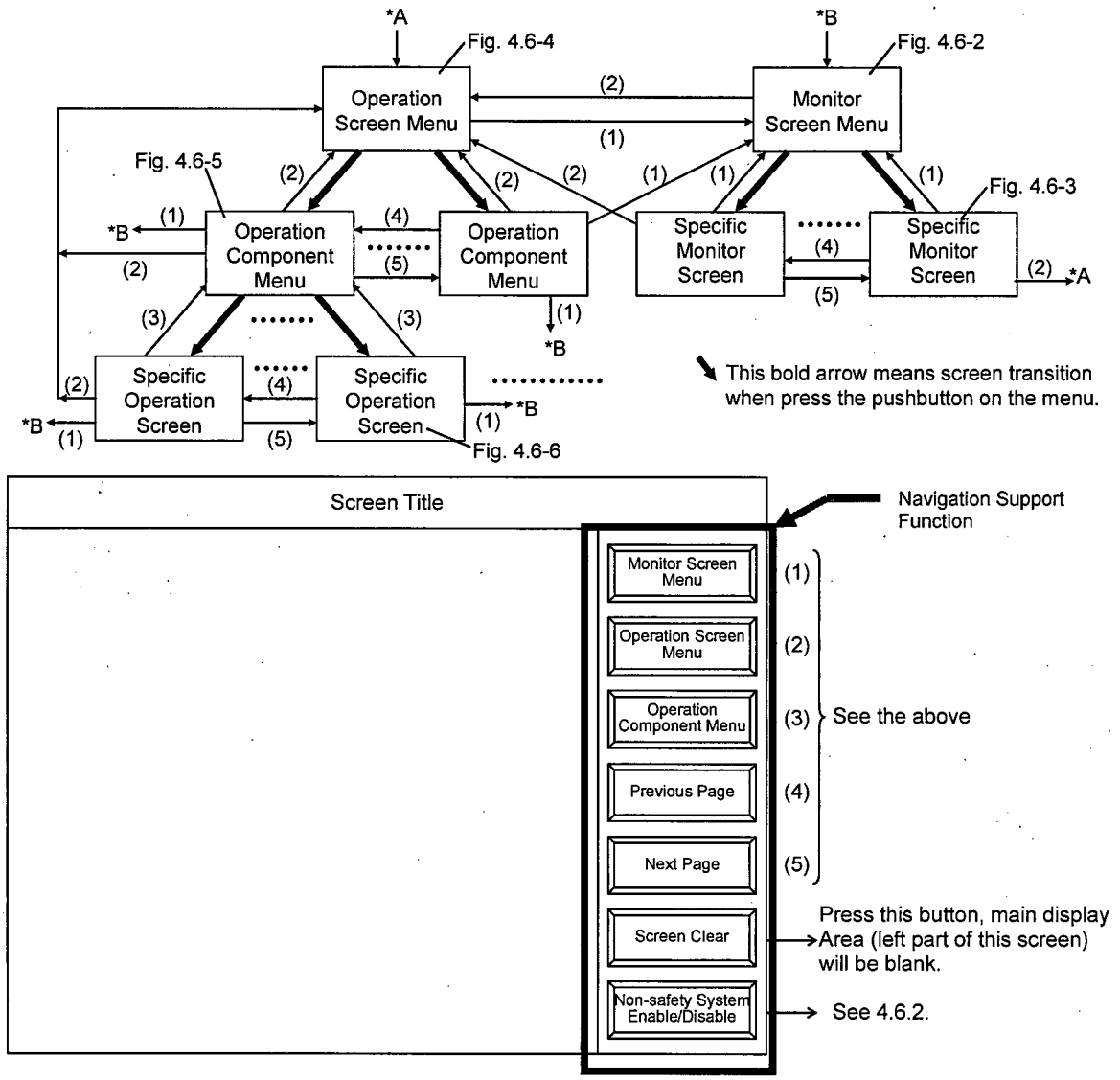
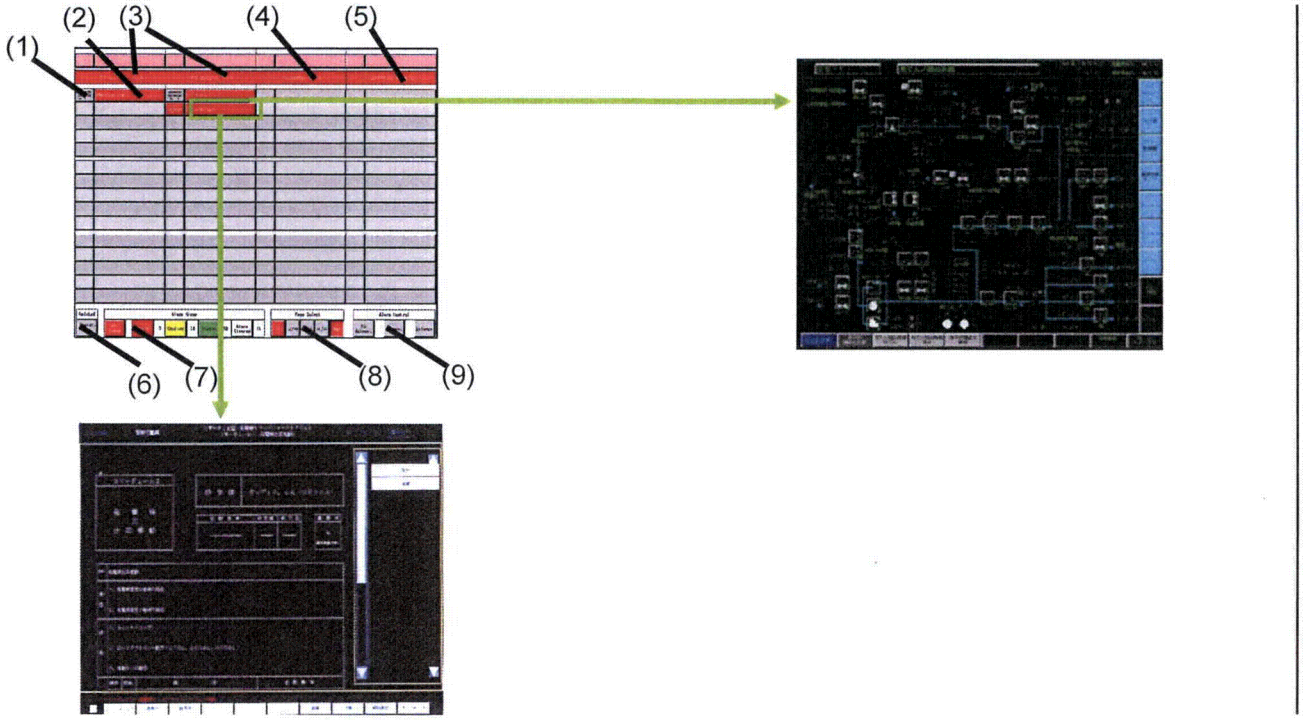


Figure 4.4-2 Screen Request Methods (Safety VDU)

c. Alarm display navigation

When an alarm message displayed on the alarm VDU screen is touched or clicked, the related display can be selected on the operational VDU near the Alarm VDU.
Or the alarm response procedure (Alarm Response Procedure (ARP); one of the plant operating procedures) can also be selected by touching or clicking the alarm message on the Alarm VDU display.



Note: See table 4.4-3 for specifications of alarm VDU navigation icons, (1)-(9). Also see Figure 4.7-1 for larger image of alarm VDU.

Figure 4.4-3 Screen Request Methods (Alarm VDU)

Table 4.4-3 Specifications of Alarm VDU icons

No.	Type	Color/icon Color/letter (Normal mode)	Color/icon Color/letter (Alarm mode)	Shape	Function
(1)	Support information	-	Light gray Black	Rectangle	Date & time when alarms occurs and Static Priority are displayed
(2)	Alarm name	Light gray Black	R/Y/G W/Bk/Bk	Rectangle	Alarm name is displayed in red, yellow or green by dynamic priority system.
(3)	Primary system area	Red White	Red White	Rectangle	Primary system alarms are displayed here.
(4)	Secondary system area	Red White	Red White	Rectangle	Secondary system alarms are displayed here.
(5)	Electrical system area	Red White	Red White	Rectangle	Electrical and transmission system alarms are displayed here.
(6)	Select screen mode	Light gray Black	Light gray Black	Rectangle	Alternative mode switches or select request screen (Operational VDU display or ARP) when touched or clicked an alarm name.
(7)	Alarm group	R/Y/G/W W/Bk/Bk/Bk	R/Y/G/W W/Bk/Bk/Bk	Rectangle	Total number of alarms (red), caution (yellow) status (green) and cleared alarms (white).
(8)	Page select	Light gray Black	Red White	Rectangle	Page selects in case that numbers of alarms in a page overflow.
(9)	Alarm control	Light gray Black	Light gray Black	Rectangle	First out Acknowledge area, Acknowledge area, and Silence area. Touching or clicking "Acknowledge", flicker stops and sound stops. Touching or clicking "Silence", buzzer stops.

Note: R: Red Y: Yellow G: Green W: White Bk: Black

d. Operating procedure display navigation

On the operating procedure display, related operation display names/numbers are displayed with procedures. In addition, the related operational display is selected on the Operational VDU near the operating procedure VDU by touching or clicking the display request area on the operating procedure VDU display.

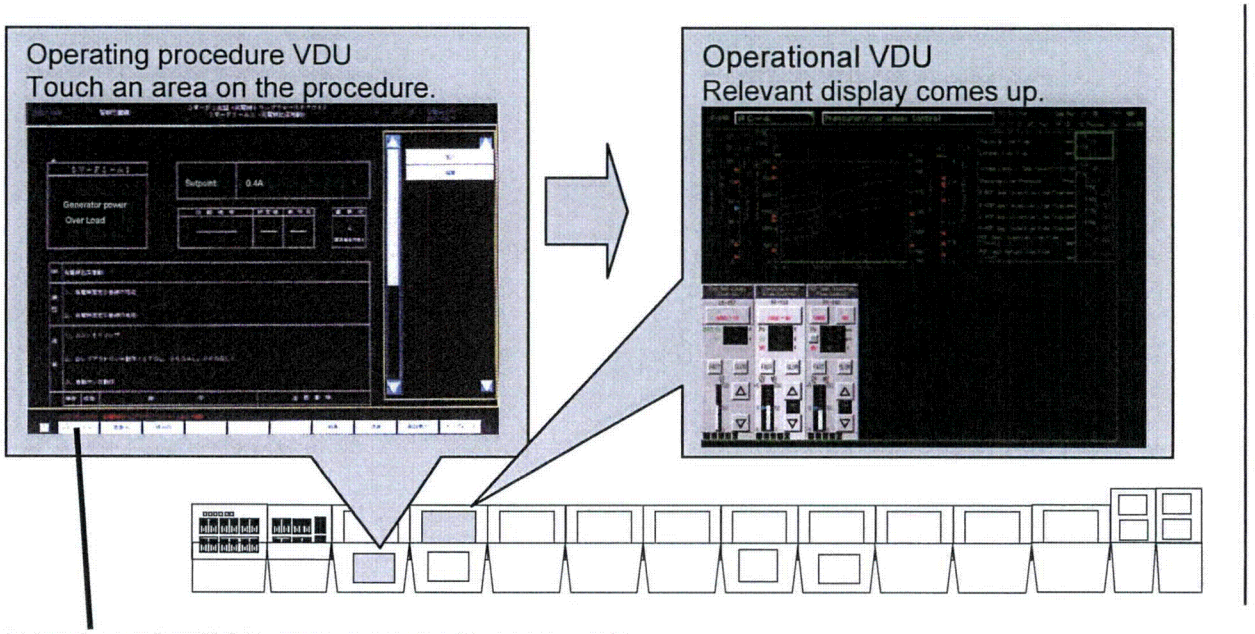


Figure 4.4-4 Screen Request Methods （Operating procedure VDU)

4.5 Operational VDU Display Design

4.5.1 Operation Devices

The Operational VDU has the following features:

- The display offers easy monitoring, taking into consideration the guidance in NUREG-0700 Rev.2, Sections 1.5.1 and 1.5.2.
- The size of the display on the Operational VDU is approximately 19 inches, which takes into account the quantity of displayed information and the size of displayed symbols and characters.
- The display is of the flat type, which makes it easy to hit the target area and minimizes glare.

4.5.2 Operation Method

This section describes the soft operation methods used in the screen-based main control board.
Soft operations are performed by requesting a system on the diagram screen and then touching or clicking an operation area of a soft switch displayed on the screen.

a. Calling Up Switches

- ON/OFF Switches;
  On the Operational VDU, by touching or clicking the symbol of the device on a system flow diagram, the ON/OFF switch pops up on the screen. There is only one switch popup on the screen at any one time in order to avoid erroneous operation. The default popped up position is consistent (right-lower side) and if the related information is hidden by the popup window, the default popup position is automatically set in the other corner of the screen. The popup window can be moved by the operator in the unusually case that other information relevant to the operation may be hidden.

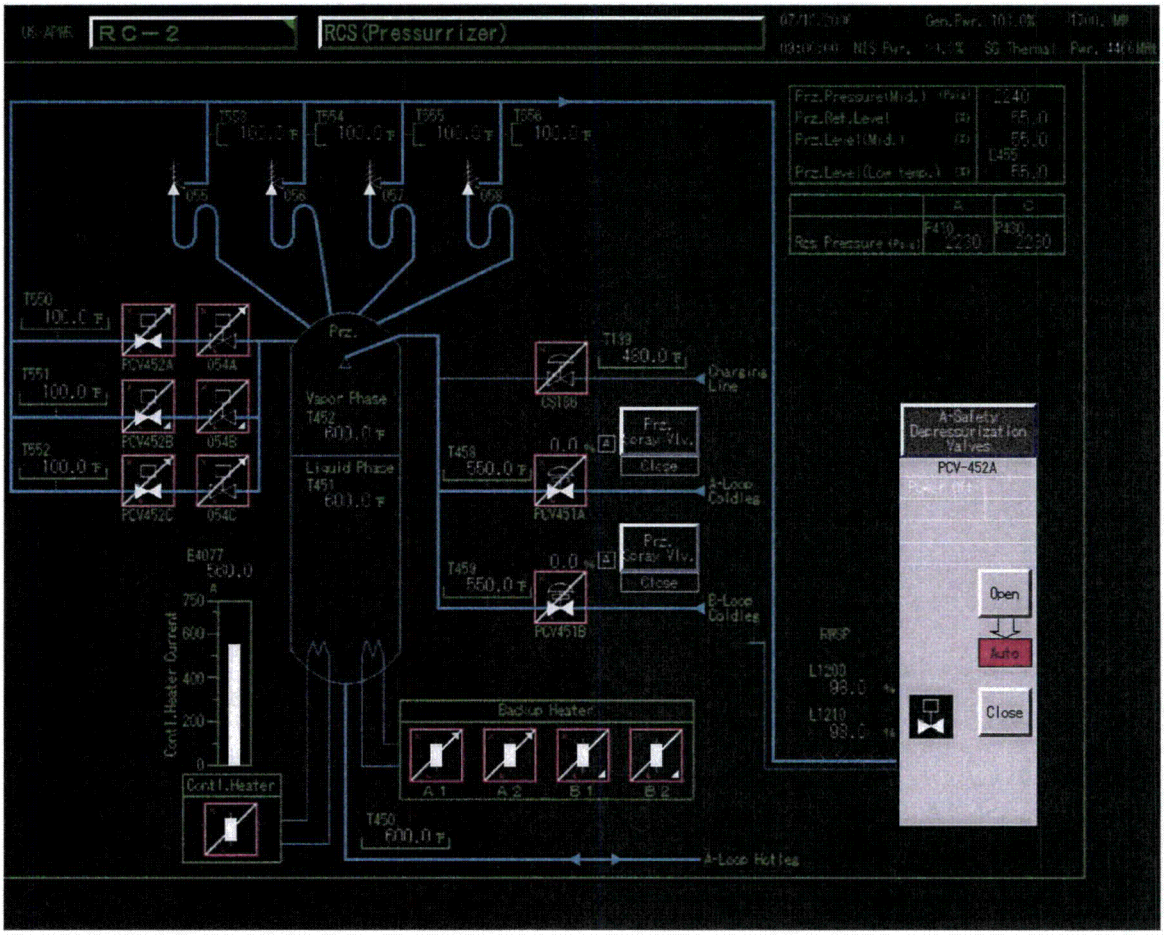


Figure 4.5-1 Example of ON/OFF Switch Popup

b. Controller and Mode Selector

In general, controllers and mode selectors are only available in fixed positions on a Controller screen that displays trend graphs and related parameters, since controlled processes require monitoring of their changing trends.
However, some controllers which are used in a manner similar to ON-OFF switches are available on the system display because they are operable without the need to see a trend. Controllers have a setpoint adjustment function and a manual demand adjustment function. These types of continuous control functions are usually difficult to utilize due to the digital system processing delay. However, in the MHI HSI System these functions are easily used based on the following methods. (See also Section 4.5-3 b.)

- **Target point indicator:** To avoid the stress, confusion and overshoot often caused by typical manual demand feedback indication delay, the HSI System accepts the demand signal, displays the target point in the manual value bar immediately (within one second) and sends the target value to the controller. A discrepancy between the demanded value and the value in the controller is easily seen by the operator.(See Figure 4.5-7)

- **Adopting a slow speed adjustment mode:** In addition to conventional adjustment mode (Normal/Fast), a slow speed mode is applied in order to modulate the setpoint correctly with the expected digital signal delay environment.
- **Adopting the soft numeric keypad for setting the setpoint:** In addition to control setpoint adjustment utilizing increasing/decreasing buttons, the setpoint can be directly input using the numeric keypad function. The HSI System then sends the target setpoint value to the controller. A discrepancy between the demanded value and the value in the controller is easily seen by the operator on controller screen. (See Figure 4.5-2 and Figure 4.5-7)
- **Auto/Manual Transfer:** A bumpless bidirectional auto/manual transfer function is installed in the controller to avoid the instability resulting from an auto/manual transition.

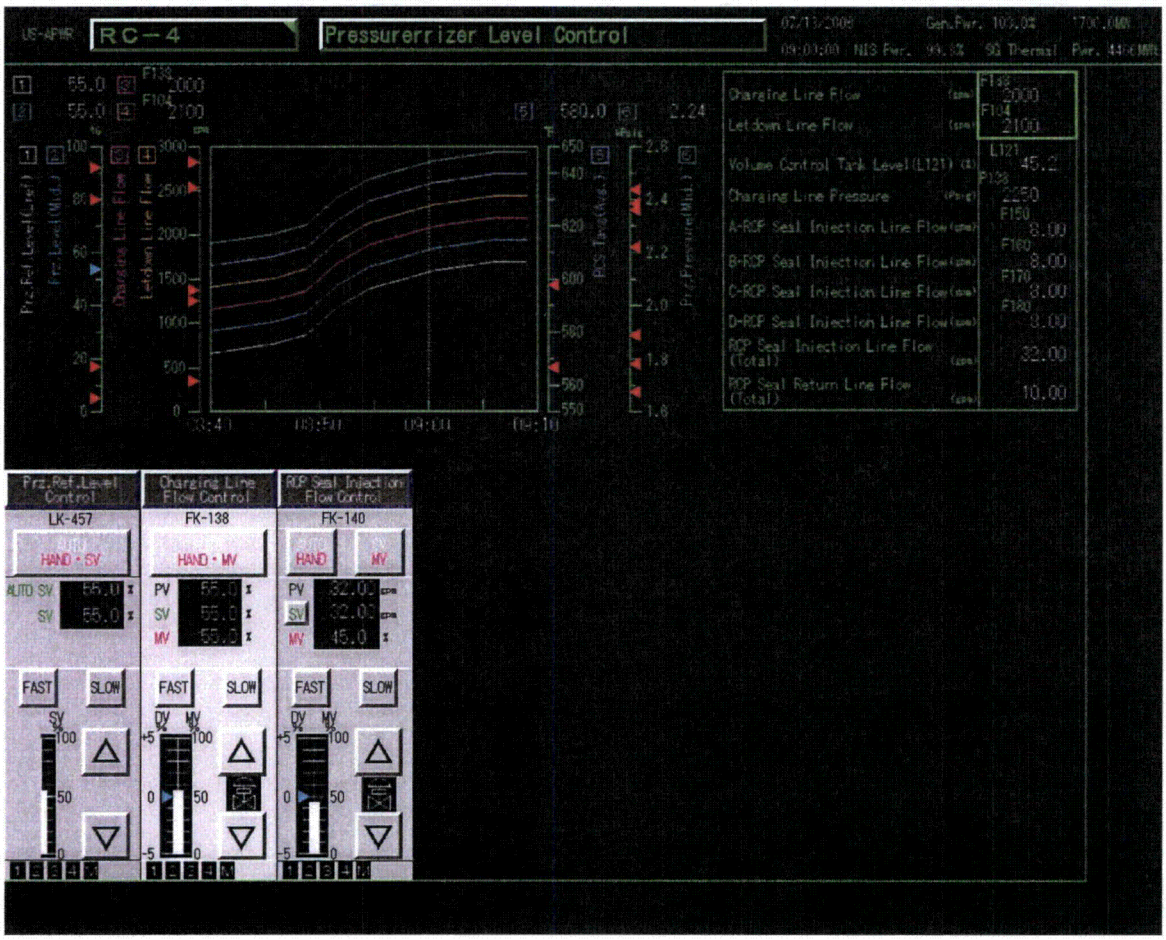


Figure 4.5-2 Example of Controller Screen

c. Displaying Screens Related to Soft Operations

•Identifying soft Operation Areas

All soft operation areas on the screen appear as convex buttons, allowing operators to distinguish operable components/valves (components/valves which respond to touch or click) from non-operable devices. All soft operation buttons are used for the soft switches and the

soft controllers. The select buttons for the soft switches and the soft controllers are located in a graphic area which is distinguished by the display select area. (See Figure 4.4-1)

•Soft Operation Feedback

Soft operation areas appear concave when continually pressed (during input), thereby providing local feedback indicating touch or click input acceptance. Controller feedback related to operation process is indicated by the color of the background on the soft operation area.

4.5.3 Switch Features

a. ON/OFF Switches Operation Related Information Display Feature

Operation related information messages which correspond to lamp information in conventional switches (e.g., control power status, operation availability status, etc.) are displayed using software switches. In addition, these messages can be viewed and acknowledged on system flow diagram screens without requiring the operator to request the control switch display. Component/valve status is also displayed on the soft switch using contact signals (result signals) from component status feedback.
A Switch software cover is an HSI interlock function which requires double action for executing the operation in order to avoid erroneous manipulation. Whenever the soft switch pops up, it is inoperable until the cover is unlocked by touching or clicking on the switch name area.

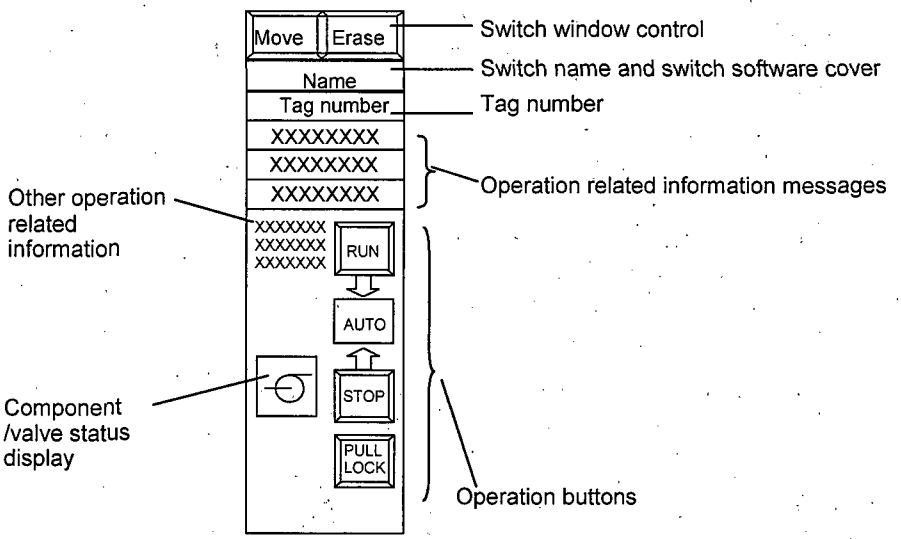


Figure 4.5-3 Example of ON/OFF Switch

Other Operation Related Information Display Features are follows:

- On the Other Operation Related Information Display Area, the following information is displayed;
    - Safety system interlock signal name: The safety system interlock signal name, such as ECCS signal, isolation signals, etc. is displayed for components that are

automatically actuated by safety system signals. The display shows the dynamic active safety signal name physically and statically.

- Inching:
  "Inching" appears on switches, allowing operators to distinguish inching valves from ON/OFF valves. "Inching" corresponds to valves that have throttling or bumping capability.
- Fail position : "FO"(Fail to Open), "FC"(Fail to Close)
- Lock status : "LO"(Locked Open), "LC"(Locked Closed); which means the valve status is mechanically locked (Full Open or Full Close) by a local gear chain, etc.,

- Soft Operation Switch Moving Feature:
  The function allows operators to move the position of the popup window to the four corners of screen in the unusual case that the necessary information was covered by a switch popup display. Touching or clicking the function, the soft switch moves to each successive corner of the screen. (See Figure 4.5-4)

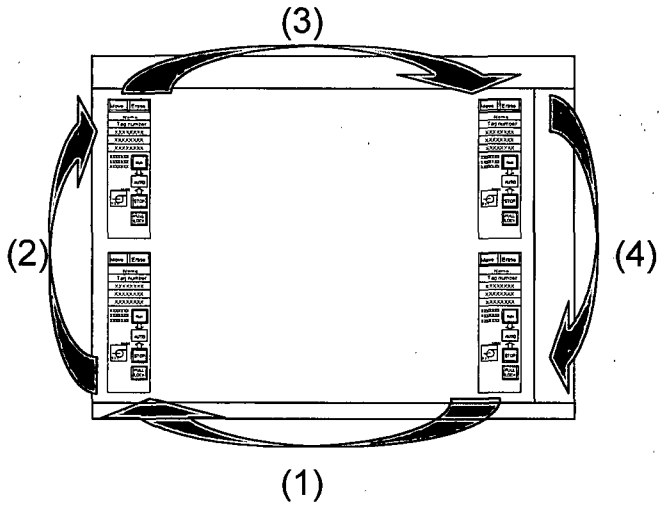


Figure 4.5-4 Soft Operation Switch Moving Feature

- Soft Operation Switch Clearing Feature;

  This function enables the soft switch to be cleared on the screen. The soft switch is also cleared when another soft switch is selected on the screen.

- Tagging Feature:
  For maintenance related work order management, operators are able to attach and remove

tags by soft operations and the system is able to indicate the tag status by the addition of checkmarks on the applicable component/valve symbol both on the soft operation switch popup window and on the switch selection button on the Operational VDU screen. The tag type is identifiable by the color of the checkmark. Detailed tag information is displayed in a dedicated popup window. The dedicated popup window is popped up with the soft operation switch popup window touching or clicking the switch selection button.
Tagging is an administrative status function that has no effect on the operability of the component.

The tagging system provides soft electronic tags for the HSI system and physical tags for plant components. The electronic tag ID for the HSI system and the physical tag ID for plant components are identical for each component. Electronic tags are implemented within the HSI system and physical tags are attached at each component in local areas of the plant.

The tagging sequence is as follows:

1) Isolation and tagging data (electronic tags) and physical tags are prepared by the maintenance/operations crew.
2) Electronic tag data is manually uploaded to the HSI system and available to be set on tagging on the dedicated tag popup window. This status shows the icon of the component with a dotted line marked.
3) After setting on tagging on the tag popup window, the status change shows the icon of the component with a line.
4) At certain stages of maintenance, the maintenance/operations crew touches the icon and popup the dedicated tag window for changing the tag status. Another tag status change shows a line color of the icon of the effective component. The tag status is updated appropriately for various stages of maintenance. At the local area, the physical tags are attached at components to indicate their maintenance mode.
5) After the maintenance is complete, the maintenance/operations crew touches the "Remove" icon on the tag popup window, and then the component icon is unmarked on the system displays. At the local area, the physical tags are removed.

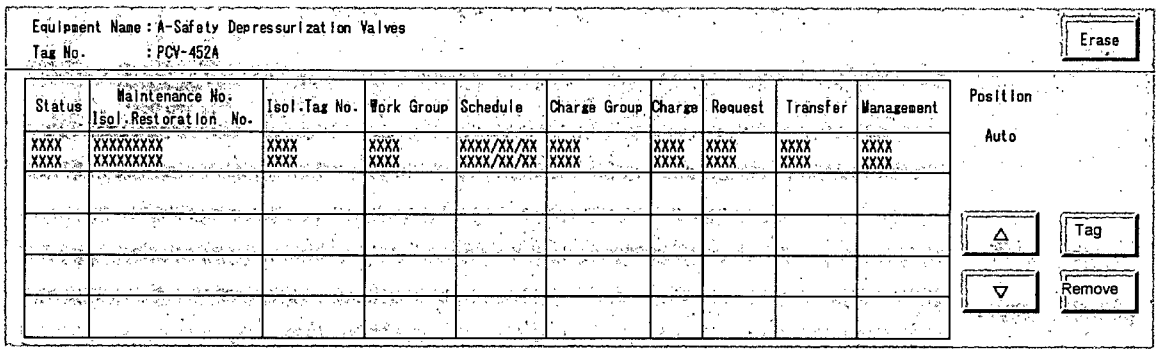


Figure 4.5-5 Tag Popup Window

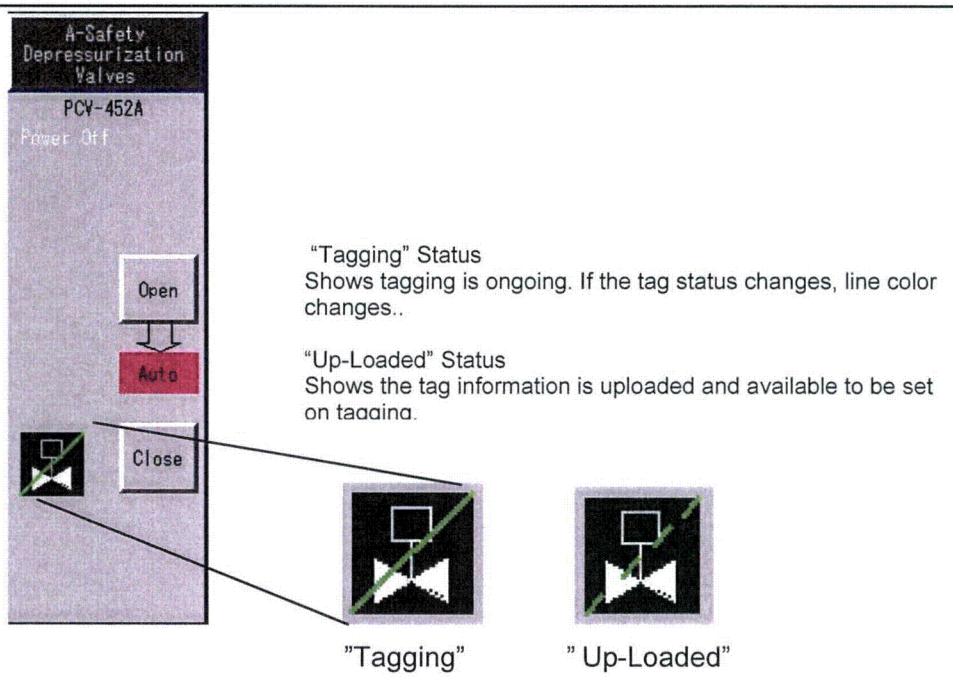


Figure 4.5-6 Example of Tag Status Display

System screens display component status, the component's acronym name/tag name, representative operation Information messages and tagging information respectively.

b. Manual Operation of controller Information Display Feature

Manual Operation of a controller has the following features;

- The controller is provided with an AUTO/MANUAL button, an INC/DEC button to input MV (Manipulated value) and SV (Setpoint value), a slow/normal/fast mode button and an SV value direct digital value feature.
- Target Parameter Display Feature:
  This feature displays PV (Process value), SV, and MV in digital values.
- Normal/Fast/Slow Mode Selection Feature:
  The Normal and Fast mode increase/decrease rates are comparable to that of conventional HSI devices.
  To accommodate software operation based fine-tuning, the controller is provided with slow mode in addition to the above two modes, offering 1/10th the increase/decrease rate of normal mode. "Fast" and "Slow" modes are selected by touching or clicking the "Fast" and "Slow" button respectively. The Normal mode is selected by selecting neither the "Fast" mode nor the "Slow" mode. The "Fast" and "Slow" mode return by touching or clicking the "Fast" and "Slow" button again.
- Target point indicator Feature:
  To avoid MV indication delay from the controller, the HSI System displays the operation demand immediately (within one second)

On the system display, control valve status is represented with the position limit, tag name. The representative operation Information messages are also displayed.

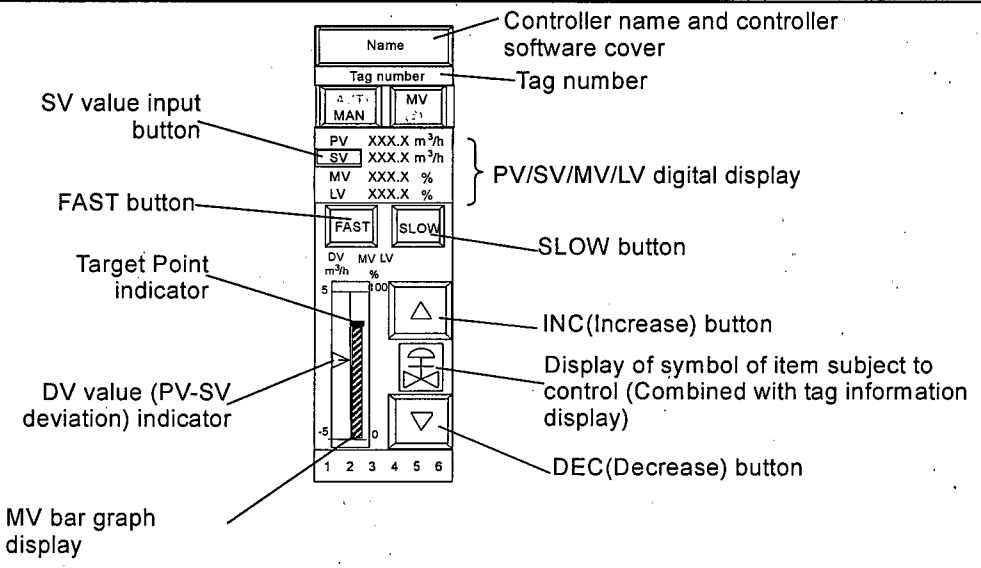


Figure 4.5-7 Example of Controller

c. Provisions to Prevent Erroneous Operation

Provisions to prevent the erroneous operation of switches and controllers are as follows:

- Soft operation switch (including soft operation touch area) dimensions, shape, identification method, arrangement are established based on ergonomic design standards.
- A software cover (a feature which blocks miss-touch input) is provided for all touch operation switches and controllers. The switch is operable when the software cover is removed by touching or clicking the name area of the switch. It is also inoperable by touching or clicking the name area again.
- The operation method and function of conventional switches and controllers are covered and integrated on the soft switch. The feature and function of all switches and controllers are made consistent.
- In cascaded controller (i.e., pressurizer pressure control and boron concentration control, etc.,), operators can adjust the target value using the master controller which makes each subcontroller's target accommodated to the main target automatically. The accommodated target value created by the master controller is automatically set on the subcontroller at the auto mode and displayed as an auto-MV indicator value.

4.6 Safety VDU Display Design

4.6.1 Operable Devices

The Safety VDU has the following features:

- The display allows easy monitoring, taking into consideration the guidance in NUREG-0700 Rev. 2, Sections 1.5.1 and 1.5.2.
- The size of the display on the Safety VDU is approximately 10 inches.
- The display is of a flat type, which makes it easy to hit the target area and minimizes glare.

The Safety VDU is used when the Operational VDUs are unavailable. All safety related switches displayed in the Safety VDU are also shown in the Operational VDU display. Therefore, during normal operations, monitoring screens that indicate Type A and B post accident monitoring (PAM) parameters are continuously displayed on the Safety VDUs.

4.6.2 Operational VDUs Connect/Disconnect

Figure 4.6-1 Screen Transition of Request Area

4.6.3 Monitor Screen

Figure 4.6-2 shows the menu on the monitor screen. Figure 4.6-3 shows an example of a specific monitor screen. When the number of monitored parameters in the system is less than 16, the remaining area of the screen remains blank.

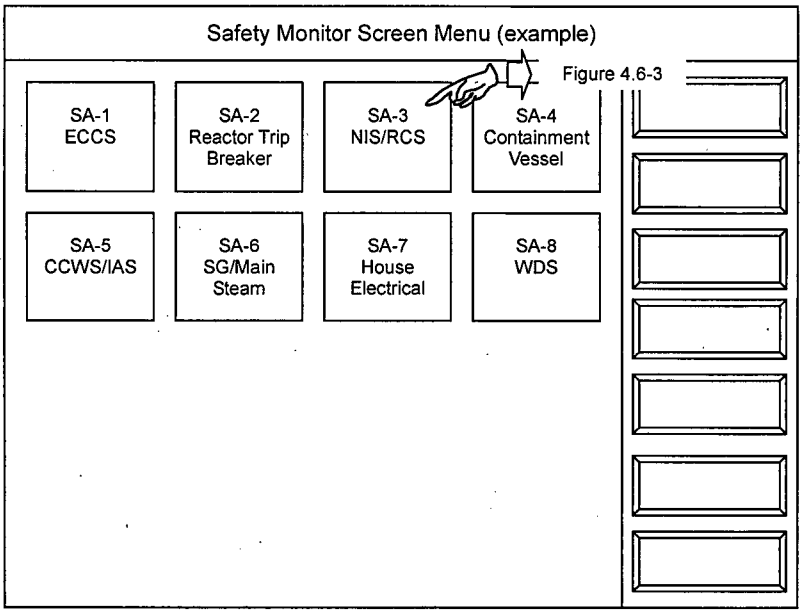


Figure 4.6-2 Monitor Screen Menu

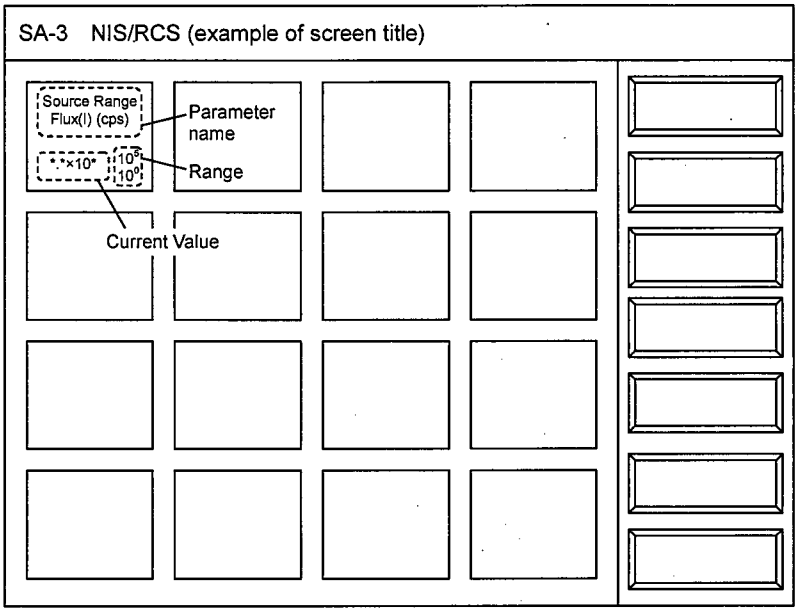


Figure 4.6-3 Example of Specific Monitor Screen

c. Operation Screen

Figure 4.6-4 shows the menu of the safety operations screen. Figure 4.6-5 shows the operation component menu of a specific system. When the number of operational components in the system is less than 20, the remaining area in the screen will remain blank. When the operational components in the system are more than 20, the components over 20 will be presented on the next page.
Figure 4.6-6 shows an example of specific operation screen. From this screen, the operator controls the target component. The feature representation of the switch shown on both of the safety VDU and the non-Safety VDU (the Operational VDU) is the same.

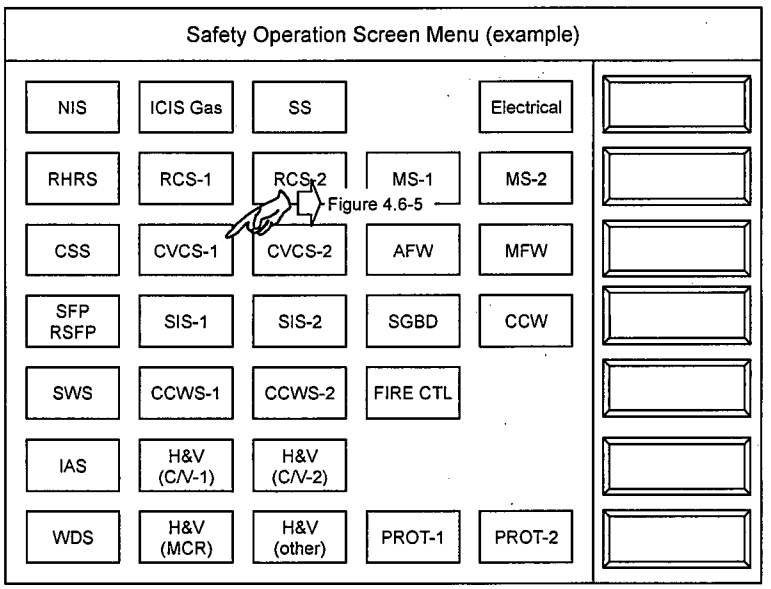


Figure 4.6-4 Operation Screen Menu

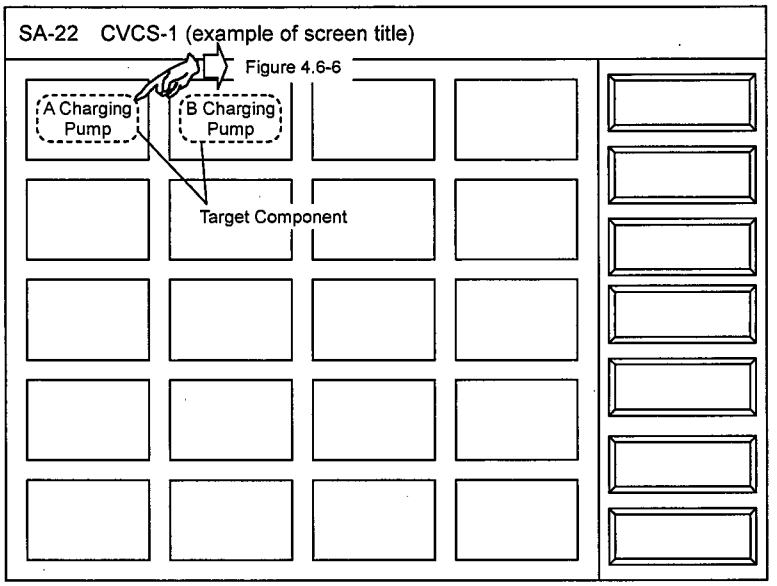


Figure 4.6-5 Operation Component Menu

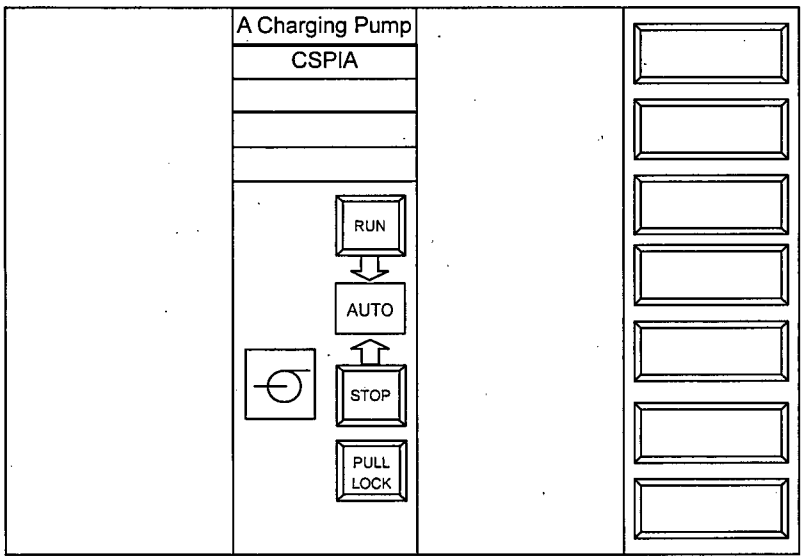


Figure 4.6-6 Example of Specific Operation Screen

4.7 Alarm System

The alarm system provides all information necessary for detecting abnormal plant conditions. The alarm system ensures that the operator can easily recognize the fault conditions even when the number of fault conditions or the severity of the faults are increasing.

The main features of the alarm system are as follows:

- adequate information presentation that allows the operator to acknowledge and recognize alarm information and take appropriate corrective actions
- establishment of an alarm prioritization system that allows the operator to identify the relevant and important alarm information and not to deal with "alarm avalanche".
- Implementation of a navigation system display that provides easy access from the alarm display to the relevant system display and the alarm response procedures.

These functions help the operator to identify and diagnose the transient condition causing the alarms and complete the necessary corrective actions.

4.7.1 Alarm Display System

a. Display Location

All alarm information is displayed on the alarm VDU, LDP and the Operational VDU respectively.

On the alarm VDU, all alarms are categorized into four system categories (i.e., two primary systems, a turbine system and an electrical system). Alarms are recorded in each category display area in chronological order using color coding, blinking coding and audible tones.

On the LDP, all alarms are grouped in each system (i.e., reactor coolant system (RCS), residual heat removal (RHR), etc.) and these grouped alarms are located in the fixed position area of the LDP representing as the alarm tiles (system labels). (See Figure 4.9-6) The grouped alarm tiles (system labels) are also blinking and color-coded when the new alarm occurs. Primary parameter labels and component labels are also used for the individual alarm indications related with the parameters and components. These are also blinking and color coding when a new alarm related to the parameter or the component occurs.

Alarms are also shown in graphic displays on the Operational VDU representing the related parameter's numerical value with red color and switch information (i.e., trip, power-off, etc.).

There are four alarm states – new, acknowledged, cleared, reset (normal).

- New - The operator can become aware of a new alarm by the blinking display and audible tone, and recognize the new alarm information in the alarm VDU display.
- Acknowledged -The operator can confirm (acknowledge) the new alarm by touching the new alarm display area (blinking area), which stops blinking and audible tone sounding on the Alarm VDU. Then the operator can call up the related alarm procedure display on the Operation Procedure VDU and the related operational display on the Operational VDU respectively directly by touching or clicking the alarm message display area (See (2) in Figure 4.7-1) on the Alarm VDU in order to diagnose and take actions smoothly. Acknowledged alarms are identifiable by continuous color indications.
- Cleared - When alarm conditions return to normal the alarm is displayed as cleared.

Cleared alarms can be identifiable by low speed blinking and white color indications.

- Reset - Cleared alarms are manually reset by operator acknowledgement. Reset alarms are identifiable by turning to normal indication (i.e., no-indication on the Alarm display and normal color (gray color) on LDP).

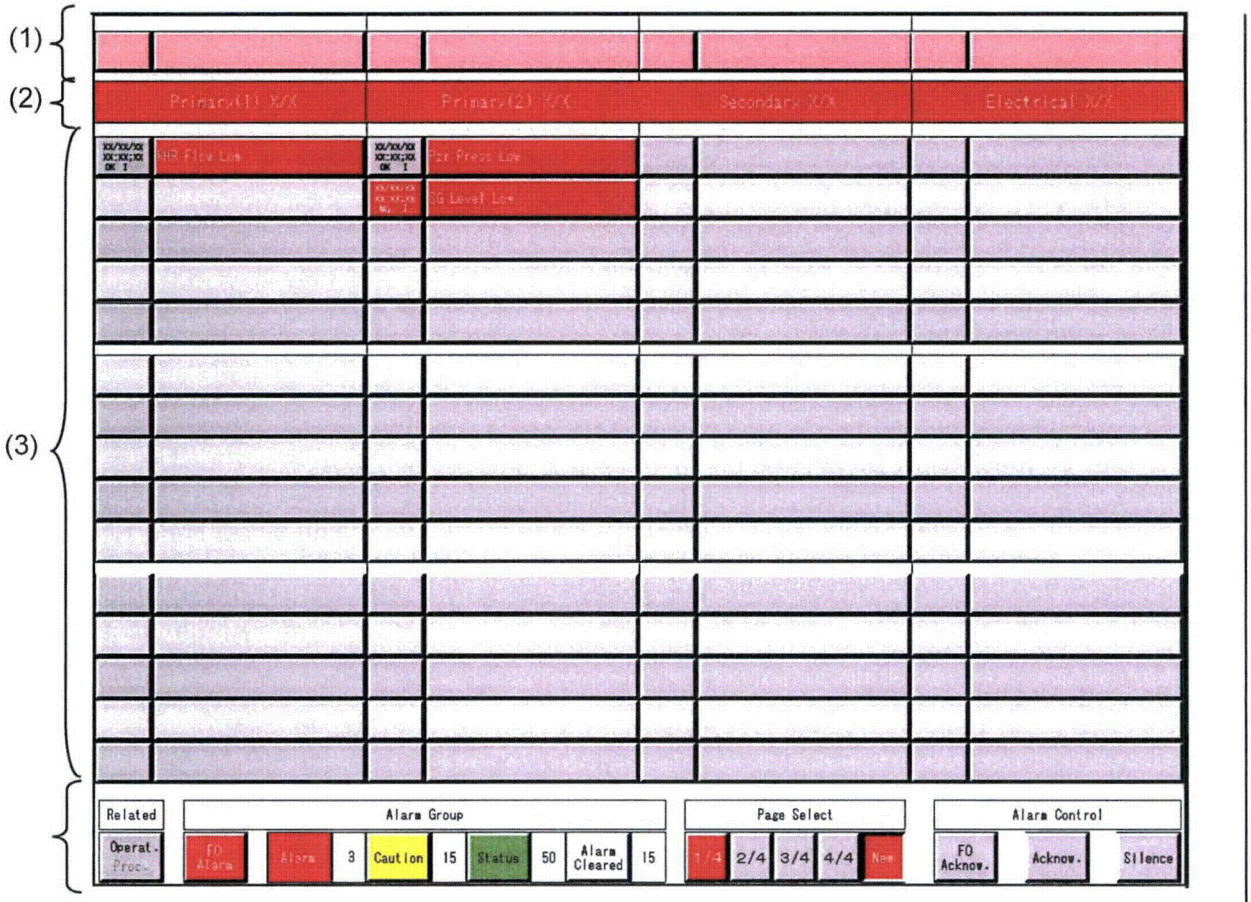
b. Allocation of roles between the Alarm VDU and the Large Display Panel

The LDP provides grouped alarms in the upper area of the fixed screen. And the related individual alarms are located near the primary parameter indications in the fixed display area. This approach ensures an effective identification of the plant emergency state and the overall system status. Individual alarms are displayed on the alarm VDU display utilizing the location information on the LDP as follows:

Four division display areas on the Alarm VDU are located in accordance with the location of the system mimic information in the fixed position area in LDP. Therefore, the left two primary systems on the Alarm VDU are the primary systems outside the CV (Containment Vessel) (all primary systems except those described next) and Reactor/NSSS systems (i.e., RV, RCS, SG, MS, FWS), respectively. And to the right, the next two areas are turbine system and electrical system, respectively. (See Figure 4.7-1 and the layout of the fixed display area on LDP in Section 4.7.2) Therefore, the operator can easily make a transition from becoming aware of the new alarm occurrence on the LDP to identifying the new alarm information on the alarm VDU.

In addition, the operator can acknowledge the new alarm by touching the alarm acknowledgment button which will stop blinking and ringing of the alarm VDU. The acknowledgement button only affects alarms that are visible to the operator. If there are multiple alarm pages, each page must be acknowledged separately.

To easily identify the most important alarms, multiple screens are provided to display the dynamic alarm prioritization logic. The most important alarms at that time remain in the highest prioritized alarm (Priority Level 1) display which is color-coded as red. Less important alarms at that time and cleared alarms are moved to the other lower priority alarm (Priority Level 2 or 3) screens which are color-coded as yellow and green (see section 4.7.2). The cleared alarm screen is color-coded as white.



(1) Fast-out Alarms display area
Each first-out alarm of "ECCS Actuation", "Reactor Trip", "Turbine Trip" and "Generator Trip" is displayed respectively.

(2) Alarm title area
"Primary (1)"; Primary systems outside the CV (all primary systems except "Primary (2)")
"Primary (2)"; Reactor/NSSS systems (i.e., RV, RCS, SG, MS, FWS)
"Secondary"; Turbine system
"Electrical"; electrical and transmission system

(3) Alarm message display area
All individual alarm messages are displayed in the four system categories with its occurrence date/ time and static prioritization levels.

(4) Alarm acknowledgement/reset and screen request buttons area
Related; Alternative switch for related display selection between Operational display and Operation procedure display
Alarm Group; Alternative switches for prioritization alarm display selection, "Fast out alarm", "Alarm (Priority 1 alarm display)", "Caution (Priority 2 alarm display)", "Status (Priority 3 alarm display)" and "Alarm Cleared (Cleared alarm display)"
Page Select; Alternative switches for multiple alarm page selection which displays 15messages x4categories alarms in one page.
Alarm Control; Alarm acknowledge buttons for Fast out alarm and other alarms which can make all alarm displayed on the current page acknowledged by each alarm page and each prioritization alarm page.
Alarm sound stop button which can make the alarm sound stopped to reduce operator's stress. Blinking still remains so that unacknowledged alarms are identifiable.

Figure 4.7-1 Alarm VDU Screen Specifications

4.7.2 Alarm Prioritization

a. Prioritization Based on Specific Importance (Static Prioritization)

Many alarms are statically prioritized by importance based on plant impact including release of radioactive materials and the demand for operator action. The static priorities have six levels. Table 4.7-1 shows the static prioritization category. The prioritization levels are displayed on an alarm message area on the Alarm VDU.

b. Prioritization Based on Dynamic Prioritization (Dynamic Prioritization)

The priority of other alarms is dynamically determined by alarm processing logic which focuses on the relationship between each issued alarm based on physical relationships such as the plant process and equipment status. Based on that dynamic determination, each alarm is prioritized at the given moment to its importance. The dynamic priorities have three levels. The prioritizations for all alarms are as follows:

- Priority Level 1 (alarm information; Need actions)
- Priority Level 2 (caution status information ; Need acknowledgment but no need for actions)
- Priority Level 3 (status information ; No need for actions nor acknowledgement)

The dynamic prioritization rules are simple, consistent and do not depend on the plant specific mode. In the dynamic prioritization, there are three rules:

- Higher prioritization rule: For multiple-setpoint alarms, lower importance alarms are regarded as status information when higher priority alarms are activated. For example, Figure 4.7-2 shows the tank level alarm which has multiple setpoints.(i.e., Low and Low-Low) In this case, the Low alarm is displayed as Priority 1 (alarm information) until the tank level achieves to the Low-Low alarm setpoint. When the level achieves the Low-Low alarm setpoint, the Low-Low alarm is displayed as Priority 1 and the Low alarm is changed to Priority 3 (status information).
- Cause-consequence rule (Component level): For those alarms which have a relationship between "result" and "cause", the “result” alarm is regarded as status information when the “cause” alarm is activated. For example, Figure 4.7-2 shows the illustration of the fluid system. Normally the outlet pressure low alarm is Priority 1. However, whenever the pump is tripped the outlet pressure low alarm will also occur. Therefore, the low pressure alarm (“result” alarm) is regarded as Priority 3 (status information) when the pump is stopped by the interlock alarm (i.e., “cause” alarm) which is displayed as Priority 1 (alarm information).
- Mode rule: This is the Cause-consequence rule at the system level. For example, the charging pump trip alarms are regarded as Priority 3 (status information) when an SI signal is actuated. (See Figure 4.7-2)

If a Priority Level 3 alarm is used for an interlock and the status of the component relevant to the interlock is not monitored by the alarm system, it must be regarded as a Priority Level 2 alarm. For example, “Pressurizer level deviation high from setpoint” alarm is initially Priority 1. It would normally turns to Priority 3 when the “Pressurizer level high alarm” occurs. However, since the level deviation alarm controls the backup heater it is downgraded only to Priority 2. This prompts the operator to confirm the actuation of the backup heater.

Table 4.7-1 Static Alarm Priority

(High)

(Low)

Priority	Primary System		Ventilation System		Turbine & Electrical systems	
	Type	Contents	Type	Interim	Type	Interim
I	ECCS Actuation	Alarms related with ECCS, C/V isolation signals	Safety System Activate	Ventilation isolation alarm of MCR	-	-
II	Reactor Trip	First out Alarms	-	-	Turbine Generator Trip	First out Alarms/ Blackout
III	Caution for ECCS Actuation	1.Malfunction alarms of ECCS actuation 2.Manual actuation alarms after ECCS actuation	Same as the Primary system	Same as the Primary system	Same as the Primary system	Electric power supply about ECCS
IV	Caution for Reactor Trip	1.Causing alarms of reactor trip 2.Manual actuation alarms about protective actuations 3.Primary component's alarms	-	-	Turbine Generator Trip Caution	1.Causing alarms of Turbine and Generator trip 2.Emergency manual actuation alarms 3.Primary component's alarms
V	Cautions for Operation	Alarms concerning cautious system monitoring (including partial trip)				
VI	Operation Management	1.Local operating alarms 2.Alarms concerning plat maintenance 3.Alarms concerning testing				

On the Alarm VDU, alarms are distinguished and displayed on each prioritization alarm page. For Priority 1 and 2 alarms, the operator needs to acknowledge new alarms so that when alarms move to Priority 1 and 2 pages, these alarms are blinking and audible on the new page. On the other hand, Priority 3 alarms are not acknowledged and because they do not need operator's actions and confirmation. Avoiding new alarm acknowledgment and recognition on the blind pages, the prioritization page select button (i.e., Alarm group area in (4) on Figure 4.7-1) is blinking and continuing to sound until all alarms are recognized on each Prioritization alarm page.
Alarm prioritization is also identifiable on the LDP representing the Priority color code which is the same as on the Alarm display. Regarding the group alarms, the higher priority color code in the same group is represented. (See section 4.9.3 e.)

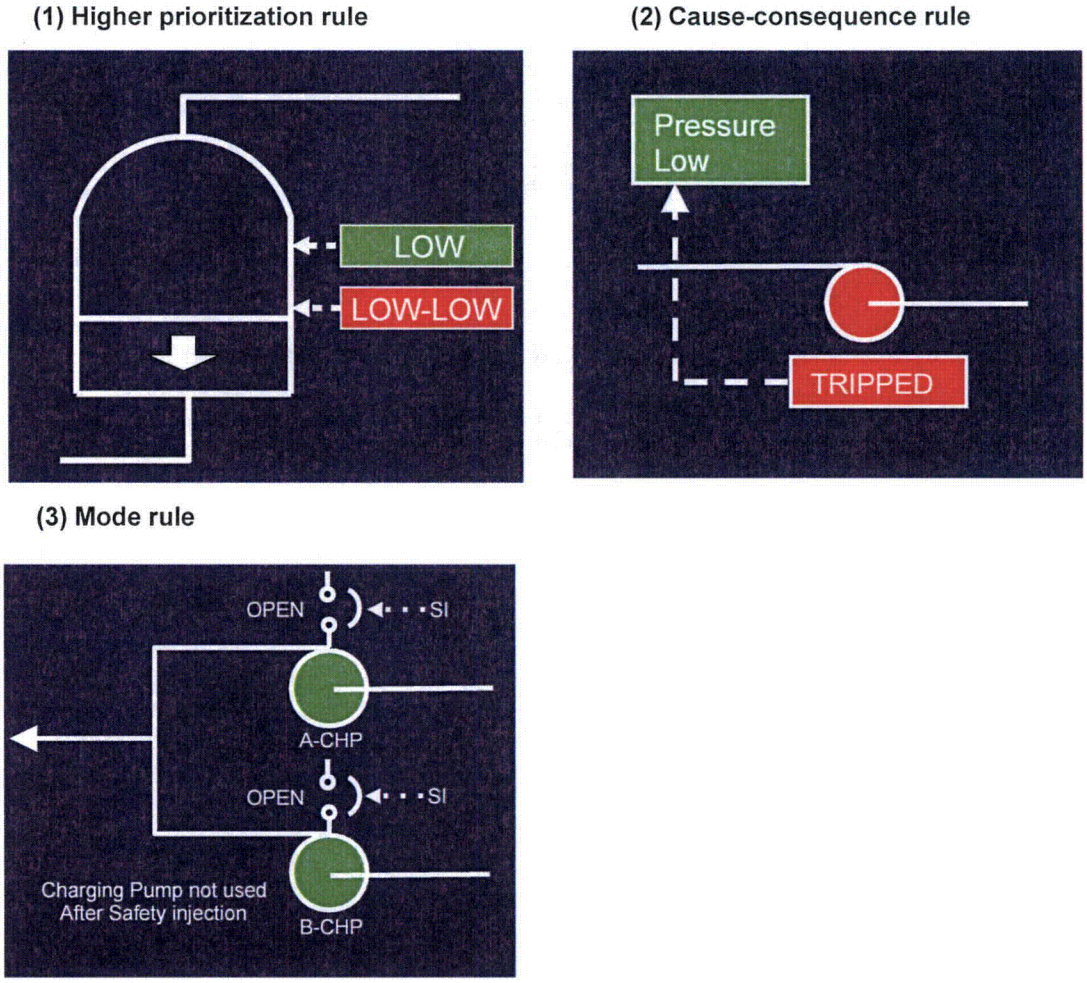


Figure 4.7-2 Dynamic Alarm Prioritization

4.7.3 Coding by Alarm Sound

Alarms are coded by four distinct sounds to enable operator identification of alarm type (first-out, general alarm) and the dynamic prioritization (red, yellow). A First-out alarm needs to be distinguished from other alarms because it identifies a plant trip or ECCS actuation. Dynamic prioritization alarms are distinguished by priority levels. It helps the operator to identify which priority page the new alarm is displayed on. Bypass and permissive indicators are also acknowledged by sound and blinking. They can be also identifiable from the alarm sounds. The sounds are coded based on frequency and repeating cycle. There are no sounds for cleared alarms.

4.7.4 First-out Alarms Displaying

A first out alarm is the first condition to cause a major change in plant state (i.e., reactor trip, turbine trip, generator trip, and ECCS Actuation). First out alarm groups are designated for each separate condition (i.e., reactor trip, turbine trip, generator trip, and ECCS Actuation). The first out alarms for each group is displayed on the Alarm VDU and on the LDP. All alarms after the first out alarm are displayed in time series on a dedicated first-out screen on the alarm VDU.
The first-out alarm is detected by the PSMS processor, turbine protection or hard-wired equipment (Generator trip) with a high time resolution (less than 100 milliseconds).

4.7.5 Acknowledging and Resetting Alarms & Stopping Alarm Sound

'Acknowledging' means the operator identify and confirms the individual new alarm concretely and 'Resetting' means the operator delete the cleared alarms. Alarms are acknowledged and reset using alarm acknowledgement and reset buttons provided on the alarm dedicated screen (displayed on the Alarm VDU).

In addition to acknowledging and resetting, there is an alarm sound stopping function. This function simply stops the sound associated with existing new alarms. Blinking still remains so that unacknowledged alarms are identifiable. The alarm sound is stopped using an alarm sound stop button provided on the Alarm VDU screen and an operator console hardware button. It stops all sounds associated with existing new alarms at the moment. Therefore, sounds are generated for any new alarms that occur after the alarm sound stop button is activated.

4.7.6 Avoiding Nuisance Alarms

A "Black Board" alarm concept is applied so as to improve operability. Alarm logics distinguish normal conditions that are not alarmed (e.g., low flow when the pump is demanded to be off,) and abnormal conditions which are alarmed (e.g., low flow when the pump is demanded to be on) judging from equipment status and process measurement status.

4.7.7 Link to Related Display

Touching or clicking the alarm message area, the related operational display is selected on the Operational VDU next to the Alarm VDU or the related alarm response procedure is selected on the Operating Procedure VDU in front of the Alarm VDU.
The selection is made by alternative switch located on the Alarm VDU. (See Figure 4.7-1)

4.8 Computer-Based Operating Procedure

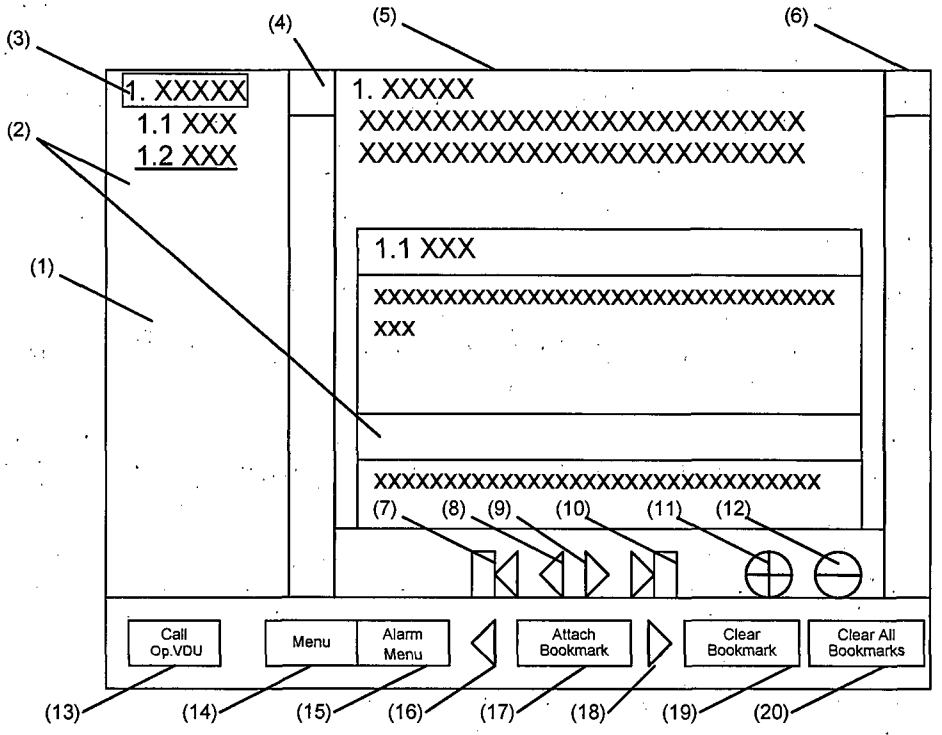
Computer-Based Procedures (CBP) are provided on the Operating Procedures VDU, the essential interaction principles are:

- The procedure is structured in accordance and compliant with the textual images, so that it is easy to handle and has the flexibility to incorporate textual modifications. The textual document can also be available for backup of the CBP.
- By requesting operations on the Alarm VDU, alarm response procedures (ARPs) are directly selected on the Operating Procedure VDU which is located in front of the Alarm VDU.(See Figure 4.4-3 and Table 4.4-2)
- In case of emergency, such as plant trip, the operators can request the emergency procedure for reactor trip or ECCS by touching the first-out alarm on the Alarm VDU. Distinctive accident procedures (e.g., LOCA, SGTR) are requested from the CBP menu screen after the operator identifies the plant status.
- By selecting hyper-links on the Operating Procedures VDU, the related operational VDU display is automatically displayed on the Operational VDU. (See Figure 4.4-4).
- The related soft switch or controller is not requested directly on the Operating Procedures VDU to avoid operator's omission of relevant information (line-up, inlet difference pressure, etc.) confirmation. For example, when the operator is executing a procedure that requires a valve to be opened, the operator takes the following steps:
  1) Select the hyper link on the CBP for the Operational VDU page
  2) Select the component to be controlled
  3) Select the component switch software cover
  4) Select the control action (open/close)
- When the operator completes the current task on the CBP, the operator selects the hyper link concerning the next task on the CBP in order to call up the related operational VDU page without closing the current windows or pages.

A Commercial off the shelf (COTS) platform and a generic format (PDF, MS Word, HTML, etc.) are used for the operation procedure system. This approach enables lower cost for utilities' alterations to operating procedures. The development process is as follows:

1) The procedure is manually created or revised using the COTS platform. The procedure includes fields with unique tag identification for links to appropriate Operational VDU screens and links to other procedures.
2) The procedure is manually reviewed and approved through appropriate plant administrative quality assurance (QA) procedures.
3) The approved procedure is compiled using automated CBP tools to integrate into the digital HSI System. The CBP tools are developed using a design process that includes Verification and Validation, and Configuration Management. This process is equivalent to the design process used for the PCMS.
4) A series of manual checks are performed to ensure the CBP tool has compiled with the procedure correctly. Since the automated CBP tool has been previously verified, these manual checks include samples of procedure steps and hyperlinks. Complete manual verification is not required.

5) The new CBP software, which includes the newly compiled procedure, is maintained under Configuration Management.



Note: See table 4.8-1 for specifications of CBP icons, (1)-(20)

Figure 4.8-1 Computer-based Operating Procedure

Table 4.8-1 Specifications of Operational VDU icons

No.	Type	Color/icon Color/letter	Shape	Function
(1)	Index window	White Black	Rectangle	Index of the selected procedure. Link to top of each chapter or section at (5) by touching or clicking chapter or section title.
(2)	Bookmark	White Blue	Underline	By touching or clicking certain chapter/section title or paragraph, then touching or clicking (17), a bookmark is attached. The letters change to blue and underlined.
(3)	Selected procedure in procedure steps	-	Rectangle Frame	Selected procedure (chapter, section or page) in the procedure steps displayed on (5).
(4)	Scroll bar	Light Gray	Rectangle	Scroll window (1).
(5)	Procedure Window	White Black	Rectangle	Display procedure page, including text, figure table, etc.
(6)	Scroll bar	Light Gray	Rectangle	Scroll window (6).
(7)	Page control	Light Gray Blue	Triangle	Go to previous chapter.(Also available by touching or clicking previous chapter on (1))
(8)	Page control	Light Gray Blue	Triangle	Go to previous page.
(9)	Page control	Light Gray Blue	Triangle	Go to next page.
(10)	Page control	Light Gray Blue	Triangle	Go to next chapter. (Also available by touching or clicking next chapter on (1))
(11)	Page control	White Blue	Circle	Zoom in.
(12)	Page control	White Blue	Rectangle	Zoom out.
(13)	Call operational VDU	Dark Grey White	Rectangle	Call up the related screen on the Operational VDU. Repeat to touch or click, to call other screens, grouped as the "related screen" to the page, current displayed on CBP.
(14)	Menu	Dark Grey White	Rectangle	Select a procedure from procedure list. (e.g., Reactor Operation, Turbine Operation, Accident Operation)

Table 4.8-1 Specifications of Operational VDU icons (continued)

No.	Type	Color/icon Color/letter	Shape	Function
(15)	Alarm menu	Dark Grey White	Rectangle	Same as select "Alarm Response Procedure" (ARP) at (14), prepared to approach quickly. Procedures for "First out alarms" (plant trip, ECCS activation) are included in the ARP.
(16)	Bookmark control	Dark Grey White	Rectangle	Go to previous bookmark.
(17)	Bookmark control	Dark Grey White	Rectangle	Attach a bookmark. (See (2))
(18)	Bookmark control	Dark Grey White	Rectangle	Go to next bookmark.
(19)	Bookmark control	Dark Grey White	Rectangle	Clear the bookmark.
(20)	Bookmark control	Dark Grey White	Rectangle	Clear all bookmarks.

Note: Generic control functions, such as "Open the window", "Close the window", "Save", "Load" are supported by the commercial off the shelf platforms and not included in the Figure4.8-1 and table 4.8-1.

4.9 Large Display Panel

4.9.1 Purpose of Large Display Panel Installation

The purposes of the LDP are followings:

- To provide continuously visible information to the plant operator in order to ensure that the operator has available to all relevant plant information.
- To make plant information simultaneously available to all plant operating staff on duty and to support operator team activities

4.9.2 Large Display Panel Screen Display Features

The large display panel for the US-APWR has four 100-inch diagonal screens. The sizes and locations of these screens may vary for operating plants based on physical limitations of the MCR. For example, if 100-inch screens cannot be accommodated, smaller screens can be duplicated in multiple MCR locations to ensure readability by all operators. The actual sizes and locations for operating plants will be described in the Plant Licensing Documentation.

4.9.2.1 Fixed Display Area

The fixed display area displays the same information at all times. The following section explains how that information supports plant operation during various plant conditions.

- During Normal Operation
  The fixed display area displays the main plant parameters required for monitoring the plant status during normal operation, enabling quick error detection. It also displays the main plant parameters required for monitoring the plant status during power fluctuation and parameters that may cause a plant trip. The fixed display area simplifies verification of performance of main plant systems during normal operation.
- In the Event of a Plant Trip
  In the event of a plant trip, the fixed display area displays information required for verification of trip status information related to the reactor, turbine and generator immediately following a plant trip, thereby simplifying the trip status verification process.
- In the Event of an ESFAS Actuation:
  In the event of an ESFAS actuation, the fixed display area displays the engineered safety features components status and process values indicating system performance, thereby simplifying verification of the safety injection operation status (See section 4.10).
- During Accident Response (Status Identification)
  At the time of an accident, the fixed display area displays the main plant parameters required for plant status identification (Type A and B parameters of R.G.1.97), thereby simplifying status identification when an accident occurs.
- In the Event of an Alarm
  In the event of an alarm, the fixed display area displays grouped alarms, thereby simplifying detection.
- Safety system bypass or inoperable state indication (BISI) is continuously visible on the fixed display area based on the principles of design and industry guidelines (IEEE-603-1991, R.G. 1.46, IEEE-497, etc.).

Table 4.9-1 shows the typical parameters mentioned above for the LDP.

4.9.2.2 Variable Display Area

The variable display area shows detailed plant information and trend displays on the operational VDU display, thereby supplementing the information provided in the fixed display area and facilitating retrieval of plant information. The contents of the variable display area can be selected from the operator console and from the supervisor console, thereby helping the operating staff's common awareness and communication. The variable display area can also automatically display pre-selected screens. Manual and automatic screen selections are described below.

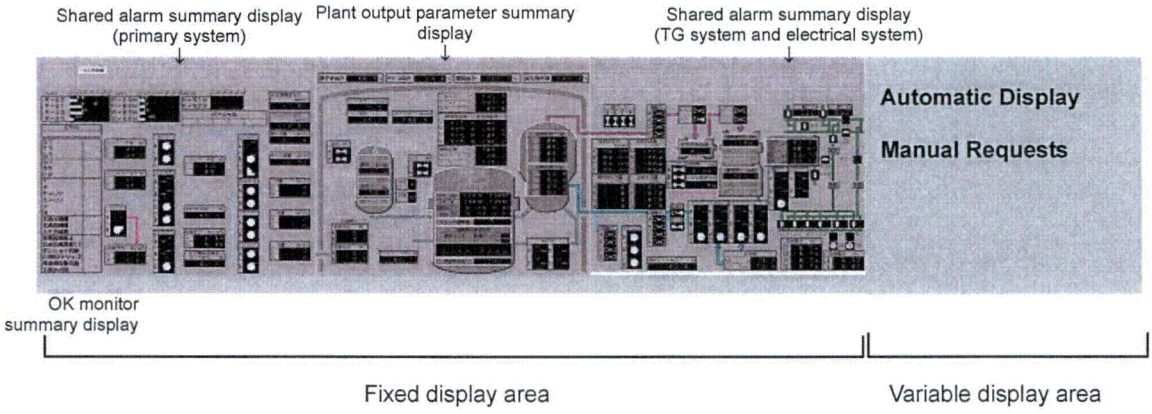


Figure 4.9-1 Large Display Panel Specifications (Overall)

a. Automatic Display

The variable LDP screen can be automatically selected based on the following trigger signals:

- First Out Alarm – The screen that is automatically selected is relevant to the First Out alarm condition. This screen helps the operator diagnose the condition that lead to the plant disturbance.
- Permissive signal activated/deactivated – The screen that is automatically selected is relevant to the specific Permissive/Bypass function.

The automatic display function can be blocked by the operator.

b. Manual Request

The ability to manually select displays for the variable display area on the LDP requires that the operational VDU be available, since it features a request menu button on each screen. The function of the menu button is as follows:

1) Transmission menu

The transmission menu button is set as a function key on each operational VDU screen. When the transmission menu button of the screen currently displayed on the operational VDU is pushed, the current screen is displayed on the variable display portion of the LDP. Even if the display screen of the operational VDU changes after the transmission menu button is pushed, the display screen in the LDP variable display is not changed.

2) Connection menu

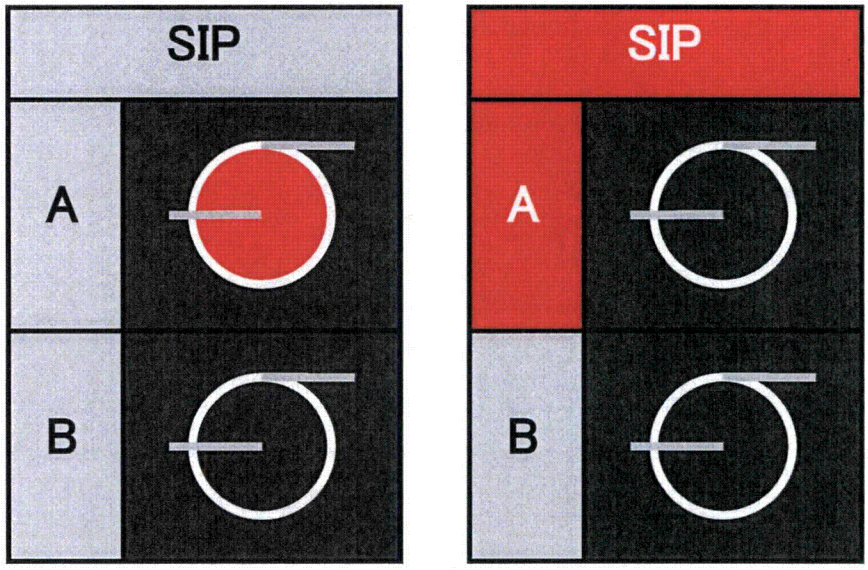
The connection menu button is set as a function key on an operational VDU screen. By turning on the connection menu button, the variable LDP screen is automatically requested to be the same as the operational VDU screen requesting it. When different screens are selected on the operational VDU these same screens are displayed on the LDP.

There is no priority between the manual selection commands from operational VDUs used by the RO, SS or STA. Therefore the last requested screen is displayed. In addition, if the automatic display function is not blocked, when an automatic display trigger signal comes, the variable portion of the LDP changes to an automatic display screen.

4.9.3 Alarm Display on the Large Display Panel

a. Flow Sheet Image

The LDP uses equipment symbols to display alarms when conditions arise that affect the particular equipment. For example, a pump trip alarm is displayed by having the pump icon flicker.



A-SIP trip
(A-SIP icon turns red)

A-SIP AOP bearing oil pressure low-low
("A" and "SIP" frames turn red)

Figure 4.9-2 LDP Component Alarm Status Display

b. Abbreviation of Alarm Name

Although an alarm is displayed by using the symbol and parameter name label of the equipment and the alarm name, if the equipment's name is contained in an alarm name, the equipment name is omitted if the recognition of the affected equipment does not become difficult. The design intent is for the alarm display on the LDP not to become complicated or unclear by excessive display of the alarm identification information.

c. Message Slot System

For alarms related to the same parameter (e.g., high, high-high, low, low-low) the alarm display in the LDP includes dynamic display areas instead of separate window tiles as is typical on conventional control boards. The dynamic display area shows the highest priority alarm condition.

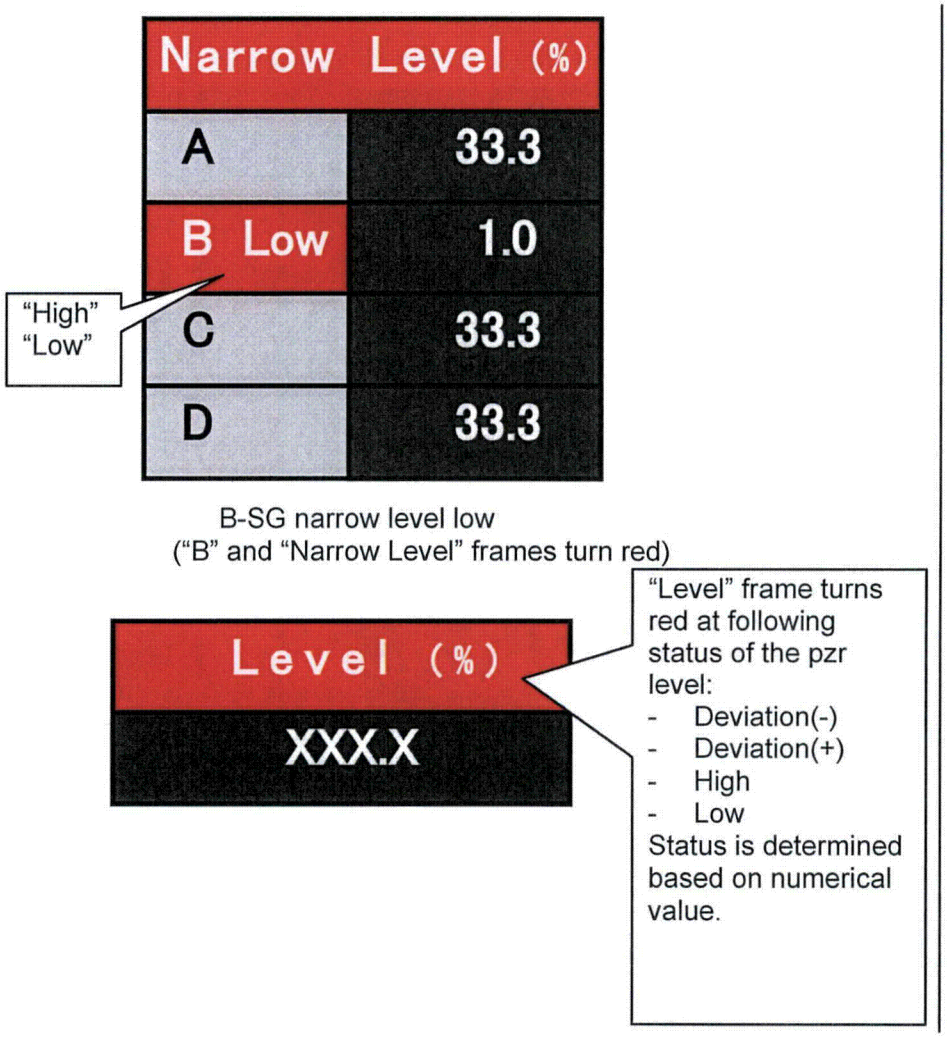


Figure 4.9-3 LDP Process Parameter Alarm Status Display (1/2)

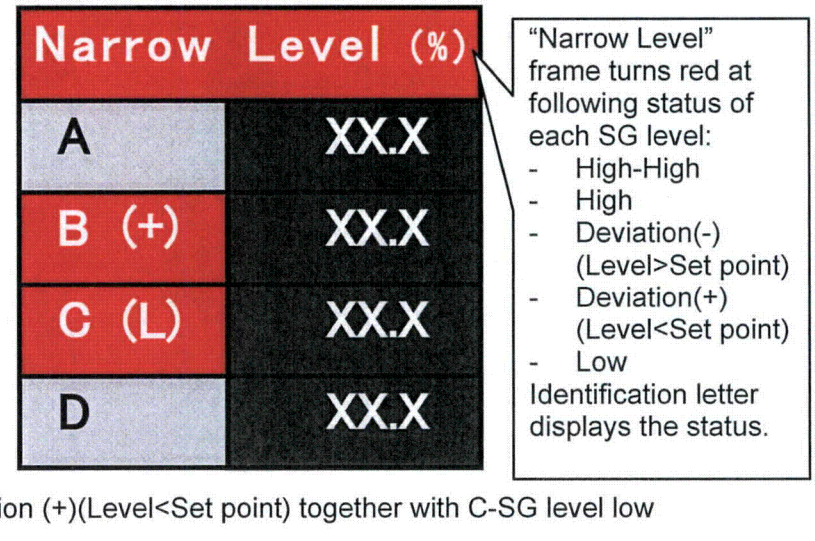


Figure 4.9-4 LDP Process Parameter Alarm Status Display (2/2)

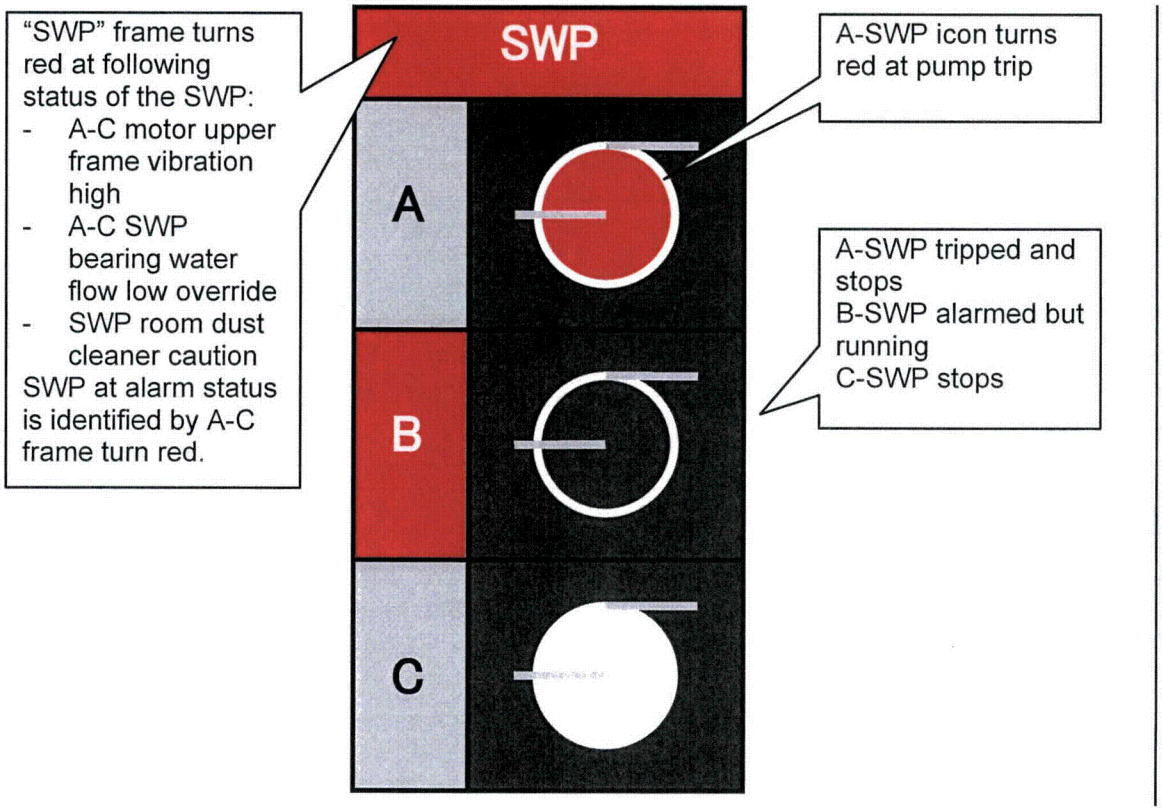
d. First-out Alarm

In order that a first out alarm may show directly the initiation of a nuclear reactor trip signal, an ECCS signal, etc., alarm sharing is not performed because performing such sharing could cause identification and corresponding operation difficulties. However, the LDP fixes for every first out the display of the first hit alarm. Checks are also made on the alarm VDU screen after second hits. Each first out alarm for "ECCS Actuation"/Reactor Trip"/"Turbine Trip"/"Generator Trip" is arranged in the topmost part of the Large Display Panel screen.
Each first out alarm indicates as a message in the message display area for each first out alarms (message slot) rather than in window tile form like a conventional control board.

e. Shared Alarms

Certain alarms are basically shared for every parameter state.
However, the alarm of a multi-level alarm displays the state and provides a display location which is commonly used for every parameter.
("Water Level Low" ->"Water Level High" if a state changes, the message will change)

The shared alarm represents the highest priority color code of the individual dynamic prioritization alarms involved in each shared alarm display frame. Whenever a new alarm occurs, the shared alarm display area is blinking with sound and may change the priority color if a new alarm is higher dynamic priority alarm. If all individual alarms in the shared display frame are cleared, then the display color turns white with low blinking. If all individual alarms in the shared display frame are reset by touching or clicking the reset button on the Alarm display, then the shared display area turns normal background color.



A-Service Water Pump trip together with B motor upper frame vibration high

Figure 4.9-5 LDP Shared Alarm Status Display

f. SDCV Alarms and BISI status

The following alarms are displayed on the fixed section of the LDP (i.e., the display format is SDCV):

- alarms relevant to PAM parameters (Pressurizer Level Low, CV Pressure High, etc.)
- alarms demanding urgent responses (SG Level Low/High, etc.)
- alarms used for identification of major events (Radiation monitoring system (RMS) monitor High, Alarms related LBB, etc.)
- alarms important for overall supervision of plant status (Pressurizer Press Low, etc.)

The Bypassed or Inoperable Status Indication (BISI) is also displayed as SDCV features as "OK Monitor". (See section 4.10.3)

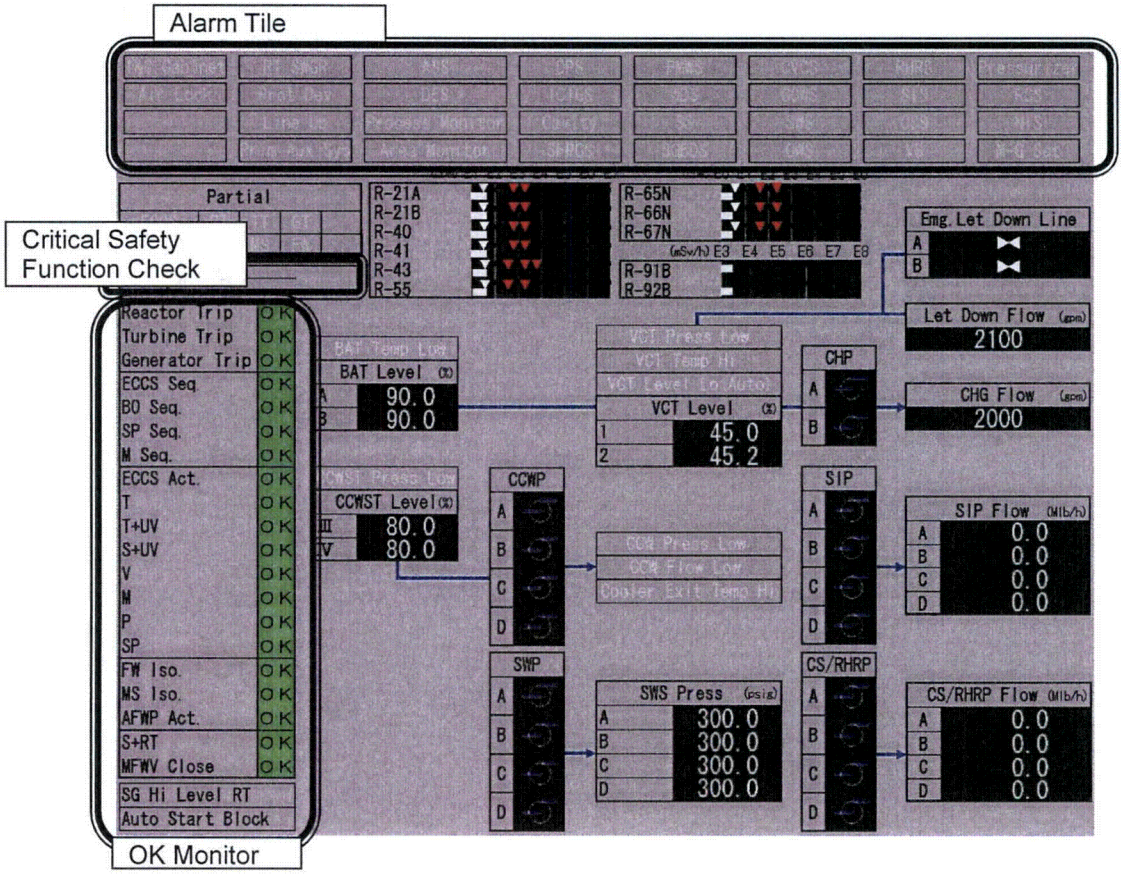
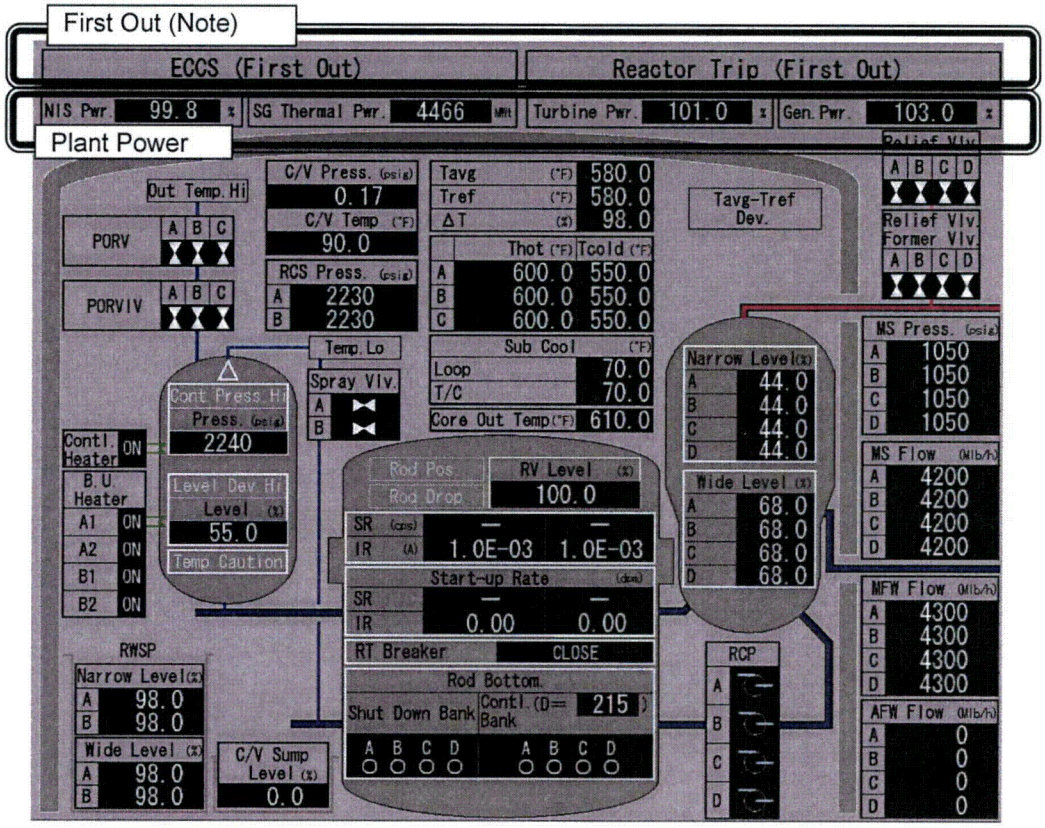


Figure 4.9-6 Large Display Panel Specifications (Left Wing)



Note:
PSMS tag the "First Out" when reactor (generator, turbine) trip or ECCS signal transmits for the first time. Although other trip or ECCS signals follow it and transmit at same cycle of data bus, HSI systems read the tag and display the "First Out".

Figure 4.9-7 Large Display Panel Specifications (Center Wing)

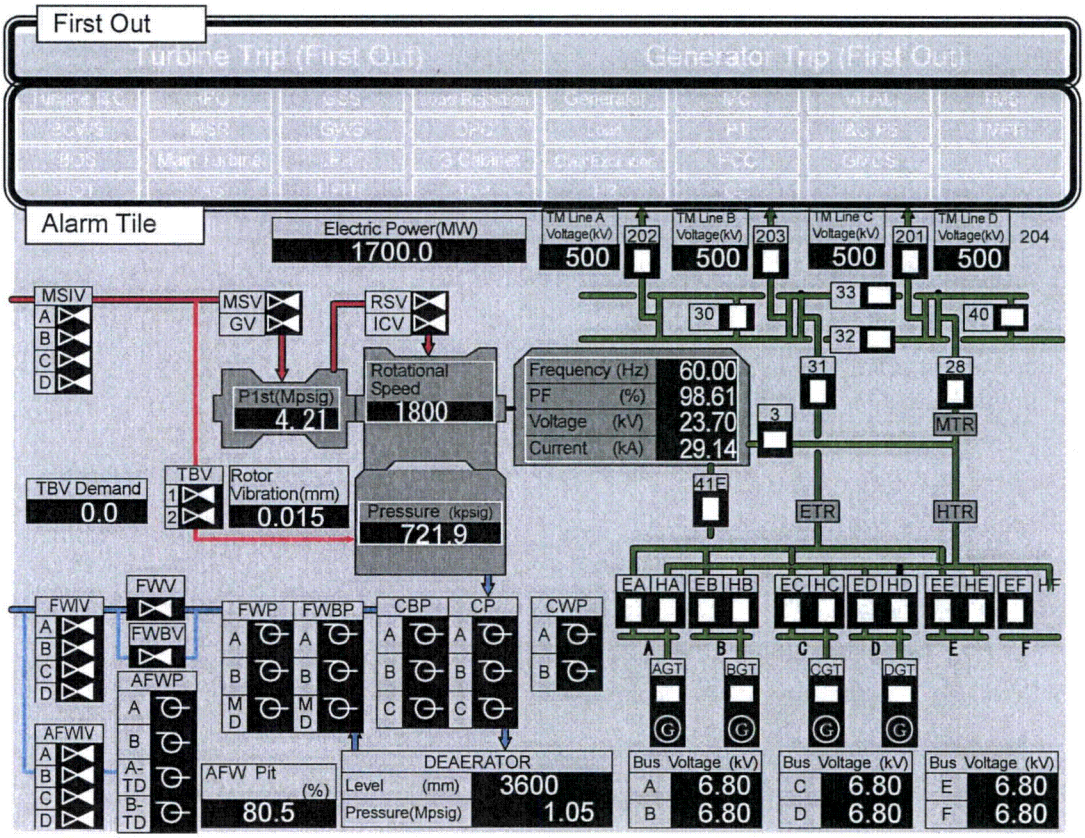


Figure 4.9-8 Large Display Panel Specifications (Right Wing)

Table 4.9-1 Parameters on LDP

	Plant Power	Cause of Reactor Trip	Plant Trip	ESFAS Actuation	PAM	SDCV Alarm	OK Monitor
Reactor Thermal Power	X						
Turbine Power	X						
Generator Power	X						
Nuclear Instrumentation System (NIS) Power	X	X			X		
Pressurizer Pressure	X	X			X	X	
Pressurizer Water Level	X	X			X	X	
Pressurizer Reference Water Level	X						
RCS Average Temperature	X	X					
RCS Reference Temperature	X	X					
RCS Delta-Temperature	X	X					
RCS Hot Leg Temperature (Wide Range)					X		
RCS Cold Leg Temperature (Wide Range)					X		
RCS Subcooling (Loop)					X		
RCS Subcooling (T/C)					X		
Core Outlet Temperature					X		
RCS Pressure					X	X	
Power Range Neutron Flux	X	X					
Intermediate Range Neutron Flux	X	X	X	X	X		
Source Range Neutron Flux	X	X	X	X	X	X	
Intermediate Range Neutron Flux Change Rate		X	X	X			
Source Range Neutron Flux Change Rate		X	X	X			
SG Water Level (Narrow Range)	X	X			X	X	
SG Water Level (Wide Range)					X		
SG Reference Water Level	X	X					
Main Steam Pressure	X	X			X	X	

Table 4.9-1 Parameters on LDP (continued)

	Plant Power	Cause of Reactor Trip	Plant Trip	ESFAS Actuation	PAM	SDCV Alarm	OK Monitor
Main Steam Flow	X	X					
Main Feed Water Flow	X	X				X	
Main Steam Tie Line Pressure	X	X					
Main Feed Water Head Pressure	X	X					
Turbine First Stage Pressure	X	X					
Charging Water Flow	X	X					
Letdown Water Flow	X	X					
Boric Acid Tank Water Level					X		
CCW Surge Tank Water Level					X		
Service Water Supply Line Pressure					X		
Containment Pressure					X	X	
Containment Temperature					X		
CV Annulus Pressure					X		
Safety System Component Room Pressure					X		
R/V Water Level					X		
Safety Injection Water Flow					X		
RHR Flow					X		
EFW Flow					X		
CV Spray Cooler Outlet Flow					X		
SFP Water Level					X		
RWSP Water Level							
EFW Pit Water Level					X	X	
CV Sump Water Level					X	X	

Table 4.9-1 Parameters on LDP (continued)

	Plant Power	Cause of Reactor Trip	Plant Trip	ESFAS Actuation	PAM	SDCV Alarm	OK Monitor
CV High Range Radiation Monitor					X		
CV Dust Radiation Monitor					X	X	
CV Gas Radiation Monitor					X	X	
Condenser Ejection Gas Radiation Level					X	X	
SG Blow Down Radiation Monitor					X	X	
Main Steam Radiation Monitor					X	X	
N-16 Main Steam Radiation Level					X	X	
Exhaust Duct Gas Radiation Level					X	X	
Control Room Emergency HVAC System Status					X		
Emergency Power Generator				X			
Reactor Trip Breaker Status		X	X	X	X		X
Control Rod Position	X	X	X		X	X	X
Pressurizer Relief Valve	X	X			X		
Pressurizer Relief Valve Shutdown Valve	X	X			X		
Pressurizer Spray Valve	X	X					
Pressurizer Back Up Heater	X	X			X		
Pressurizer Control Heater	X	X			X		
MFW Control Valve	X	X		X			X
MFW Bypass Control Valve	X	X		X			X
SG Makeup Water Line Valve		X					X
MFW Isolation Valve	X	X		X			X
EFW Isolation Valve				X			X
Turbine Bypass Valve	X	X					
Main Steam Relief Valve	X	X			X		

Table 4.9-1 Parameters on LDP (continued)

	Plant Power	Cause of Reactor Trip	Plant Trip	ESFAS Actuation	PAM	SDCV Alarm	OK Monitor
Main Steam Relief Valve Isolation Valve	X	X			X		
Main Steam Isolation Valve	X	X		X			X
Reactor Coolant Pump	X	X					
Charging Pump	X	X					
Component Cooling Water Pump		X		X			X
Service Water Pump		X		X			X
Safety Injection Pump				X			X
CV Spray/RHR Pump				X			X
Emergency Feedwater Pump				X			X
IA Compressor				X			X
CV Recirculation Fan				X			X
Bearing Cooling Water Pump		X					
Main Stop Valve	X	X	X				
Governor Valve	X	X	X				
Reheat Stop Valve	X	X	X				
Interceptor Valve	X	X	X				
Turbine Rotation Rate	X	X					
Deaerator Pressure	X	X					
Deaerator Tank Water Level	X	X					
Condenser Vacuum Rate	X	X					
Condensate Pump	X	X					
Condensate Booster Pump	X	X					
Circulating Water Pump	X	X					
Power Factor	X	X					

Table 4.9-1 Parameters on LDP (continued)

	Plant Power	Cause of Reactor Trip	Plant Trip	ESFAS Actuation	PAM	SDCV Alarm	OK Monitor
Generator Frequency	X	X					
Generator Voltage	X	X					
Generator Current	X	X					
Turbine Shaft Vibration	X	X					
Feed Water Pump	X	X					
Feed Water Booster Pump	X	X					
Transmission Voltage	X	X		X			
Safety M/C Bus Voltage	X	X		X	X		
Non-Safety M/C Bus Voltage	X	X		X			
Main Trans Circuit Breaker	X	X	X	X			
Generator Load Break Switch	X	X	X				X
Generator Field Circuit Breaker	X	X	X				X
Emergency Trans Circuit Breaker	X			X			X
Emergency Power Generator Circuit Breaker	X	X		X			X
House Trans Power Receive Circuit Breaker		X					X
Safety M/C Bus Power Receive Circuit Breaker	X			X			
Non-Safety M/C Bus Power Receive Circuit Breaker	X			X			
Switching Station Circuit Breaker		X					
Emergency Trans Power Receive Circuit Breaker		X					X
Transmission System Circuit Breaker	X	X		X			X
Safety DC Current C/C Bus Voltage					X		
Reactor Trip Status			X				X
Turbine Trip Status			X				X
Generator Trip Status			X				X

Table 4.9-1 Parameters on LDP (continued)

	Plant Power	Cause of Reactor Trip	Plant Trip	ESFAS Actuation	PAM	SDCV Alarm	OK Monitor
ECCS Status (ECCS Line-Up Valves)				X			X
ECCS Sequence Components				X			X
Black Out Sequence Components				X			X
CV Spray Sequence Components				X			X
Main Control Room Isolation Sequence Components				X			X
CV Isolation Phase A (T Signal) Actuating Valves				X			X
CV Spray Signal Actuating Valves				X			X
CV Isolation Phase B (P Signal) Actuating Valves				X			X
CV Isolation Phase A (T Signal) & Emergency Bus Under Voltage Signal Actuating Valves				X			X
Safety Injection Signal & Emergency Bus Under Voltage Signal Actuating Valves				X			X
CV Ventilation Isolation Signal Actuating Valves				X			X
Main Control Room Ventilation Isolation Signal Actuating Valves				X			X
Automatic Activation Block				X			
Main Steam Bypass Start Up Valve				X			X
EFWP Outlet Flow Control Valve			X				X
EFWP Drive Steam Inlet Valve			X				X
SG Sampling Line CV Outside Isolation Valve				X			X
SG Blow Down CV Outside Isolation Valve				X			X
SG Blow Down Stop Valve				X			X

4.10 Automatic Checking of Actuations

4.10.1 Integration of Monitoring and Operation

Typical actions of plant operators include checking the standby condition of equipment before operation, monitoring operating parameters (direct and relevant parameters) and identifying the plant behavior during operation. In order to improve the operability of the HSI system, all of the manipulation information on each switch (i.e., control power status, operation availability status, etc,) is displayed on an Operational VDU display with the component/valve status.

4.10.2 Automatic Checking of Actuations for Events

When a significant event like a plant trip occurs, or if an ECCS actuation occurs in case of an emergency, the operator's required actions and the attendant stress increase because the operator must simultaneously carry out many tasks, e.g., the operator must collect the safety-related system information and confirm plant conditions, etc,. In the HPI System, the status of components, valves and breakers, as well as the plant trip signals, ECCS signals and isolation signals are automatically checked and compared against the design conditions stored in the computer. The check results are displayed on the fixed area of the LDP and the Operational VDU as "OK monitor".

The following signals are verified:

- Reactor Trip
- Turbine Trip
- Generator Trip
- ECCS Actuation
- Containment vessel isolation phase A (T signal)
- Main steam flow isolation
- Emergency feedwater flow isolation
- Actuation of emergency feedwater flow
- Actuation of containment vessel spray
- Containment vessel isolation phase B (P signal)
- Containment vessel HVAC isolation (V signal)
- Main control room HVAC isolation (M signal)
- Charging water flow isolation

Figure 4.10-1 shows how the OK monitor results are displayed on the LDP and operational VDUs.

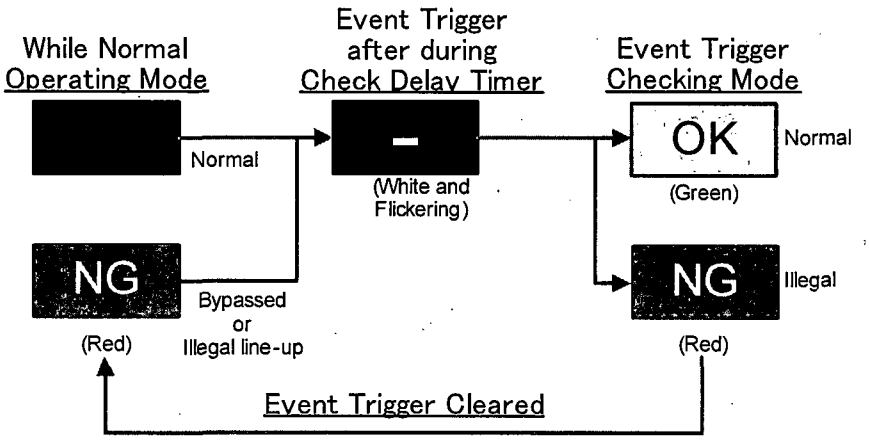


Figure 4.10-1 OK Monitor Display Format

4.10.3 Automatic Verification of Critical Safety Functions

When an event of accidents happens, the Unit Management Computer (UMC) continuously checks the plant conditions and confirms the integrity of the following Critical Safety Functions':

- Reactivity Control
- RCS Inventory
- Core Cooling
- Secondary Heat Sink
- RCS Integrity
- Containment Integrity

Note that Radioactivity Control from Supplement 1 to NUREG-0737 is maintained by maintaining all other critical safety functions, including containment integrity. Monitoring and controlling the six critical safety functions, defined above, is consistent with the Emergency Operation Procedures (EOP) of US operating plants and with the EOPs of the US-APWR. All EOPs, including those of the US-APWR, are described in plant licensing documents.

If any of the above mentioned functions are threatened the highest importance function message is displayed on the fixed area of the LDP (see Figure 4.9-6), and operators are able to transfer to the state-oriented response procedures.

4.11 Response to HSI Equipment Failures

The following standard and degraded operating configurations are considered in the HSIS design:

- Standard configuration (no loss of HSI functions)
- Degraded HSI systems by single failure
- Loss of all non-safety HSI
- Loss of all digital non-safety and safety HSI (Common cause failure (CCF))
- Loss of MCR

For each of the operating mode, the means to monitor and control the plant is as follows:

4.11.1 Standard Configuration

The operation of the plant is performed from the MCR whatever the plant status is, provided that the technical and operating criteria for the HSI are met. In this mode, the secondary control means are not allowed to send orders to the process.

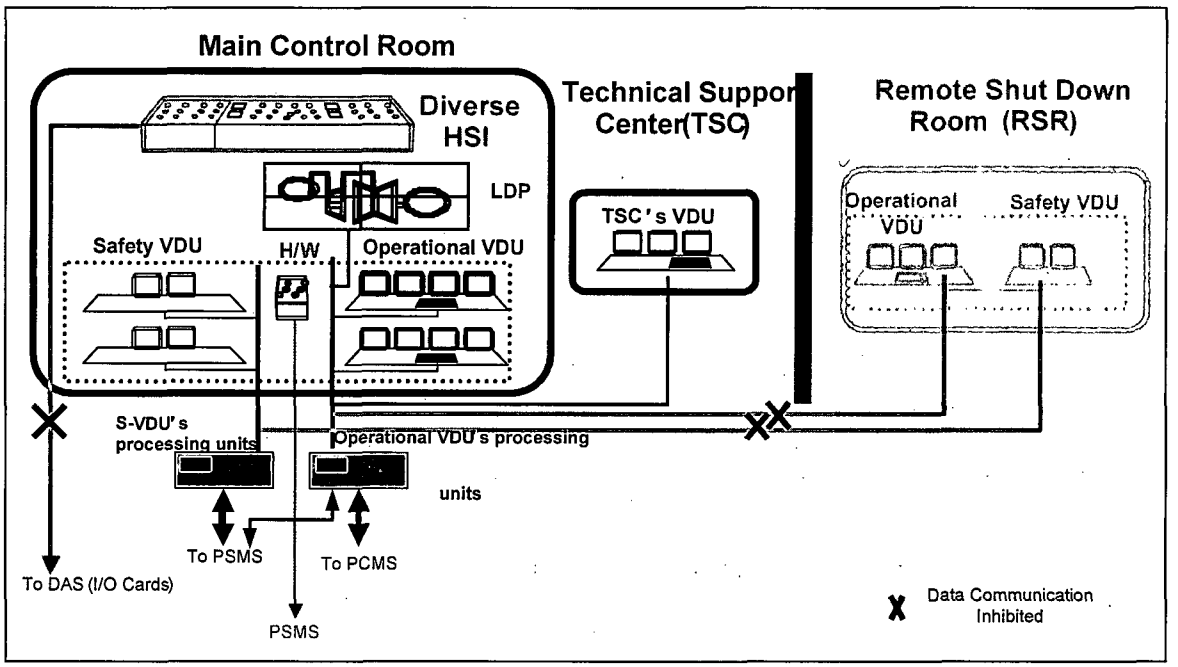


Figure 4.11-1 Standard Configurations for the Plant Operation

4.11.2 Degraded HSI Systems by a Single Failure

Figure 4.11-2 shows the overall architecture of the I&C System. In this architecture the HSIS data communication buses and computers have a duplicated configuration:

- Unit Management Computer (UMC)
  - Plant performance calculation (Reactor thermal power, etc.)
  - Logic calculation for monitoring (OK monitor, etc.)
- Process Recording Computer (PRC)
  - Plant operation logging instead of recorders of conventional plants
  - Plant trip sequence record
  - Long term recording of specific analogue parameters in case of a accident
  - Fast recording of specific analogue parameters in case of a tangent or accident
- Alarm logic Computer
  - Dynamic prioritization of alarms
  - Alarm control (acknowledge. Reset, etc.)
  - Alarm logging with time
- Large Display Computer
- TSC Computer
- EOF Computer

Therefore, a single failure of the bus or computers induces no influence on plant operation tasks. However, a single failure of VDUs, VDU processors or the LDP is considered.

As for a failure of LDP, The most likely failure of the LDP is that of the back lamp. The LDP has a spare lamp in it and easily exchanged by manual. In addition, it is also available to change the variable area to display a failed fixed area display and the SDCV function of the LDP is maintained.

The set of VDUs for a single operator is as follows:

- Operational VDU 3
- Alarm VDU 1
- Operating Procedure VDU 1

The appropriateness of the above described quantity of VDUs is confirmed by task analysis and by static and dynamic V&V by operators. Since there are two complete sets of 5 VDUs at the Operator Console, for use by one or two ROs, the operability is also validated in case of failure of one of the above VDUs.

As for the failure of the console for SS or STA, the SS console and STA console has the same function and capability. The SRO can shift to the non-failed console.

The appropriateness of the operator staffing of one Reactor Operator (RO) and one Senior Reactor Operator (SRO) under these degraded HSI conditions is confirmed by task analysis and by static and dynamic V&V by operators.

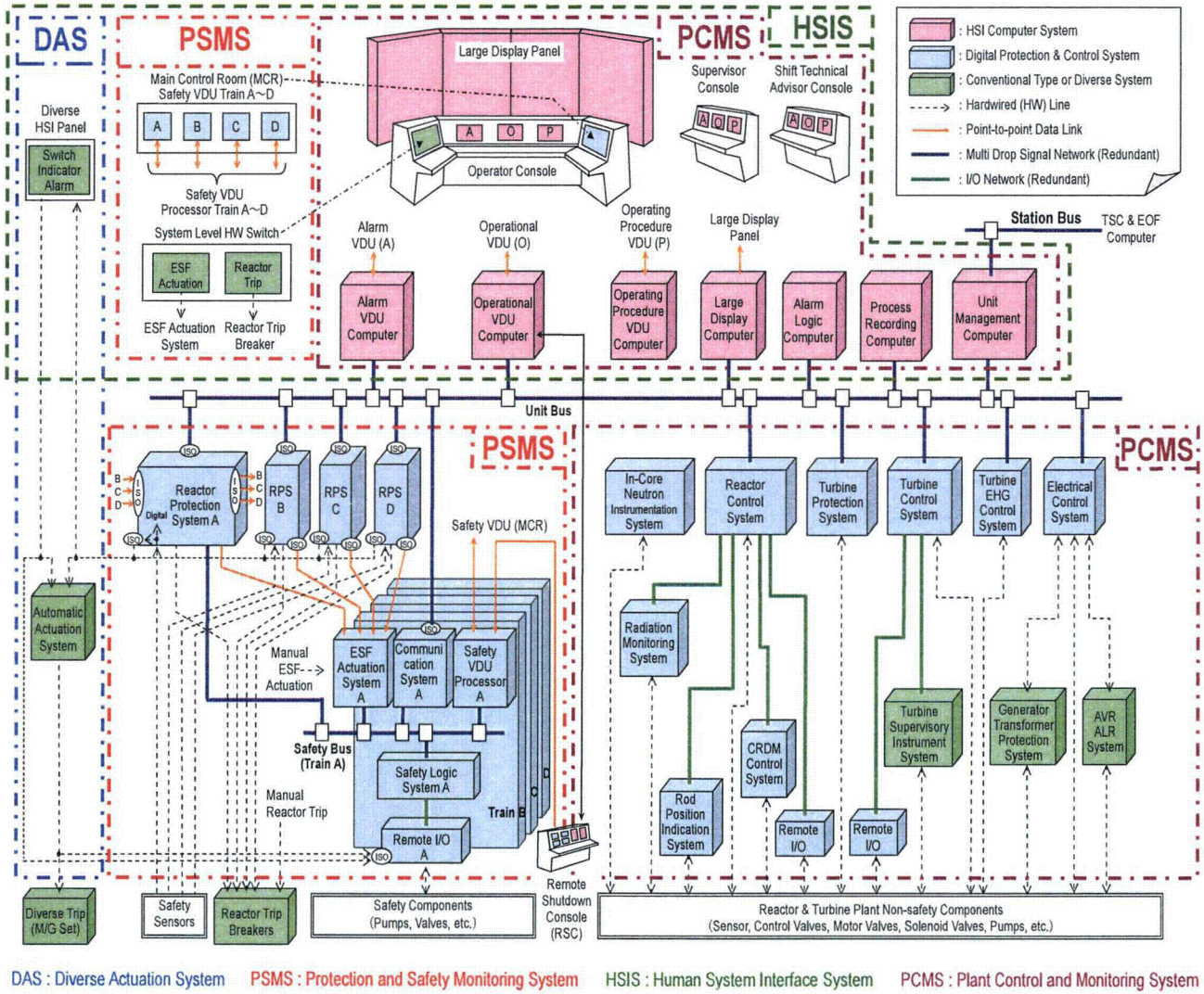


Figure 4.11-2 Overall I&C System of the US-APWR

4.11.3 Loss of All Non-safety HSI

The loss of the HSI is defined by a set of criteria (e.g., how many workplaces are needed to operate the plant and how many screens per workplace are needed). These criteria are defined during the detail design. However, for the worst case design basis, loss of the LDP and all non-safety VDUs is postulated.

The self diagnosis of non-safety HSIS system is expected to inform operator of the failures on LDP alarms and the Data Management Console (DMC) buzzer and messages. But since failure of all non-safety HSI is assumed, final credit for plant operability is supported by only the safety VDUs.

The criteria based on the operational needs are mainly defined by determining the minimum information and controls required to execute paper-based Emergency Operating Procedures (EOP). Even in this case the minimum staffing of one RO and one SRO is considered. The safety VDUs provides means to monitor safety parameters and controls of all of the safety components.

The Limiting Condition for Operation (LCO) is defined as follows:

Condition 1: Maintain present conditions and monitor and maintain critical safety functions by safety VDU and repair failures within 12 hours.
This condition is preferred because it avoids a forced shutdown plant transient under degraded HSI conditions. However, the ability to maintain this condition is largely based on the operability of the plant's non-safety control systems. If the failure only affects the non-safety HSI, it is likely the plant control systems will remain operable and will continue to control the plant in automatic modes. If the failure also affects the non-safety control systems, it is likely that a forced shutdown will be required.

Condition 2: If condition 1 is not satisfied, the plant is shutdown, and maintained in a hot stand-by state by safety VDUs (using only safety plant systems) and repair failures within 72 hours.

Condition 3: If condition 2 is not satisfied, the plant is moved to and maintained in a cold shutdown condition by safety VDUs (using only safety plant systems).

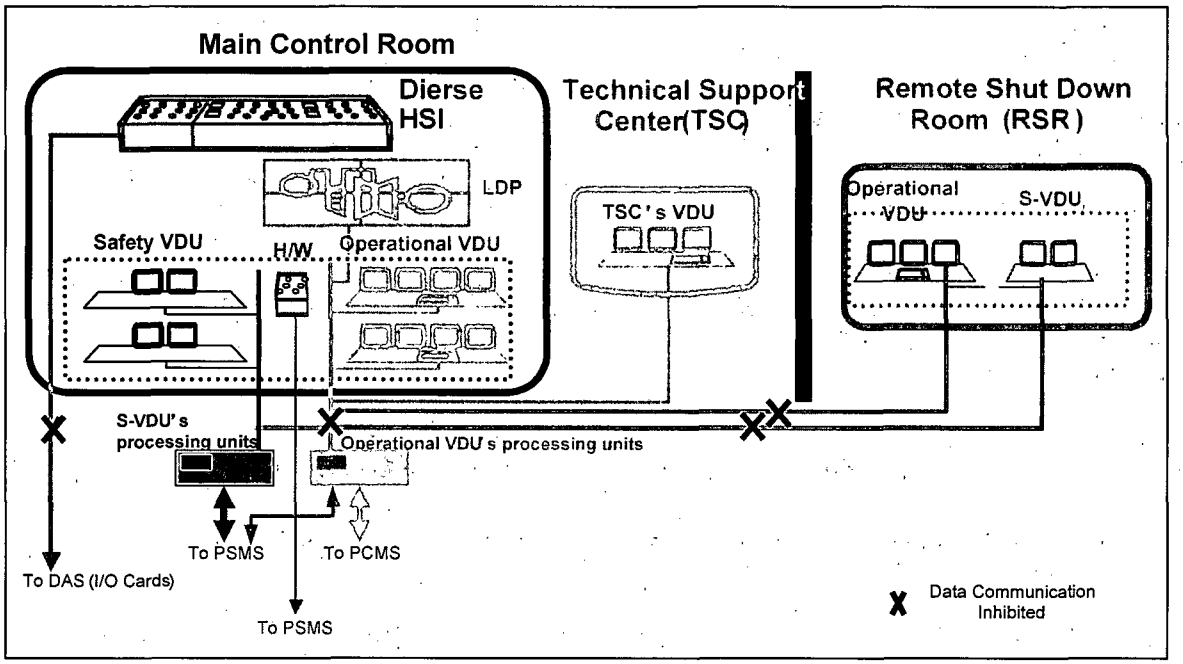


Figure 4.11-3 Configurations in Case of Operational VDU Loss

The appropriateness of the operator staffing of one Reactor Operator (RO) and one Senior Reactor Operator (SRO) under these degraded HSI conditions is confirmed by task analysis and by static and dynamic V&V by operators. Additional operators that are available at the plant are utilized as needed.

4.11.4 Loss of All Digital Non-safety and Safety HSI (CCF)

If all digitalized I&C including HSI related processors is lost, the operation of the plant is transferred to the DAS HSI Panel (DHP). The MCR and the RSS are not allowed to send orders to the process. The switch of control mean is governed by a procedure.
The following functions are maintained by the DHP, as a minimum:

- Reactivity Control
- RCS Inventory
- Core Cooling
- Secondary Heat Sink
- RCS Integrity
- Containment Integrity

The control and monitoring means for the DHP are provided as hard wired switches and indicators. It ensures the diversity to the other digital HSI systems.
The configuration and system architecture are described in the Defense in Depth and Diversity (D3) Topical Report.

The Limiting Condition for Operation (LCO) is defined as follows:

The plant is shutdown, and maintained in a hot stand-by state by the DHP (using all available, but primarily plant safety systems) and repair failures. The DHP does not provide the capability to transition to cold shutdown.

The D3 Coping Analysis also demonstrates the ability to cope with Anticipated Operational Occurrences and Postulated Accidents under this CCF condition. The operator actions credited in this coping analysis are executed from the DHP. These actions are encompassed and evaluated through the HFE design process described in section 5.

The appropriateness of the operator staffing of one Reactor Operator (RO) and one Senior Reactor Operator (SRO) under these degraded HSI conditions is confirmed by task analysis and by static and dynamic V&V by operators. Additional operators that are available at the plant are utilized as needed.

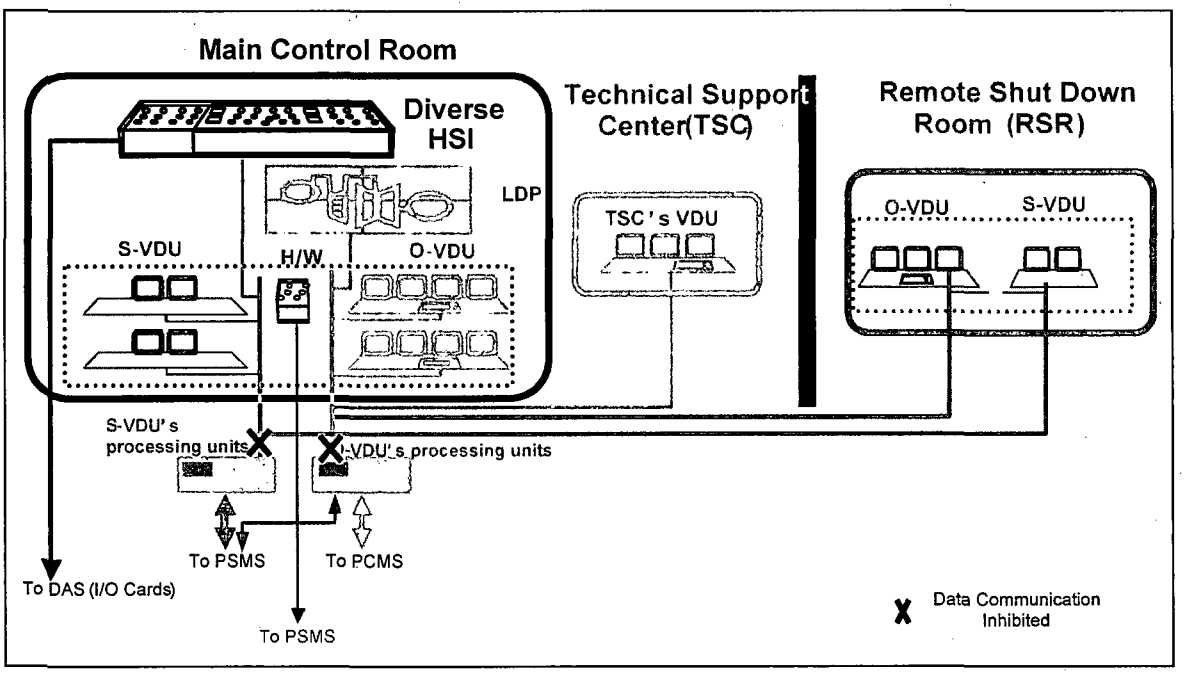


Figure 4.11-4 Configurations in Case of CCF

4.11.5 Loss of MCR

In this configuration, the main control room must be evacuated due to undefined reasons or due to fire. Initially any degradation to HSI equipment is limited to only one safety or non-safety division due to separation and independence of divisions in the MCR. However, ultimately it is assumed that the fire damages all MCR HSI equipment. Therefore the operation of the plant is transferred to the remote shutdown room (RSR) where the plant is brought and maintained to a safe shutdown condition.

Before leaving the MCR, the shift team performs preliminary actions like tripping the reactor. However, if time permits reactor trip is not executed until the RSR is manned. This avoids creating a plant transient that cannot be monitored. Once operators arrive in the RSR, the MCR control means are isolated from the process so that they are not allowed to send orders (but the RSS is). This transfer is governed by an operating procedure. Since all MCR HSI

functionality is available at the RSR (i.e., all safety and non-safety divisions) there is no need for evaluation of display, alarm or control availability.

The appropriateness of the minimum operator staffing of one RO and one SRO is confirmed by analytic validation of the task analysis and the static and integrated V&V by operators.

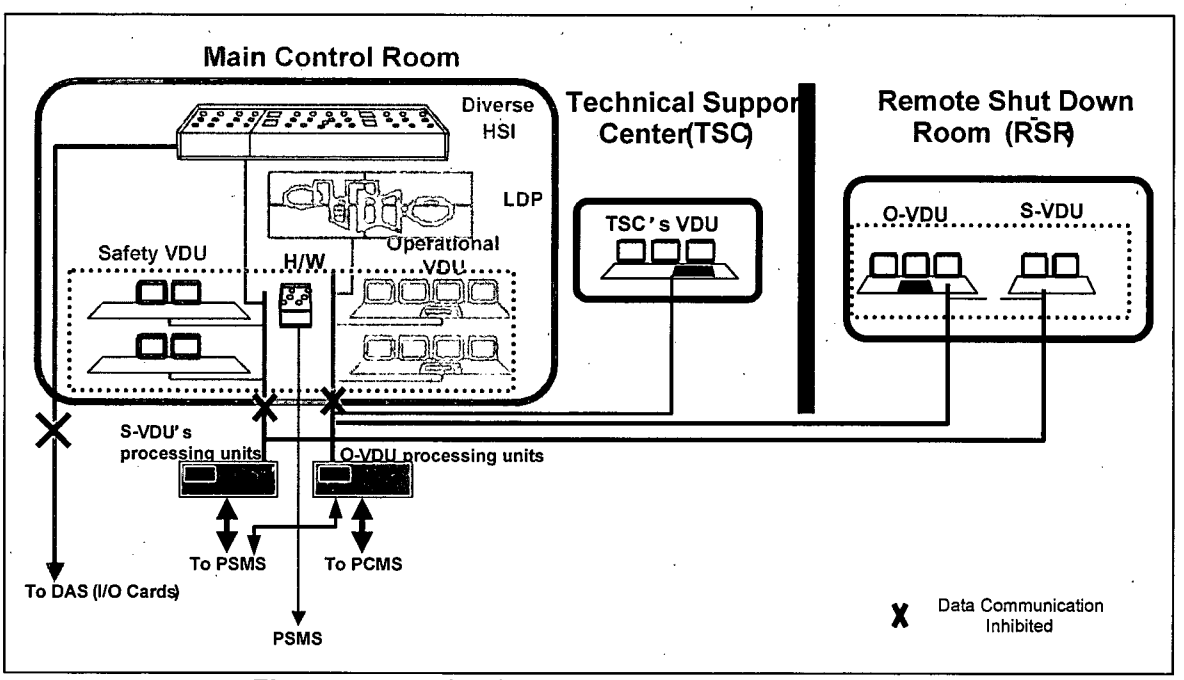


Figure 4.11-5 Configurations in Case of MCR Loss

4.12 Key Technical Issues

This section summarizes the key HSI related technical issues.

a. Multi-channel operator stations

For all plant conditions, including DBA and safe shutdown, the primary operator interface is provided by

- Non-safety Multi-channel LDP
  - SDCV information and alarms significant to safety and power production
- Non-Safety Multi-channel VDUs
  - Selectable interface for all other information, alarms and controls
- Conventional Class 1E switches
  - SDCV controls for system level actuation of safety functions

Safety VDUs provide back-up Class 1E information and control for all safety functions. And also provides SDCV monitoring function for Post Accident Monitoring parameters.

Non-safety multi-channel HSI allows the operator interface to match the integration of safety and non-safety functions that exist in plant systems and to utilize those systems in an integrated manner to maintain plant functions. The non-safety multi-channel HSI is developed under the HFE Program and with a software development process that ensures suitable quality for use during all normal and abnormal plant conditions.

b. HSI to accommodate reduced operator staffing

Integrated safety and non-safety functions on the Multi-channel LDP and VDUs provide the following benefits:

- Continuous awareness of critical safety functions while immediate focus may be plant maneuvering and power production.
- A single operator can execute procedures that involve multiple safety divisions and non-safety systems, simplifying task coordination for maintaining a single safety function.
- Operators can execute computer based procedures with integrated information and controls and/or hyperlinks.

It minimizes operator transitions between safety and non-safety VDUs, thereby reducing operator workload during critical plant situations.

The benefits reduce operator task burden, reduce potential for human error, and facilitate reduced MCR operator staffing.

The minimum staffing of one SRO and one RO in the MCR and one additional SRO and RO at the plant, meets the staffing requirements of 10CFR50.54. This minimum staffing is validated for normal operation and all degraded HSI conditions.

c. Operation under Degraded Conditions

The HSIS accommodates the following degraded HSI conditions:

- Degraded HSI systems by single failure
- Loss of all non-safety HSI
- Loss of all digital non-safety and safety HSI (Common cause failure (CCF))
- Loss of MCR

The HFE Program validates operation under these degraded conditions with the minimum plant staff.

d. Minimum inventory of HSI

The fixed area of LDP presents SDCV information to the operating staff. The parameters and alarms on the LDP are described in section 4.9, including SDCV indications for BISI of RPS, ESFAS and plant safety systems.

Means are provided in the MCR for manual initiation of protective functions at the system level. These functions are realized by conventional hard-wired Class 1E switches that enable easy and prompt access by the operator. Means for manual control of safety systems at the component level are realized by the safety VDUs described in section 4.6.

The minimum SDCV inventory and the minimum inventory for degraded HSI conditions are established to monitor and control the six critical safety functions:

- Reactivity Control
- RCS Inventory
- Core Cooling
- Secondary Heat Sink
- RCS Integrity
- Containment Integrity

This applies to all normal and emergency plant modes. The specific functions and tasks and the key required HSI resources, including alarms, controls, displays and procedures, are extracted from Normal Operating Procedures, Emergency Operating Procedure (EOP) and Plant probabilistic risk assessment (PRA), which are described in plant licensing documents. The minimum inventory is based on monitoring key performance parameters for each critical function and controlling the preferred non-safety and safety success paths. The design of the minimum inventory HSI is developed and evaluated through the HFE design process described in section 5.

There is no specific process for identifying the minimum Class 1E HSI inventory. This is because Class 1E HSI is provided for all Class 1E instrumentation and plant components via Safety VDUs.

e. Computer based procedures

In addition to the display Navigation system for HSI, the computer based operating procedure VDU is provided. It enables operators to perform certain and reliable operations.
The computer based procedures (CBP) are developed under the HFE Program and with a software development process that ensures suitable quality for use during all normal and abnormal plant conditions. The change process defined for CBP maintains the original quality while reducing the maintenance burden to a manageable level.

5.0 HFE DESIGN PROCESS

The HFE design process described in this section is applicable in its entirety to the US-APWR. The applicability to operating plants is dependent on the scope of the HSI upgrade. For operating plant upgrades Plant Licensing Documentation identifies the specific sections of this document that are applied and any deviations from the methods described in this report.

This section describes the generic HFE design process. Any portions of the HFE design process that are not complete for a specific plant and therefore may require future commitments, such as Design Acceptance Criteria or licensing conditions for operating plants, are described in Plant Licensing Documentation.

5.1 Human Factors Engineering Program management

The overall goal of the HFE program management is to ensure the HSI system reflects the latest human factor principles and satisfies all of the required regulatory requirements. In addition, the goal is to define the means by which HFE activities are executed.

5.1.1 Human Factors Engineering Program

5.1.1.1 Human Factors Engineering Program Goals

The general objectives of the HFE Program are stated in "human centered" terms, which, as the HFE Program develop, are defined and used as a basis for HFE test and evaluation activities. The Human Factors Engineering Program goals include the following:

- Personal tasks are accomplished within the required time and in accordance with specified performance criteria
- The HSIs, procedures, staffing/qualifications, training and management and organizational support results in a high degree of operating crew awareness of plant conditions.
- The plant design and allocation of functions maintains operational vigilance and provides acceptable workload levels to minimize periods of operator underload and overload.
- The operator interfaces minimize operator error and provide for error detection and recovery capability.

5.1.1.2 Assumptions and Constraints

An assumption or constraint is an input to the HFE program. The design assumptions and constraints are following:

- Program must conform to regulations and rules related to safety and human factors design.
- Program must meet the requirements of utility operators. For this purpose, functional requirements analysis and function allocation are processed by the method described in Section 5.4., verification of the function allocation is conducted by the task analysis method described in Section 5.4, and validation of the HSI design is ultimately evaluated by the

verification and validation method described in Section 5.10.

- Human system interface requirements are to be met the plant system of the US-APWR and operating plants.
- State-of-the-art human factors practices and computer technologies must be utilized. However, hardware restrictions are taken into account in the human system interface design.

The detail design HFE implementation plan is described in Section 5.11.

5.1.1.3 Applicable Facilities

The description of the applicable facilities is implemented in section 4.2.

5.1.1.4 Applicable HSIs, Procedures and Training

The applicable HSIs, procedures, and training for the HFE Program is comprise all operations, accident management, maintenance, test, inspection and surveillance interfaces (including procedures).

5.1.1.5 Applicable Plant Personnel included in HFE Program

The description of the Plant Personnel in HFE Program is implemented in section 4.1.

5.1.2 Human Factors Engineering Design Team and Organization

5.1.2.1 Organization

The organizational structure to control the Human Factors Engineering is shown in Fig. 5.1-1.

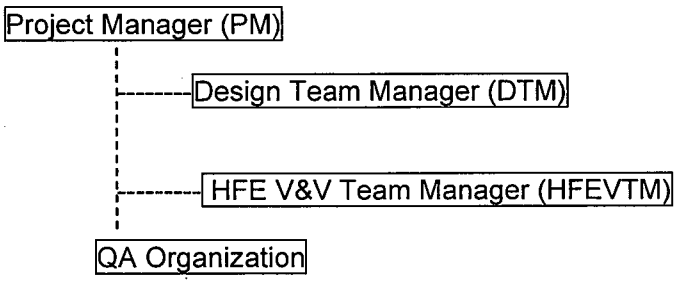


Figure 5.1-1 Organization of HFE Design Team

5.1.2.2 Roles and Responsibilities

The roles and responsibilities for the key sections of the organization are described in this section.

1) Project Manager (PM)
   The PM assures that process of design, V&V and quality assurance is appropriately implemented in accordance with the HFE Implementation Plan.

2) Design Team Manager (DTM)
The Design Team conducts all design activities for hardware and software. The DTM assures that the design team correctly performs the design based on the technical requirements and the development process in accordance with the HFE Implementation Plan. The DTM is also responsible for

- Initiation, recommendation, and provision of solutions for problems identified in the implementation of the HFE activities
- Verification of the effectiveness of the solutions provided to problems
- Assurance that HFE activities comply with HFE plans and procedures
- Phasing of activities
- Methods for identification, closure, and documentation of human factors issues
- HSI design and HFE documentation configuration controls

The HFE Design Team holds the following technical skills.

- Human Factors Engineering
- Systems Engineering
- Nuclear Engineering
- Instrumentation and Control (I&C) Engineering
- Architect Engineering
- Plant Operations
- Computer System Engineering
- Plant Procedure Development
- Personnel Training
- Systems Safety Engineering
- Maintainability/Inspectability Engineering
- Reliability/Availability Engineering

3) HFE V&V Team Manager (HFEVTM)
The V&V team conducts the HFE Verifications and Validations in accordance with the HFE V&V Implementation Plan.
The V&V Team Manager is responsible for all activities of the V&V Team. HFEVTM has sufficient resources (budget, staff, etc.) and authorities to ensure V&V activities are not adversely affected by commercial and schedule pressures.
The V&V team holds following technical skills:

- plant operation and operator training
- Human System Interface design
- Human factor engineering

The V&V Team has technical competence equivalent to the Design team.

4) QA Organization
The QA organization conducts the quality assurance in accordance with the Quality Assurance Plan which includes conformance of the suppliers' overall QA program.

5.1.3 Human Factors Engineering Processes and Procedures

a. General Process Procedures

The process through which the HFE Design team executes its responsibilities is depicted in Figure 5.1-2.

- The HFE Design team manager is responsible for assigning HFE activities to individual team members, governing the internal management of the team, and making management decisions regarding HFE.
- HSI design is made and prepared by the HFE design team and the answers to the comments on the design are approved by the HFE Design team manager.
- Equipment design changes are conducted using the Review record sheet in accordance with the process flow shown in Figure 5.1-1.
- Design team review of HFE products is conducted in accordance with the process flow shown in Figure 5.1-1.

b. Process Management Tools

The HFE Design team uses "Review Record Sheet" to implement the HFE review process. An example of the HFE review form attached to the Review Record Sheet is shown in Table 5.1-1.

c. Integration of HFE and Other Plant Design Activities

The inputs from other plant design activities to the HFE Program and the outputs from the HFE Program to other plant design areas are extracted and summarized in discrepancy reports before the open review committee meeting. These results are reviewed in the review committee meetings. The review committee meetings are held concurrently with the design process described in Figure 5.1-3.

d. HFE Program Milestones

HFE Program Milestones are shown in Figure 5.1-3. A relative schedule of HFE tasks showing relationships between HFE elements and activities, products, and reviews is also shown in Figure 5.1-3.

e. HFE Documentation

Deviations from the evaluation criteria derived from functional requirements and/or other input documents, are documented and rated for severity in terms of their potential effect on performance of the HSI system.

f. Subcontractor HFE Efforts

The HFE Team confirms that HFE requirements are included in each subcontract. The subcontractor's compliance with HFE requirements are periodically verified by review of the subcontractor's HMI design and manufacturing guidelines by the HFE Team.

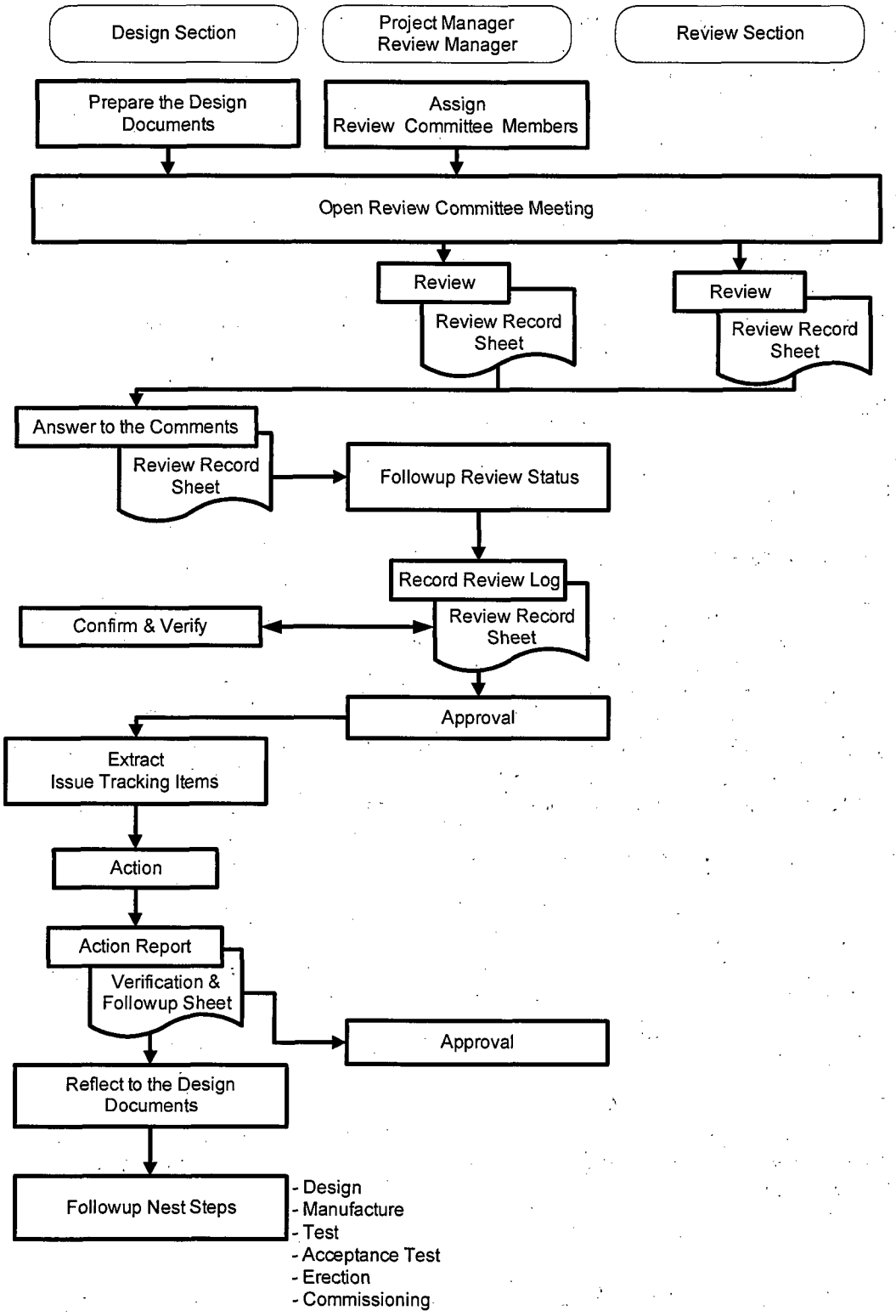


Figure 5.1-2 General Process Procedure of HFE Design

Table 5.1-1 Example of Comment Sheet in Review Process

				Date	Document
Review Items	**Clause/ Subclause**	**Paragraph Figure/ Table**	**Type of comment** (General/ Technical/ Editorial)	**COMMENTS**	**Answer to the comments**

5.1.4 Human Factors Engineering Issues Tracking

The HFE Issues Tracking System is the same as tracking system used for the rest of the design effort of the US-APWR. It is available to address human factors issues that are either (a) known to the industry or (b) identified throughout the HFE design, development, and evaluation process.

- HFE Design Team members are responsible for issue logging, tracking and resolution, and resolution acceptance.
- Each issue or concern that meets or exceeds the threshold of significance established by the design team is entered into the system when first identified.
- Each action taken to eliminate or minimize the issue or concern is thoroughly documented. The final resolution of the issue is documented in detail, as is the design team's acceptance of the resolution.

5.1.5 Human Factors Engineering Technical Program and Milestones

The HSI design implementation activities include the development of static and dynamic models for evaluating the overall plant response as well as the performance of individual control systems, including operator actions. The dynamic models are used to:

- Analyze steady state and transient behavior,
- Confirm the design of the advanced alarm system concepts,
- Confirm the adequacy of control schemes,
- Confirm the allocation of control functions to a system or an operator,
- Develop and validate plant operating procedures, and
- Incorporate as effectively as possible, into the plant design the utilization of full scope or limited use simulators.

Using part-task simulation an initial set of plant systems is identified through modeling, including the development of the graphical user interfaces (GUI). The part-task simulator is used in the preliminary US-APWR design and expanded to include US-APWR –unique design features. As the US-APWR design progresses, the part-task simulator proceeds through a series of iterative evaluations resulting in the development of a complete control room full scope simulator. In addition, the simulator facility is the focal point for operator evaluations and feedback checkpoints throughout the HSIS design process.

The general development of the following eleven key implementation plans, analysis, and evaluations is identified and described in Figure 5.1-3.

- Operating experience review
- Functional requirements analysis and function allocation
- Task analysis
- Staffing and qualifications
- Human reliability analysis
- HSI design

- Procedure design
- Training design
- Human factors verification and validation
- Design implementation
- Human performance monitoring

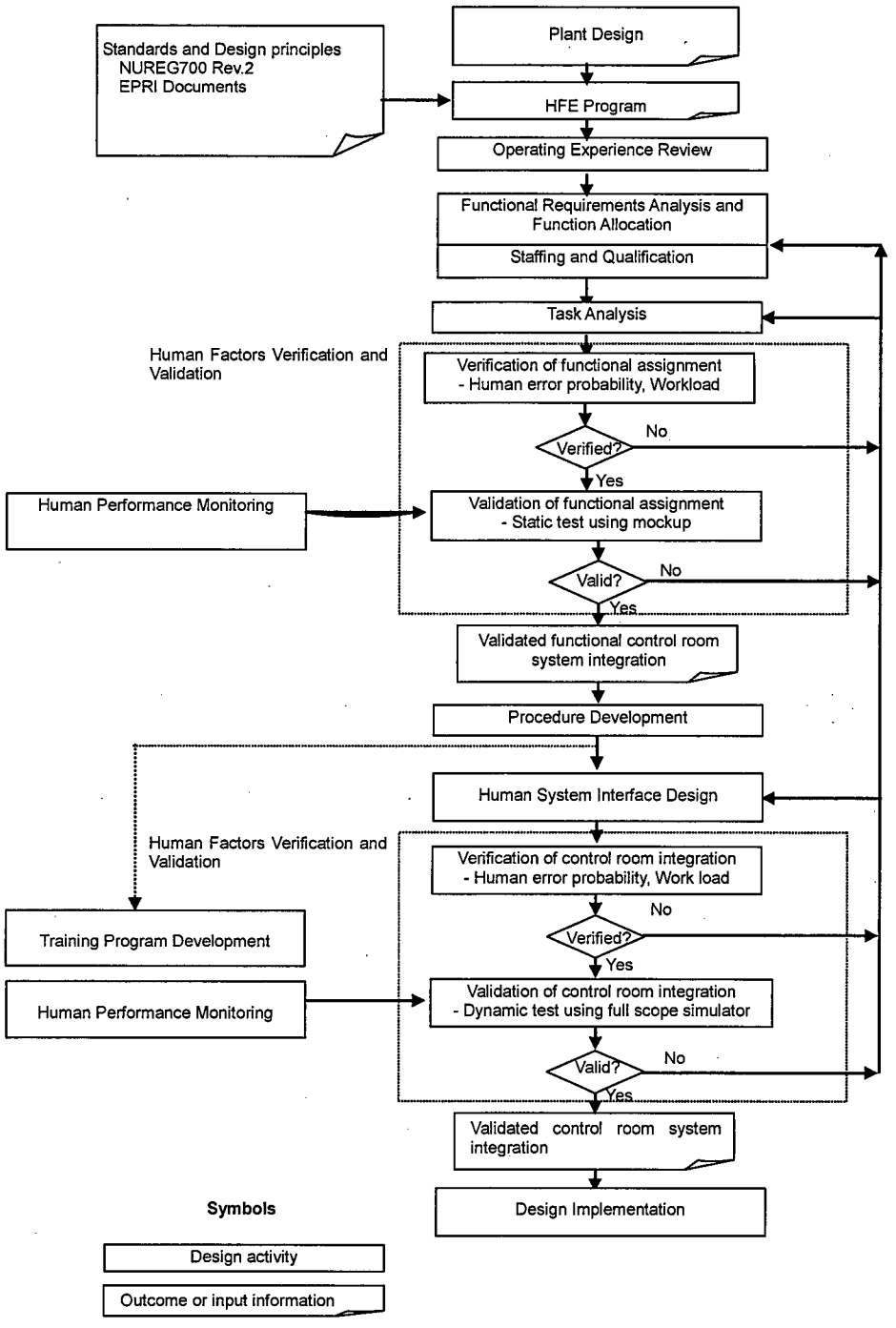


Figure 5.1-3 Overall Design Process

5.2 Operating Experience Review (OER)

The main purpose of the operating experience review is to identify HFE-related safety issues that arose in previous designs. HFE-related issues are extracted from the past commissioning and operating experience and are addressed in the new design.
OER information sources include NUREGs, Nuclear industries reports (e.g., INPO, LER) and Utilities operator's interviews.

The OER implements the following process:

- Extracting and screening HFE-related issues to identify those relevant to the MHI HSI System. Brief explanations are provided for issues considered not relevant.
- Relevant issues are evaluated. Explanations are provided for issues that are already accommodated in the HSI design. It is noted that the HSI design is still evolving at this point, so the evaluation considers the design only as it is defined in documentation at the time of the OER (i.e., anticipated design features that are not currently documented are assumed not to exist at the time of this evaluation). Issues not accommodated in the current HSI design documentation are added to the HFE Issues Tracking System for further resolution.
- Conducting the HFE issues resolution process.

MHI has examined and addressed the issues and causes of the events in the past commissioning and/or the present operating plants, both domestic and overseas, and improved the in-service plant facilities and the construction plant designs if necessary in order to avoid the issue again.

Table 5.2-1 shows the example of the OER analysis.

Table 5.2-1 Example of OER Analysis

Control Number	Prepared	Source Number	Plant	Issue Date	System	Components	Subject	Abstruct	Situation	Contributing Factors	Corrective Actions	Status	Analysis of Countermeasures for the Domestic plants
2006-12-0204	-	NRC Information Notice 2006-18	FORSMARK 1 (AA/BWR/SWEDEN)	2006/07/25	Electrical system	Emergency Battery	The loss of two of the four trains of safety-related AC and DC power due to a common mode failure	The event occured in the 400 kV switchyard to support maintenance. During the maitenace, a short circuit in the switchyard led to the loss of two of the four trains of safety-related alternating current(AC) and direct current(DC) power due to a common mode failure. The events is significant in that it could have caused the common mode failure in all four trains and therefore, could have resulted in the loss of all hour trains of safety-related AC and DC power The Swedish Nuclear Power Inspectorate categorized the event under the International Nulear Event Scale (INES) as a level 2 event.	The event began when an arc and a two phase short circuit occurred when a breaker was opened in the 400 kV switchyard to support maintenance.The electrical transient dropped the voltage to about 30 percent of nominal voltage and the unit was disconnected from the grid. In adition, the electrical transient caused a brief increase in voltage on the main generator. This sudden overvoltage caused two of the four electrical inverters to fail and consequently disabled two emergency diesel generators(EDGs) from powering the corresponding buses as expected. The reactor successfully scrammed and all control rods inserted. The control room staff were challenged by the absence of control room indications associated with the two trains of power supply that were lost. The event was further complicated by the actuation of the containment spray and emergency cooling systems. After restoring power, the operators were able to secure the containment spray and emergency cooling sysytems.	Based on the INPO reports which was attched blow. ...	Based on the INPO reports which was attched blow. ...	N2	In domestic plant, the same event does not occure as the following reasons; a. Switch gear shall not be opened during applying currency by interlock logics. b. The safety inverter shall not be tripped caused by the overvoltage. c. Generator shall be tripped by Turbine trip instead of low freqency signal. d. Safety voltage line shall be automatically supplied by a backup power source.
2006-12-0216													

5.3 Functional Requirements Analysis and Function Allocation

Functional requirements analysis is the identification of functions that must be performed to satisfy plant safety objectives. Functional allocation is the analysis of the requirements for plant control and the assignment of control functions to
Personnel (e.g., manual control)
System elements (e.g., automatic control and passive, self-controlling phenomena)

- Combinations of personnel and system elements (e.g., shared control and automatic systems with manual backup)

Since this is an evolutionary plant, the functions and allocations are based primarily on historical practices, except as may be necessary to accommodate:

- Issues identified in the OER
- Reduced operator staffing
- New functions for the US-APWR that were not in previous plants
- Functions that are changed significantly by the use of digital technology

Therefore the focus of this HFE effort is to identify any changes from historical practices (i.e., a detailed evaluation of unchanged practices is not be conducted).

The key function allocation changes of the US-APWR are followings;

- An automatic isolation of the broken SG.
- Elimination of recirculation of ECCS

Other detailed allocation changes are described in the Plant Licensing Documents.

5.3.1 Functional Requirements Analysis

Functional requirements analysis is the identification of functions that must be performed to satisfy plant safety objectives. A functional requirements analysis is conducted to;

- Determine the objectives, performance requirements, and constraints of the design,
- Define the high-level functions that have to be accomplished to meet the objectives and desired performance
- Define the relationships between high-level functions and plant systems(e.g., plant configurations or success paths) responsible for performing the functions
- Provide a framework understanding the role of controllers(whether personnel or system) for controlling the plant

Figure 5.3-1 shows the hierarchical structure of the plant's functions that is performed to satisfy conventional plant safety objectives. The top hierarchical level (Critical Safety Function level) shows essential functions for the plant safety. The lower level (Event level) shows the specific emergency and accident events that are caused to affect each plant safety function. The component level shows the components that cause to affect each accident event and safety function.

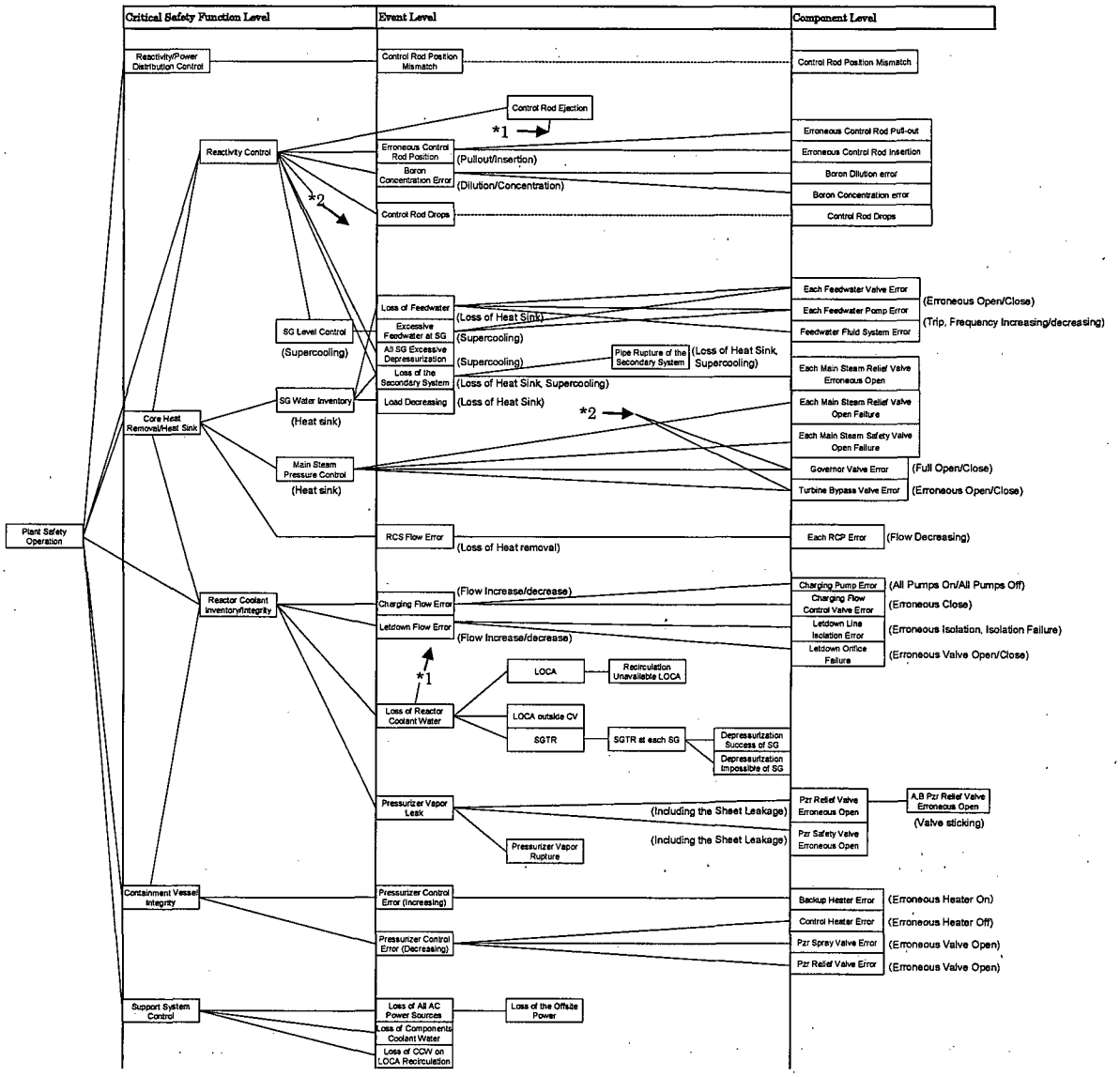


Figure 5.3-1 Hierarchical Structure of Safety Plant Functions

5.3.2 Function Allocation

The operator is ultimately responsible for the safe operation of the plant. Therefore automation is a tool applied to aid the operator, not replace the operator. Automation is applied only when it results in clear and distinct operational or efficiency advantages, and there is no adverse effect on human performance to support plant safety or availability.

The following two main automation rules apply:

- automated sequences have to help the operator to eliminate certain operating tasks provided that:
  - those tasks are not necessary in order for the shift operating team to maintain its knowledge of the plant situation or to build itself a comprehensive representation of that situation;
  - technological and economical objectives of sequence automation are met.
- automation of sequences has to foster co-operation between the shift operating team and the I&C designers. It is therefore necessary to inform the shift operating team of the reason, meaning, achievement, and progress of the actions performed by the I&C system.

Those rules aim at enabling the operator to stay in control of the automation installation in order to address:

- those situations that the automated sequences cannot handle completely or in an optimal way
- the malfunction or erroneous of automated sequences, which is handled by enabling a detection of faults and by limiting the risk of error following a manual recovery.

Therefore, the shift team needs to keep its knowledge on the system behavior up-to-date and needs current HSI functions (dialogues, information displaying, and controls) and documentation.
Automation is implemented according to predefined general criteria which dictate that significant improvement be identified in plant safety, availability and economics.

5.3.2.1 General Rules

The following tasks, contributing to the previous objectives, are automated regardless of the status of the plant:

- tasks requiring a quick or highly reliable reaction:
  - actions credited for beyond design basis events prior to 10 minutes are generally automated. This criterion is based on the Defense-in-depth and diversity (D3) coping analysis. The thermal hydraulic portion of the D3 analysis determines the time available for operator action. The HFE portion of this analysis ensures that manual action within this time can be reasonably expected without human performance errors. In general, experience has shown that actions required after 10 minutes can be justified based on the HFE portion of this analysis. However, any manual actions that cannot be justified by the HFE analysis will be automated.
  - an automatic checking system supports the operator's confirmation task and

operator's quick actions after automated systems are actuated.
- actions on components required within short time needed to ensure the plant availability in power operation, or to cope with transients not manageable by closed-loop controls
- tasks which directly influence plant availability (e.g., reduce the time for shutdown and start-up)
- tasks which increase safety by automatic actuation of safety systems

- monotonous and repetitive tasks, leading typically to high workload (if not automated) such as:

  - continuous control of process state variables
  - continuous set-point variations for closed loop control shall be automatic (on request by the operator)
  - start-up of standby components in the case of failures of the running component
  - tasks which have to be performed frequently during shutdown and start-up
- tasks requiring significant operator workload and attention, start-up and shutdown sequences of a main component or a group of components, notably if operator judgment is not needed
- tasks that can be conducted more frequently and accurately through automation, thereby improving plant safety or availability, checking parameters relative to thresholds, e.g., when changing a plant or system state stepwise, with several intermediate steps are supported by automation
- tasks which have to be performed frequently during shutdown and start-up
- tasks which have a long duration, particularly during shutdown and start-up, and therefore require a long duration of operator attention

The criterion above is used as a basis for identifying the minimum tasks that are allocated to automation. In addition, the allocation considers the reduced operating staffing for the US-APWR and for modernized plants, which includes only one SRO and one RO in the MCR as minimum. Therefore, in addition to the minimum level of automation, operator workload is carefully evaluated. Additional automation is generally applied to burdensome functions that do not contribute to an operator's skills in maintaining plant safety or availability. In applying additional automation, carefully consideration is given to automation hold points where operator assessment and judgment adds value to the reliability of the process and to the operator's awareness of the plant status.

5.3.2.2 Other Considerations

If line-up of mechanical systems is not considered to be on the critical path for plant start-up, there is no impact on plant operation, and there are no complicated links between the different line-up actions, the corresponding actions are generally not automated. Particular operating demands (Other case by case criteria for automation)

The following automation rules are also considered when they contribute to the previous stated objectives:

- the automation has to ensure that the plant can be operated by one RO in all plant situations without multiple failures/events
- automation may be appropriate for periodic tests configuration sequences
- automation may be appropriate to standardize frequently used sequences of

actions like normal/back-up switching of actuators
- automation may be appropriate to achieve adaptation of systems participating in load changes of the plant and needed within a short time span
- automation may be appropriate to perform functions required to change the plant state, failure of which would lead to complicated/time consuming recovery actions
- automation may be appropriate for functions required for change of plant load if manual execution would introduce an important delay in this change
- automation may be appropriate for functions needed to set up the parameters of the I&C system for stretch-out operation.

5.3.2.3 Taking into Account Operating Experience Review

If most of the plant systems are already designed, stringent automation criteria may induce modifications of the plant systems design. In that situation, case by case review of the plant systems is necessary to ensure that operating experience is incorporated without major modification of the design. In practice, this consideration leads to sticking to existing automation level and modifying it only if strictly necessary in accordance with the experience feedback.

In order to comply strictly with the IEC60964 standard Section 3, the analysis of the sequences to be automated still has to be performed and justified even if they are based on the proven solution of existing plants. Therefore, the criteria listed above are valuable to do this task even if they are not necessarily of a great help to determine how to improve existing design (experience feedback is a much better improvement basis).

5.3.2.4 Priority Order Management for Automation

Adequate priorities between automatic and manual actions ensure that:

- simple erroneous manual actions cannot inhibit automatic plant protection actions, or automatic equipment protection actions;
- the operation staff has an appropriate time for decision making of manual control

The basic rules are:

- automatic plant protection actions and equipment protection actions have priority over manual actions;
- automatic plant protection actions can be blocked (prior to actuation) at the division level following administrative controls and plant technical specifications, and with appropriate bypass alarms and indications. Equipment protection actions cannot be blocked;
- after actuation automatic plant protection actions can be overridden at the component level by taking two deliberate manual actions. In general, equipment protection signals cannot be overridden. However, equipment protection signals that are normally expected due to process conditions (e.g., low tank level stopping a pump to prevent inadequate suction damage) may be overridden by manual signals that require continuous operator attention (e.g., pushing and holding a button continuously);
- automatic plant/equipment protection signals can be reset when the initiating condition is restored to normal or to an appropriate setpoint. Plant protection

signals require manual reset; equipment protection signals can be reset automatically. If the plant/equipment conditions degrade, the signals are automatically initiated again;

- manual actions have priority over closed and open loop process control functions;
- interlocks prevent manual actuation against prior automatic orders.

5.4 Task Analysis

5.4.1 Objective of Task Analysis

The functions allocated to plant personnel define their roles and responsibilities. Human actions (HAs) are performed to accomplish these functions. HAs are be further divided into tasks. A task is a group of related activities that have a common objective or goal. The objective of the task analysis is to identify requirements for accomplishing these tasks, i.e., for specifying the requirements for the displays, data processing, controls, and support aids needed to accomplish tasks. As such, the results of task analysis are identified as inputs in many HFE activities; e.g., it forms the basis for:

- staffing, qualifications, job design, and training
- HSIs, procedures, and training program design
- task support verification criteria definition

5.4.2 Scope of Task Analysis

The scope of task analysis includes:

- selected representative and important tasks that affect plant safety from the areas of operations, maintenance, test, inspection, and surveillance
- full range of plant operating modes, including startup, normal operations, abnormal and emergency operations, transient conditions, and low-power and shutdown conditions
- Has (Human Actions) that have been found to affect plant risk by means of probabilistic risk assessment (PRA) importance and sensitivity analyses should also be considered risk-important. Internal and external initiating events and actions affecting the PRA Level I and II analyses are considered when identifying risk-important actions
- where critical functions are automated, the analyses should consider all human tasks including monitoring of the automated system and execution of backup actions if the system fails.

The task analysis is iterative and becomes progressively more detailed over the design cycle. It is detailed enough to identify information and control requirements to enable specification of detailed requirements for alarms, displays, data processing, and controls for human task accomplishment.

The task analysis addresses issues such as:

- the number of crew members
- crew member skills
- allocation of monitoring and control tasks to the

  1) definition of meaningful jobs and

  2) management of crew member's physical and cognitive workload.

The task analysis results are used to define the set of alarms, displays, and controls necessary to perform crew tasks based on both task and instrumentation and control requirements. The task analysis results provide input to the design of HSIs, procedures, and personnel training programs.

5.4.3 Methodology for Task Analysis

Tasks are linked using operational sequence diagrams. Task analyses begin on a high level and involve the development of detailed narrative descriptions of what personnel have to do. The analyses define the nature of the input, process, and output needed by and of personnel. Detailed task descriptions address (as appropriate) the topics listed in Table 5.4-1

Table 5.4-1 Task Considerations

Type of Information	Example
Information Requirements	alarms and alerts parameters (units, precision, and accuracy) feedback needed to indicate adequacy of actions taken
Decision-making Requirements	decisions type (relative, absolute, probabilistic) evaluations to be performed
Response Requirements	type of action to be taken task frequency, tolerance and accuracy time available and temporal constraints (task ordering) physical position (stand, sit, squat, etc.) biomechanics - movements (lift, push, turn, pull, crank, etc.) - force needed
Communication Requirements	personnel communication for monitoring information or control
Workload	cognitive physical overlap of task requirements (serial vs. parallel task elements)
Task Support Requirements	special and protective clothing job aids or reference materials needed tools and equipment needed
Workplace Factors	ingress and egress paths to the worksite workspace envelope needed by action taken typical and extreme environmental conditions, such as lighting, temp, noise
Situational and Performance Shaping Factors	Stress reduced manning
Hazard Identification	identification of hazards involved, e.g., potential personal injury

Figure 5.4-1 shows the MHI approach to Task Analysis in the HFE process. The level of design detail is changed as the design progresses. High level Task Analysis is performed in the early design stage and detail level Task Analysis is performed in later design stage (after HSI Design and Procedure Development phase). Although detail level task analysis can be considered as a part of Human Factor V&V process, its methodology is described this section.

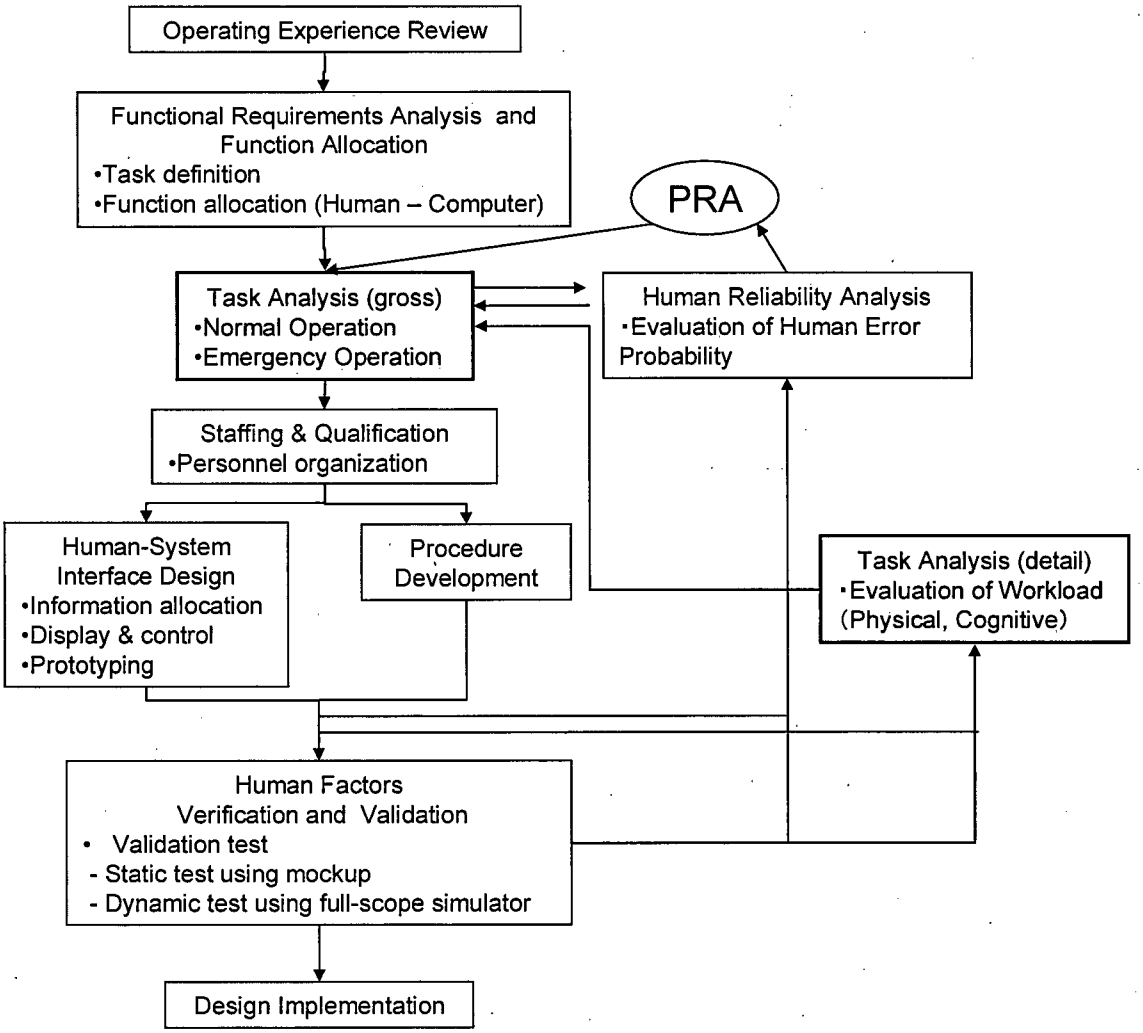
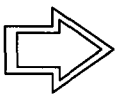
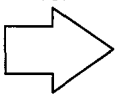
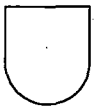
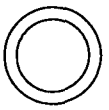
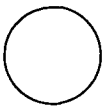
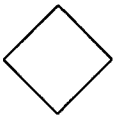
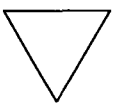


Figure 5.4-1 Task Analysis in HFE Process Flow

5.4.3.1 Method for Gross and Narrative Task Analysis Method

The operational sequence diagram (OSD) is analysis technique because it can be used from the initial design phase to the final design phase.

The OSD represents operator and computer tasks in graphical scheme sequentially. The symbols for OSD are shown in Figure 5.4-2. Through the use of symbols to indicate actions, data transmitted or received, inspections, operations, decisions and data storage, the OSD shows the flow of information through a task. The information flow is shown in relation to both time and space. If detailed information on a given action is needed, code letters (S, V, W, T) may be used to indicate the mode of actions. The OSD is used to develop and present the system reaction to specified inputs. In the OSD, the interrelationships between operators and equipment (including computers for human-machine interfaces) are easily displayed. Operator activities are sequentially categorized. Decision and action functions are clearly identified, and task frequency and load become obvious.

SHAPE			CODE	
MACHINE	HUMAN	ACTION	LETTER	MEANING
		Transmit	S	Sound
		Receipt	V	Visual
		Inspect	W	Walking
		Operate	T	Touch
		Decision		
		Storage		

* A code letter may indicate Mode of shapes

Figure 5.4-2 Symbols Used in Operational Sequence Diagram (OSD)

The OSD corresponding to each task is constructed by the following steps:

Step 1 : Description of task scenario
- Represent elements of task in simple linguistic form
- Select appropriate detail level in design phase

Step 2 : Breaking down job task into individual activities

Step 3 : Activity assignment to human and machine
- Use the result of Function Allocation
- Assign each activity to operator or machine

Step 4 : Description of activity sequence for functions assigned to operator

Table 5.4-2 shows an example of data entry in a Task Analysis Sheet which is used to record the analysis results. Fields in this table are described below:

- Operating Procedure Field: Full task contents are described in task sequence.
- OSD Description Field: Human and machine actions are represented using OSD symbols.
- Task Description Field: Key information of task execution such as plant parameter, alarm, control.
- Note Field: Remark for task execution.

An example of the OSD representation is shown in Table 5.4-2. In the column "OSD Task Description", the contents of task are described as activities in simple form. Activity description is broken down into individual actions (OSD symbols) such as 'Transmit', 'Receive', 'Inspect', etc. Each action is located in appropriate column (Human: supervisor reactor operator or reactor operator, Machine: displays and controls) according to the output of the Function Allocation process. Finally all actions are connected to each other to represent the temporal sequence of the elements of the task.

Task Analysis sheets are developed for the full range of plant operating modes, including startup, normal operations, abnormal and emergency operations, transient conditions, and low-power and shutdown conditions. Table 5.4-3 shows an example data form of Task Analysis Summary Sheet. Each task analysis result for plant operation mode is summarized in this format, and these sheets are used for the evaluation of human workload. Fields in Table 5.4-3 are described below.

- Activity Field: Description of the work activity for plant system (Primary Loop/Secondary Loop/Electric System)
- Communication, Monitoring, Decision, Operation Field: Number of each OSD actions (receive, transmit, operate, inspect)
- Parallel Monitoring Field: Number of plant parameters that are necessary to monitor simultaneously for execution of an activity.
- Parallel Operation Field: Number of operations that are executed simultaneously in an activity
- Necessary Time Field: Estimated execution time of an activity

Table 5.4-2 Example of Task Analysis Sheet

Operating Procedure Confirm ANN	OSD Description Supervisor Reactor Operator	Reactor Operator	Displays Controls	Other Personnel	Task Description	Note
1. ANN Occur 2. Confirm plant status 3. Report plant status from RO to SRO 4. Decide plant trip or not					Read ANN information Display plant parameters Communicate via voice Decide plant trip or not	

Table 5.4-3 Task Analysis Summary Sheet

Activity		Communication			Monitoring		Decision	Operation	Parallel Monitoring	Parallel Operation	Necessary Time
Primary Loop	Secondary Loop	S	S	○	○	□	◇	○			
1. Confirm ANN		2	1	0	1	2	1	0	0	0	Within 1 min
2. Recovery Operation		3	4	2	11	25	0	5	5	0	Within 10 min

5.4.3.2 Detailed level Task Analysis Method

In order to evaluate an operating crew member's cognitive workload, an interaction analysis between human and computer system is necessary. To analyze cognitive workload MHI uses human information processor model. In a detailed level task analysis phase, task scenarios which are selected in the gross level task analysis are analyzed by human information processor model. The OSD actions are broken down into their constituent components and are evaluated with HSI design information. The result of the task analysis is a set of quantitative metrics such as memory workload and processing time for each scenario. The task analysis is iterative and becomes progressively more detailed over the design cycle. It is detailed enough to identify information and control requirements to enable specification of detailed requirements for the HSI design.

Goals, operators, methods, and selection rules (GOMS) is a theory of the cognitive skills involved in human-computer tasks. Figure 5.4-3 shows a model for a human information processor. This method is described in the reference document "The Psychology of Human-Computer Interaction". It is based upon an information processing framework that assumes a number of different stages or types of memory (e.g., sensory store, working memory, long term memory) with separate perceptual, motor, and cognitive processing.

- Perception processor (tp : mean processing time = 100msec)
  - sensory input (audio & visual) and code information symbolically
  - output into audio & visual image storage (Working Memory)
- Cognition Processor (tc : mean processing time = 70msec)
  - input from Working Memory and Short Term Memory
  - access Long Term Memory to determine response
  - output response into Working Memory
- Motion Processor (tm : mean processing time = 70msec)
  - Input response from Working Memory
  - carry out response

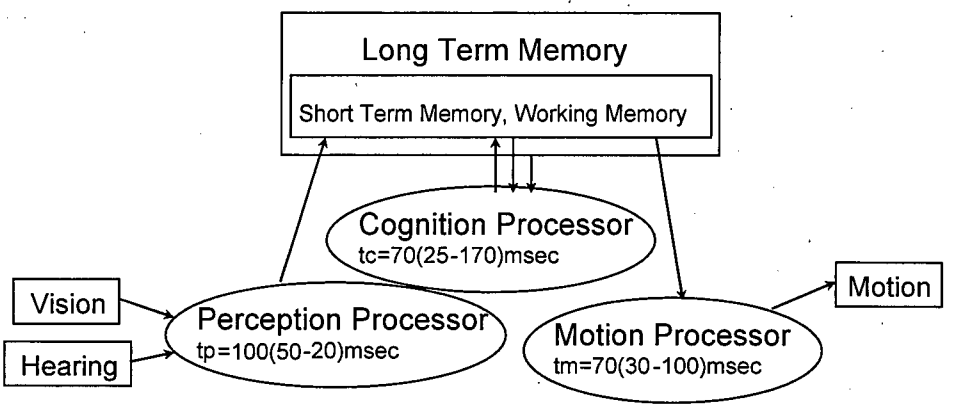


Figure 5.4-3 Model of Human Information Processor by Card et al.

Table 5.4-4 Extended Human Information Processing Model

Basic Action	Abbreviation	tp	tc	tm
simple reaction	sr	1	1	1
physical match	pm	1	2	1
name match	nm	1	3	1
class match	cm	1	4	1
move	mo	0	1	1
simple reaction without move	sr*	1	0	0
physical match without move	pm*	1	1	0
name match without move	nm*	1	2	0
class match without move	cm*	1	3	0
memory refer	mr	0	1	0

Human actions can be classified into several basic actions. Table 5.4-4 shows the relationship between basic actions and process times (tp, tc, tm). Card proposed four basic action types (simple reaction: sr, physical match: pm, name match: nm, class match: cm). MHI uses extended basic action is used to analyze VDU based monitoring and operation. Six basic actions (move: mo, simple reaction without move: sr*, physical match without move: pm*, name match without move: nm*, class match without move: cm*, memory refer: mr) are added to original basic actions. Total processing time for each basic action is calculated by using factor shown in Table 5.4-4. For example, typical processing time for a simple action (TP(sr)) is calculated as follows;

TP(sr) = 1*tp + 1*tc + 1*tm = 100 + 70 + 70 = 240 msec

Table 5.4-5 shows an example of Detail Task Analysis Sheet which is used to record analysis result. Fields in this table are described below.

- Step Field: Simple description of the task step
- Personnel Field: Who perform this step?
- Equipment Field: Which information device is used for this step?
- Operation Field: Description of task step is broken down into its constituent operations.
- Information Processing Type Field: GOMS basic action corresponding to each primitive operation.
- Cognitive Workload Field: Factors for information processing type

Selected scenarios are analyzed in this form, and quantitative metrics are gathered as detailed level analysis results. This information is used for evaluating the HSI design.

Table 5.4-5 Example of Detail Task Analysis (Workload) Sheet

Task Name: Safety Injection ANN Check							
STEP	Personel	Equipment	Operation	Information Processing Type	Cognitive Workload		
					tp	tc	tm
1. Confirm first out ANN	RO	Large Display	ANN occurrence(Confirm) Look at LDP Search first out ANN display Confirm first out ANN	pm* mo mr+pm* nm*	1 0 1 1	1 1 2 2	0 1 0 0
2. Confirm safety injection ANN	RO	Large Display	Search safety injection ANN displa Confirm safety injection ANN	mr+pm* nm*	1 1	2 2	0 0
3. Confirm reactor trip ANN	RO	Large Display	Search reactor trip ANN display Confirm reactor trip ANN	mr+pm* nm*	1 1	2 2	0 0
4. Confirm turbine trip ANN	RO	Large Display	Search turbine trip ANN display Confirm turbine trip ANN	mr+pm* nm*	1 1	2 2	0 0
					9	18	1

5.5 Staffing and Qualification Requirements

Final Staffing and Qualification requirements depend on the operating utility's applications, therefore it is a Combined License applicant responsibility.
In this section the minimum and maximum requirements for Operator Staffing and Qualification for US-APWR are described. This staffing is the basis for the HSI design and HFE analysis for the US-APWR. This staffing basis may also be applied to operating plants with an appropriate level of plant modernization. Staffing and analysis for modernized operating plants is described in Plant Licensing Documentation.

5.5.1 Operator Staffing Level

Operator staffing is based on the following three qualifications;

a. Senior Reactor Operator (SRO)

SROs are licensed pursuant to 10 CFR Part 55.54 "Operators".
Shift Supervisor (SS) is a licensed SRO and is responsible for the plant's operation for the duration of the shift.

b. Shift Technical Advisor (STA)

A degreed engineer who has fulfilled the course requirements and operator training requirements defined in NUREG-0737 TMI Action plan.

c. Reactor Operator (RO)

A RO is licensed pursuant to 10 CFR Part 55.54 "Operators".

5.5.2 Number of Operators per Shift

10 CFR 50.54(m) defines the minimum requirement of operator staffing is as follows;

- 1 SRO located within the MCR
- 1 SRO located at the plant
- 1 RO located at the controls of the plant in the MCR
- 1 RO located at the plant

In addition, NUREG-0737 requires one STA located at the plant. NUREG-0737 allows an SRO to also fulfill this requirement if the SRO also has an engineering degree with the appropriate course background.

Based on these requirements, the minimum operator staffing roles and responsibilities that are the basis for the US-APWR design are defined as follows.

- One RO at the controls of the plant within the MCR at all times. This RO is typically located at the Operator Console.
- At least one more RO present at the facility during its operation in order to shift above RO's temporary absence because of the meal time or sudden injury, etc. for redundancy and for abnormal conditions, including anticipated operational occurrences(AOOs), DBAs and

degraded HSI conditions discussed in Section 4 above. This RO can also be accommodated at the Operator Console, but continuous presence in the MCR is not required.

- One SRO within the MCR at all times. This is typically the control room supervisor. The SRO is typically located at the Supervisor Console.
- At least one more SRO present at the facility during its operation in order to shift above SRO's temporary absence because of the meal time or sudden injury, etc. for redundancy. This SRO position is typically fulfilled by the Shift Supervisor of the plant. This SRO is typically located in an office which is in close proximity to the MCR. For minimum staffing, this SRO also fulfils the STA requirement. However, a separate STA may also be designated. The HSI design accommodates the STA at a separate STA Console within the MCR.

The US-APWR is designed to be operated in normal operation by one SRO and one RO in the MCR. Other operating staffs available at the plant augment the minimum staff during abnormal plant conditions and degraded HSI conditions. The following activities have been demonstrated based on the above staffing basis:

- Task Analysis
- Human Reliability Analysis
- HSI design (including MCR layout)
- Verification and Validation

The minimum operator staffing structure is as following figure;

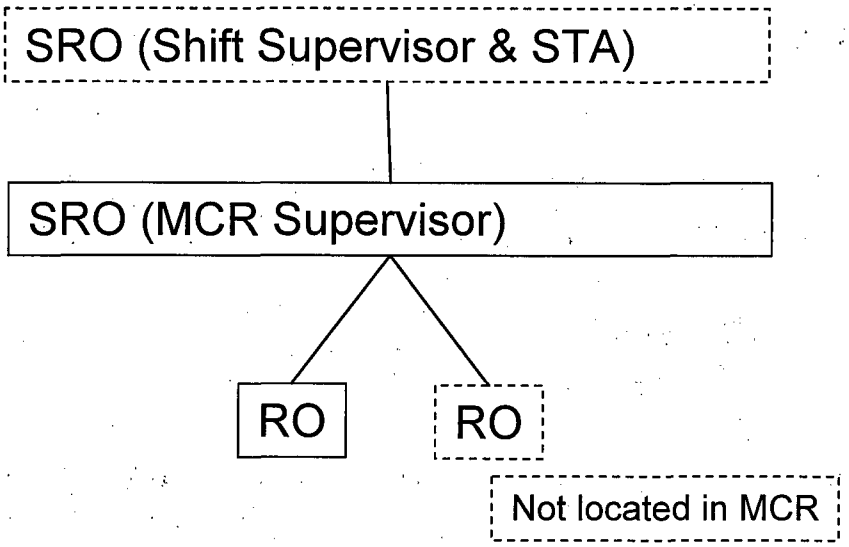


Figure 5.5-1 Operation Personnel Staffing and Organization (Minimum)

The HSI design of the US-APWR also accommodates other staffing structures, including the following maximum continuous staffing in the MCR.

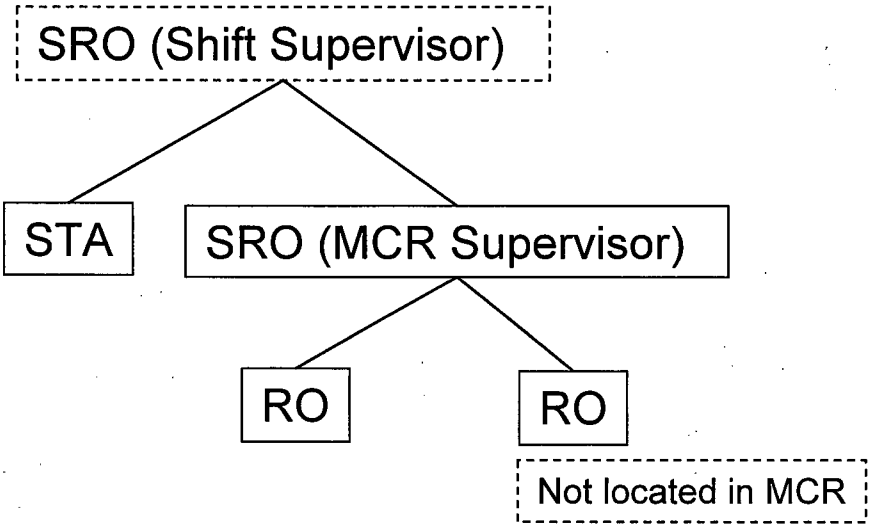


Figure 5.5-2 Operation Personnel Staffing and Organization (Typical)

5.6 Human Reliability Analysis

5.6.1 Objectives of HRA

Human reliability analysis (HRA) seeks to evaluate the potential for, and mechanisms of, human errors that may affect plant safety. Thus, it is an essential element in achieving the HFE design goal of providing a design that minimizes personnel errors, allows their detection, and provides recovery capability.

5.6.2 Scope of HRA

The HRA is conducted as an integrated activity to support both the HFE design and PRA activities. Figure 5.6-1 illustrates the relationship between the PRA/HRA and the rest of the HFE program, including the concept of performing an initial PRA/HRA and then a final one at completion of design. The quality of the HRA depends in large part on the analyst's understanding of personnel tasks, the information related to those tasks, and the factors that influence human performance of those tasks. The development of information to facilitate the understanding of the causes and modes of human error is an important human factors activity. The HRAs make use of descriptions and analyses of operator functions and tasks as well as the operational characteristics of HSIs. HRA can provide valuable insights into the desirable characteristics of the HSI design. Consequently, the HFE design gives special attention to those plant scenarios, risk-important human actions, and HSIs that have been identified by PRA/HRA as being important to plant safety and reliability.

The HRA is performed iteratively as the design progresses. The PRA and HRA are performed early in the design process to provide insights and guidance both for systems design and for HFE purposes. The robustness of the HRA depends, in large part, on the analyst's understanding of personnel tasks, the information related to them, and the factors which influence human performance. Accordingly, the HRA is carried out interactively as the design progresses.

As described in NUREG-1764, initial risk screening process is a part of PRA activities. Input information for HRA includes risk-important human action and result of task analysis process. Quantitative analysis of human errors is carried out using such input information from the cognitive viewpoint. If new risk-important human action is found in HRA, the feedback information is provided for PRA.

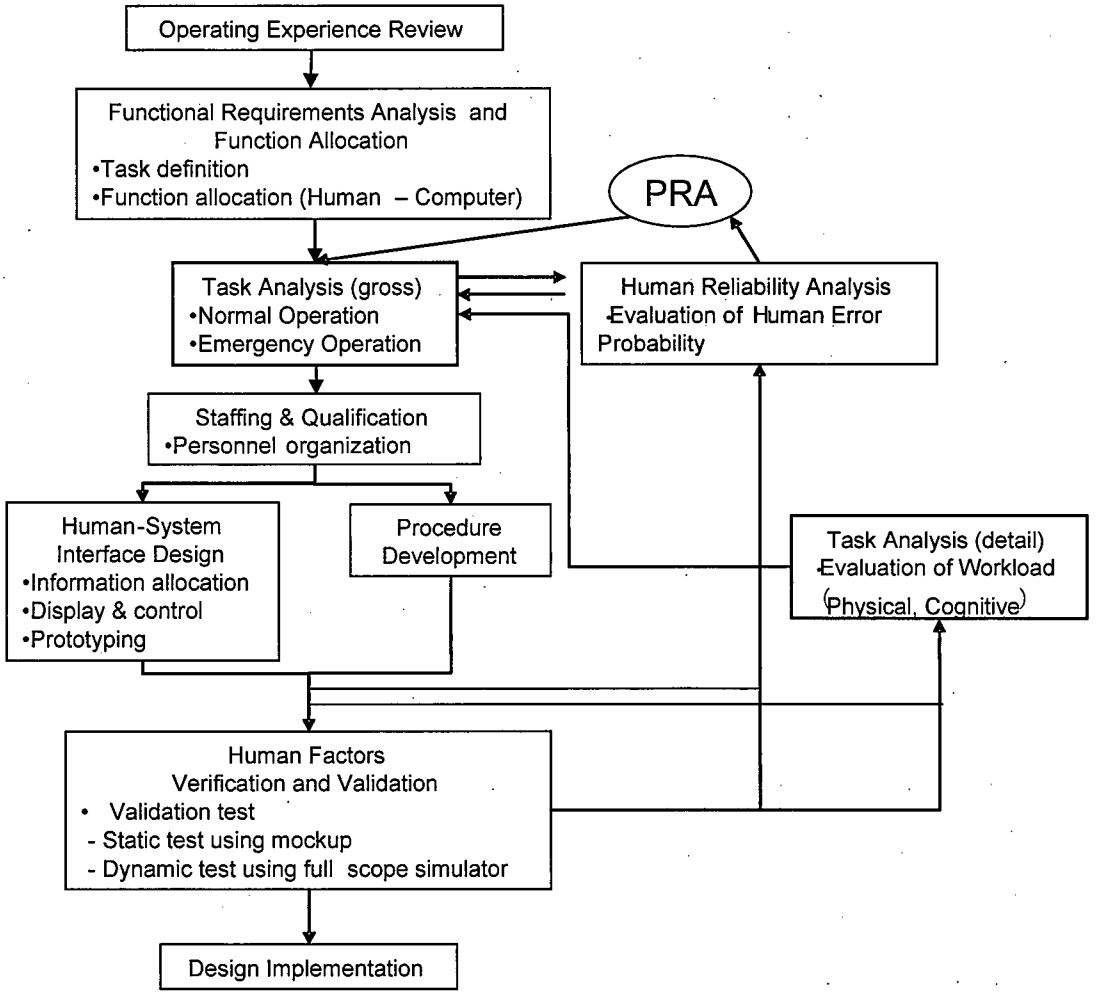


Figure 5.6-1 HRA in HFE Process Flow

5.6.3 HRA Methodology

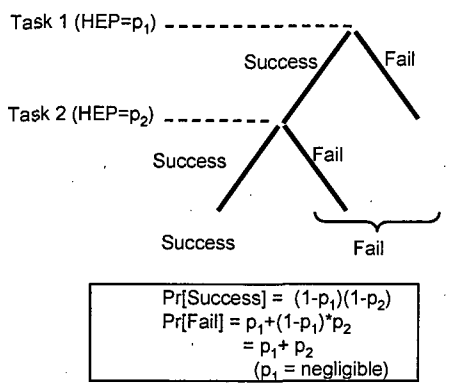
HRA has focused on omission of human error, but recent studies indicate that the analysis from the cognitive viewpoint is also important in preventing human errors, especially in some contexts where it affects the occurrence of commission errors. MHI uses the technique for human error rate prediction (THERP) for the analysis of human errors

THERP method was developed by Swain and Guttmann and documented as NUREG/CR-1278 in 1983. THERP method is used most widely for basic HRA. In the THERP handbook, the types of human error are summarized as data tables with standard occurrence probabilities assigned to each.

The fundamentals of THERP are shown in Figure 5.6-2. The procedure is divided into four fundamental steps. The first step is to investigate the objective task, divide it into detailed task

steps and form a success-fail binary tree, a so-called event tree. The second step is to select a corresponding basic human error probability (BHEP) from the associated database for each step. An example of the table is shown in the right half of Figure 5.6-2. The third step is to modify the BHEP for specific situations by multiplying it by a value of the performance shaping factor (PSF), which is in the range of 1/EF to EF (Error Factor), reflecting the influence of human factors. EF, meaning the error factor, is a numeral defined for each type of task in the table of the THERP. The modified value is called the human error probability (HEP). The final step is to calculate the HEP through the task.

THERP is founded on the notion that human errors are induced by not only the difficulty of the operation but also by the working conditions. Conversely, human errors might be reduced by improvement of the factors concerning the PSF, for example an understandable manual, freedom from stress, etc. In other words, human errors depend on the conditions or background under which the operation is performed.



THERP Table20-11

Item	Display or Task	HEP	EF
(1)	Digital indicators	.001	3
	Analog meters:		
(2)	With easily seen limit marks	.001	3
(3)	With difficult-to-see limit marks	.002	3
(4)	Without limit marks	.003	3
	Analog-type chart recorders:		
(5)	With limit marks	.002	3
(6)	Without limit marks	006	3
(7)	Confirming a status change on a status lamp	Negligible	
(8)	Misinterpreting the indication on the indicator lamps	Negligible	

Figure 5.6-2 HEP Evaluation in THERP

5.6.4 HRA using THERP

HRA sheets are prepared for tasks corresponding to risk important HAs. Table 5.6-1 shows the data entry in an HRA sheet. Fields in Table 5.6-1 are described below.

- Step Field: Task step number; each task step contains several activities
- Personnel Field: Reactor Operator (RO) or Supervisor Reactor Operator (SRO)
- Display, Controls Field: Equipment used for task step
- Activity Field: Detailed task description, task step is composed from activity
- Primary Action field :

  Omission Error
  IA (Initiate Action)
  OS (Omit Step)
  Commission Error
  SD (Select Display)
  SC (Select Control)
  RV (Read Value)

CR (Check Read)
RT (Read Text)
IC (Incorrect Calculation)
OC (Operate Control)
AC (Arithmetic Calculation)

- Action Type field:

  PU (Perceptual Unit), SA (Separate Action)

  · Recognition and confirmation of ANN : IA+SD=PU (message type)
  RT=SA
  :IA+SD+CR=PU(window type)

  ·Read and check value : SD+CR=PU
  RV=SA

  ·Confirmation of switch status : SC+CR=PU

  ·Confirmation of status lamp : SD+CR=PU

  ·Calculation : SD=SA
  IC=SA

  ·Operation : SC+OC=PU (on-off type control)
  : SC=SA (multi selection control)

- H.E Element Field: HSI design information for human error table selection

  L: Selection using label
  F: Grouping is used in HSI design
  U: Location of information is easily identified

- H.E Table Field: Table number in THERP handbook (NUREG/CR-1278)
- Standard H.E Field: Value of basic HEP which is determined by Action Type and H.E Element information
- Adjust Factor Field: Description of dependency (High Dependency :HD, Low Dependency : LD)
- Modified H.E Field: Basic HEP x EF(Error Factor) or DF(Dependency Factor)
- CAL Field: Description of calculation method
- HEP Field: Value of HEP calculated by specified method
- EF Field: Value of Error Factor
- SF Field: Value of Stress Factor
- Final HEP: Final value of HEP

THERP is used as standard HRA method in past development of Japanese PWR main control room by MHI, MELCO and Japanese PWR power utilities for 20 years.

Table 5.6-1 Example of Human Reliability Analysis Sheet

Task Name : :(1/N)

Step	Personnel	Display, Controls	Operation	Primitive Action	Action Type	H.E Element	H.E Table	Standard H.E	Adjust Factor	Modified H.E	CAL	HEP	EF	SF	Final HEP
1.	RO-1 SRO	H/W ANN	Ann (Confirm) Read first out ann Safety Injection Ann Reactor Trip Ann Turbine Trip Ann	IA SD CR	IA+SD+CR=PU		20-23 #3	0.0010	 LDa	0.0010 0.05.00	* 	0.0001	1	-	0.00005.
2.	RO-1 SRO	CRT (AUTO)	Confirm plant trip status (System check) Reactor Trip OK Turbine Trip OK Dual Check	OS 2SD 2CR CR	 IA 2SD+2CR=2PU CR=SA		20-7 #5. 20-5.#6 20-11#8 20-11#8	0.0100 0.0010 0.0010 0.0010	 LDa ZD LD	0.0100 0.05.00 0.0010 0.0010 0.05.00	* * *2 *	0.0000 0.0001	1 1	5. -	0.00000 0.00010
3.	RO-1 SRO	CRT (AUTO)	Confirm safety injection status and CV isolation (System check) Safety Injection OK CV Isolation OK Dual Check	OS SD*5. CR*10 CR	 IA 5.SD+10CR =5.OPU CR=SA		20-7#5. 20-5.#6 20-11#8 20-11#8	0.0100 0.0010 0.0010 0.0010	 LDa ZD LD	0.0100 0.05.00 0.0010 0.0010 0.05.00	* * *5. *	0.0000 0.0003	1 1	5. -	0.00000 0.00025.
4.	RO-1 SRO	 "RCP Trip "ANN (A,B,C,D) RCP Control SW	Confirm RCP status (System check) Confirm "RCP Trip "ANN (*4) Confirm RCP status (*4) (GREEN)	OS SD*4 CR*4 SD*4 CR*4	 IA 4SD+4CR=PU 4SD+4CR=PU	 F	20-7#5. 20-5.#6 20-11#8 20-12#3	0.0100 0.0010 0.0010 0.0010	 LDa ZD MD	0.0100 0.05.00 0.0010 0.0010 0.15.00	* * *	0.0000 0.0002	1 1	5. -	0.00000 0.00015.
5.	RO-1 SRO	 CRT	Confirm RCS pressure (System check) Read PRZ pressure value and history data	OS SD RV,CR	 IA SD=SA RV+CR=PU		20-7#5. 20-5.#6 20-9#3 20-10#2	0.0100 0.0010 0.0010 0.0010	 LDa ZD	0.0100 0.05.00 0.0010 0.0010 0.0010	* * +	0.0000 0.0020	1 1	5. 5.	0.00000 0.01000

5.7 HSI Design

5.7.1 HSI Design Objective

The HSI design process represents the translation of function and task requirements into HSI characteristics and functions. The HSI is designed using a structured methodology that guides designers in identifying and selecting candidate HSI approaches, defining the detailed design, and performing HSI tests and evaluations. The methodology includes the development and use of HFE guidelines, e.g., a style guide to define the design-specific conventions. The availability of an HSI design methodology helps verify standardization and consistency in applying HFE principles.

5.7.2 Scope of HSI Design

The following sources of information provide input to the HSI design process:

- Analysis of Personnel Task Requirements - The analyses performed in earlier stages of the design process (operational experience review, functional analysis and function allocation, task analysis, staffing) is used to identify requirements for the HSIs.
- System Requirements - Constraints imposed by the overall instrumentation and control (I&C) system is considered throughout the HSI design process.
- Regulatory Requirements - Applicable regulatory requirements is identified as inputs to the HSI design process.
- Other Requirements – Other necessary requirements for US-APWR are identified and used as inputs to the HSI design.

In the HSI design phase, a concept of operations is developed indicating crew composition and the roles and responsibilities of individual crew members based on anticipated staffing levels. Functional requirements for the HSIs are developed to address the concept of operations, personnel functions & tasks and personnel requirements. The functional requirement specification would serve as the initial source of input to the HSI concept design. Design-specific HFE design guidance (style guide) is developed in the HSI detailed design and integration phase. Testing and evaluation of HSI designs is conducted throughout the HSI development process and evaluations would be performed iteratively. The methodology used for testing includes the trade-off evaluations for various HSI elements and performance-based tests.

5.7.3 HSI Design Methodology

The concept and design description of Mitsubishi's standard HSI system are described in chapter 4.0. In this section, methodology of HSI design to guide designers is explained.

5.7.3.1 Input Information to HSI Design Process

The output of the preceding process is input for the HSI design process. Input information includes functional requirement of operation, result of PRA, result of HRA, performance requirement for personnel, various regulatory requirement.

5.7.3.2 HSI Detailed Design and Integration

HSI system in the MCR is composed from operator console, large display panel, diverse HSI panel, supervisor console, safety technical advisor console, data management console. MHI uses style guide to keep design consistency between various computer displays. The style guide conforms to NUREG-0700.

The style guide includes following items:
- Guideline for general display format
- Guideline for display element
- Display design policy

Guideline for general display format includes following:
- Display design consistency
  Consistent interface design conventions are evident for all display features, and displays are consistent in word choice, format, and basic style with requirements for data and control entry. There is an explicit mapping between the characteristics and functions of the system to be represented and the features of the display representation.
- Understandability of Information
  Information is displayed consistently according to standards and conventions familiar to users. The characteristics and features of the display used to represent the process are readily perceived interpreted by the operator. The methods by which lower-level data are analyzed to produce higher-level information and graphical elements are understandable to users.
- Grouping of Information
  Related information is organized into groups. Information that must be compared or mentally integrated is presented in the close spatial proximity and use similar physical dimensions to convey meaning. If information must be mentally integrated, similar color codes is used for the information items.
- Readability of Information
  Important display elements and codes are identifiable and readable from the maximum viewing distance and under minimal ambient lighting conditions. Coding should not interfere with the readability of displayed information.
- Distinctive Coding
  Distinctive means of coding/highlighting is used when a user's attention must be directed to changes in the state of the system, critical or off-normal data, and hazardous conditions. When a graphic display contains some outstanding or discrepant feature that merits attention by a user, supplementary text is displayed to emphasize that feature.
- Uncluttered Displays
  Displays are as uncluttered as possible.
- Indication of Display
  A display feature is provided to indicate to the user that the system is operating properly. Information system failures (due to sensors, instruments, and components) result in distinct display changes, which directly indicate that depicted plant conditions are invalid.
- Display Update Rate Requirements
  The maximum update rate is determined by the time required for the user to identify and process the changed feature of the display.

Guideline for display elements includes following:

- Character
  Rule for using character in title, message and label is provided, and guideline includes appropriate character size, height-to-width ratio.
- Labels
  Each individual aspect of a display (e.g., data group, field, or message) contains a distinct, unique, and descriptive label.
- Color
  Where color is used for coding, it is employed conservatively and consistently. Table 5.7-1 shows the example of color coding rule.
- Tables and Lists
  Information is organized in some recognizable logical order to facilitate scanning and assimilation. A table is constructed so that row and column labels represent the information a user has prior to consulting the table. Labels include the unit of measure for the data in the table; units of measurement are part of row or column labels.
- Graphs
  Graphs convey enough information to allow the user to interpret the data without referring to additional sources. When multiple curves are included in a single graph, each curve is identified directly by an adjacent label, rather than by a separate legend.
- Mimics
  Mimics and diagrams contain the minimum amount of detail required to yield a meaningful pictorial representation. All flow path line origin points are labeled or begin at labeled components. All flow path line destination or terminal points are labeled or end at labeled components. Flow directions are clearly indicated by distinctive arrowheads. Where symbols are used to represent equipment components and process flow or signal paths, numerical data is presented reflecting inputs and outputs associated with equipment.
- Icons and Symbols
  The primary use of icons in graphic displays is to represent actual objects or actions. Icons are designed to look like the objects, processes, or operations they represent, by use of literal, functional, or operational representations. Icons are simple, closed figures when possible. Special symbols to signal critical conditions are used exclusively for that purpose. Table 5.7-2, 3 shows the example of component symbols.

Display design policy includes followings:

- Operation console display
  The display of soft controls allows users to quickly assess the status of individual components of a control system and their relationships with other components. Displays are designed to avoid occurrence of misunderstanding of plant status. Soft controls and related process information are integrated in one display.
- Large display panel
  Large display panel provides continuously visible process information. The display consists from fixed information display area and flexible display area. The fixed display area continually provides plant information in fixed locations, and the variable display area displays screens selected by the operator or automatically displays related operational VDU screens.

- Alarm display
  All alarms are displayed in system categories (primary systems, a turbine system and an electrical system) and displayed in each display area in chronological order with color code, blinking and audible tone.

5.7.3.3 HSI Tests and Evaluations

Testing and evaluation of HSI designs are conducted throughout the HSI development process and evaluations are performed iteratively. Trade-off evaluations are executed for selecting alternative HSI design plan from viewpoint of reliability and usability. Some prototype of HSI design (part) is made for performance-based tests.

The HSI design is documented to include the detailed HSI description including its form, function and performance characteristics, the basis for the HSI requirements and design characteristics with respect to operating experience and literature analyses, tradeoff studies, engineering evaluations and experiments, and benchmark evaluations records of the basis of the design changes.

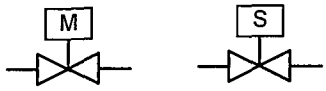
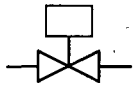
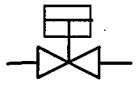
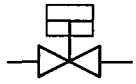
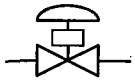
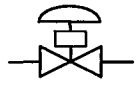
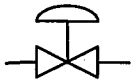
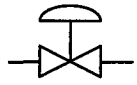
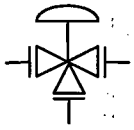
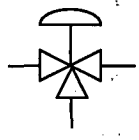
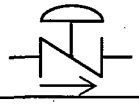
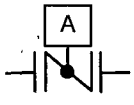
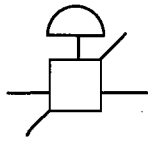
Table 5.7-1 Example of Color Coding Rule

Element	Main Color	
Component	Start, Open	Red, White(Open)
	Stop, Close	Green, White(Close)
	Uncertain	Yellow
Fixed Area	Green, Cyan	
Background	Black	
Variable Value / Characters	Normal	Green, White
	Abnormal	Red
	Uncertain	White, Yellow
Switches	Normal	Green, Gray
	Selected	Magenta, Gray
	Answer Back	Yellow, Magenta
Abnormal	Red, Yellow, Green	

Table 5.7-2 Example of Component Symbol (Pump)

Method			Remarks
Display	Color	Contents	
	White	Normal/ Start	Right Left Up Down: 4type
	White	Normal/Stop	
	Red	Abnormal/ Start	
	Red	Abnormal/ Stop	

Table 5.7-3 Example of Component Symbol (Valve)

Symbol for PID	Symbol for Display	
	Display	Remark
		
Piston Valve 		Close 
Air-operated Valve (with Positioner) 		
Air-operated Valve 		Open 
		
Stop Valve 		
Butterfly Valve 		

5.8 Operating Procedure Development Plan

5.8.1 Procedures to be Developed

The procedures for the US-APWR are categorized as follows:

- Normal Operating Procedure (NOP)
  - Plant operating procedures (including startup, power, and shutdown operations)
  - System operating procedures (including startup, power, and shutdown operations) (note) Above two categories contents same technical information, but they differs
  - Alarm response procedure (ARP)
  - Maintenance procedure
  - Periodic test procedures
- Emergency Operating Procedure (EOP)
  - Event-base EOP
  - Symptom-base EOP

a. Procedures for Normal Operation

Normal operating procedures are of two types:

- **Plant operating Procedures** for changing the state of the plant (start-up, load change, shutdown, outage, etc.)
- **System operating procedures** for the operation of individual plant systems (line-up, start-up, shutdown, change of operating mode, etc.) This category corresponds to the various operating modes

The presentation of these procedures in form of computerised formats has to respect the following requirements:

- the operator has to know the objectives to follow/to ensure: visualisation of the current state and of the pursued objectives,
- the operator has to know the state of the means, systems and functions which are available to ensure or to re-establish a given objective
- the operator is to be guided in the resolution of conflicts (if any) in the management of priorities about which function to treat first (presentation of an adequate decision logic)
- the procedure provide detailed descriptions for the execution of tasks and actions by providing adequate step programs for manual execution, or by reference to appropriate automatic sequences
- guidance of the operator is to be structured, with several levels of detail (objectives; tasks; actions),so as to enable operator to execute the procedure at any level of detail

The ARP is provided for each of alarm items. In case of failures of plant systems or unexpected plant state evolution, the alarm system warns the operator and guides operator to the corresponding actions using the associated ARP.

b. Procedures for Emergency Operation

The approach adopted for the US-APWR to provide accident response operation consists of both event-based and symptom-based. The principal characteristics of this approach are the following:

- The event-base Procedures are provided for followings:
  - Failure events those include digital I&C systems and HSI systems
  - Transients and design-basis accidents
  - Reasonable risk-significant, beyond-design-basis events, which are determined from the plant specific PRA
- The symptom-base procedures also provided to maintain plant safety critical functions as follows:
  - Reactivity Control
  - RCS Inventory
  - Core Cooling
  - Secondary Heat Sink
  - RCS Integrity
  - Containment Integrity

  The procedure defines priority between the event and critical functions.
  It also defines symptoms for each critical function.
- The operator has to know the state of the means, systems or functions which are available to ensure or to re-establish a given objective,
- The operator is to be guided in the resolution of conflicts between safety objectives respectively. in the management of priorities concerning which function to treat first,
- The operator is to be guided in the resolution of conflicts between different means (a single means is potentially used for several objectives; this may cause conflicts: it may be needed to ensure an objective, it can be rejected because it endangers an other objective),
- In case of failures of systems or in case of interaction of functions or systems, the procedure proposes substitutions.
- The procedures provide descriptions for the fulfilment of tasks and actions. Notably in this guidance may be only paper based even if other parts of the procedure are computerized.

Emergency procedures consider the degraded HSI conditions described in Section 4.11.

5.8.2 Procedures Development Process

The procedures development team consists of following personnel, some of them are to be member of the HFE team:

- Human Factors Engineer
  provides task analyses results and HRA results of risk-important human actions
- Systems Engineer
  provide knowledge of the processes involved in reactivity control and power generation of procedures

- Nuclear Engineer
  system-based technical requirements and specifications
- I&C Engineer and Computer System Engineer
  provides digital I&C system (including failure modes) and computer-based HSI technology impact to the procedures especially for introduction of computer-based procedures system
- Plant Operator
  provide knowledge of operational tasks and procedure formats, especially as presented in emergency procedure guidelines and operational procedures of current and predecessor plants
- Systems Safety Engineer
  provides risk-important human actions identified in the HRA/PRA
- Maintainability/Inspectability Engineer
  provide input in the areas of maintainability and inspectability to the development of procedures

A style guide is developed to establish the process for developing technical procedures that are complete, accurate, consistent, and easy to understand and follow. The guide contains objective criteria so that procedures developed in accordance with it are consistent in organization, style, and content. The guide is used for all procedures within the scope of this element.
The guide provide instructions for procedure content and format including the developing of action steps and the specification of acceptable acronym lists and acceptable terms to be used.

The content of the procedures incorporate the following elements as existing procedures of Japan and US:

- title and identifying information, such as number, revision, and date
- statement of applicability and purpose
- prerequisites
- precautions (including warnings, cautions, and notes)
- important human actions
- limitations and actions
- acceptance criteria
- check-off lists
- reference material

The most of operator experience is reflected present operating procedure of Japanese and US However the OER results described in section 5.2 are reviewed for checking necessity of reflection to the US-APWR procedures.

Preliminary procedures are provided before the activity of HSI V&V.
The procedures are verified first by analytical validation, such as task analysis and HRA.
They are validated and finalized in the integrated system validation described in section 5.10.

After the plant is constructed and start operation, operating experience of other plants and the changes that are made in the plant, including changes to HSI designs of HSI system are to be verified for needs of procedure changes.

5.9 Training Program Development Plan

This section describes key elements of the Training Program Development process.

5.9.1 Training Program

The training program for the HSI system is developed in accordance with the "Technical Report on Template for an Industry Training Program Description", NEI 06-13.
The IAEA's Systematic Approach to Training (SAT) program is introduced and following points are clarified:

- Clarify technical ability for performing operator's task
- Develop and execute training method to accomplish the technical ability
- Reflect training results and improve training method logically

This method also complies with NRC's "INSPECTION MANUAL CHAPTER 1245".
The training facility is settled at the corresponding NPP site at least two years before the fuel loading.

5.9.2 Operator Training Simulator Fidelity

Training simulator satisfies following requirements addressed in ANSI/ANS 3.5:

- Simulator's MCR and RSS console and their HSI system does not deviate from those of the reference
- The major PWR parameter (RCS flow, SG steam flow, SG feed flow, Charging flow, etc.,) match reference unit data within 2% of the reference unit instrument loop range.
- Instructor is able to use training simulator's basic functions (initialization, switch, check, freeze/run, snapshot, slow time/fast time, recorder power off, emergency power off, backtrack, record/replay, annunciator control, etc.,).

5.9.3 Class Room Training for Operators and Technicians

Class room training facility is also provided and following skills are in the course:

- Reactor technology
- Turbine and generator technology
- Nuclear power safety regulations
- Quality assurance
- Human factors
- Digital I&C system

5.9.4 Instructor Qualifications and Training

Instructor of training facility must have following skills and qualification:

- Instructional Skills
  - Training plan, Learning materials, Writing test
  - Training implementation, Evaluation, Critique and Reporting
  - Administrative skill
- Technical Skills

  - Knowledge of Nuclear power plant system
  - Design basis, Plant characteristics, Operating procedures and Simulators
  - Theoretical and practical technical skill based on working experience
- Interpersonal Skills
  - Elicit trainees' opinion and question, sincere gratitude
  - Corporate colleague and other staff
- College diploma and working Experience
- Operating Test
  - Initial Training Course : manipulate simulator
  - Continuing Training Course : Diagnose
- Assessment of instruction skill
  - Lecture
  - simulator training
- Assessment of produced training materials
- Assessment of training records

5.9.5 Role of the HFE Design Team in the Training Development Program

HFE Design Team provides following input to the training development program:

- **Licensing Basis** - Final Safety Analysis Report, system description manuals and operating procedures, facility license and license amendments, licensee event reports, and other documents identified by the staff as being important to training.
- **Operating Experience Review** - previous training deficiencies and operational problems that may be corrected through additional and enhanced training, and positive characteristics of previous training programs.
- **Function Analysis and Allocation** - functions identified as new or modified
- **Task Analysis** - tasks identified during task analysis as posing unusual demands including new or different tasks, and tasks requiring a high degree if coordination, high workload, or special skills.
- **Human Reliability Analysis** - coordinating individual roles to reduce the likelihood and/or consequences of human error associated with risk-important HAs and the use of advanced technology of digitalized I&C and computerized HSI system.
- **HSI Design** - design features of the computerized HSI system whose purpose or operation to be different from the past experience or expectations of personnel.
- **Plant Procedures** - tasks that have been identified during procedure development as being problematic (e.g., procedure steps that have undergone extensive revision as a result of plant safety concerns).
  The CBP system is the most characteristic difference in the computerized HSI system.
- **Verification** and **Validation (V&V)** - training concerns identified during V&V, including HSI usability concerns identified during validation or suitability verification and operator performance concerns (e.g., misdiagnoses of plant event) identified during validation.

5.10 Human Factors Verification and Validation

5.10.1 Principle of Verification and Validation (V&V)

There are four major human factor verification and validation (V&V) activities: Operational Condition Sampling, Design Verification, Integrated System Validation, and Human Engineering Discrepancies (HEDs) Resolution.

Operational Condition Sampling is the activity intended to identify the range of operational conditions relevant to guide V&V activities.

The Human Factors Verification and Validation program involves two types of Design Verification activities: HSI Task Support Verification and HFE Design Verification. HSI Task Support Verification is an evaluation whose purpose is to verify that the HSI supports personnel task requirements as defined by task analyses. HEDs are identified for: (1) personnel task requirements that are not fully supported by the HSI, and (2) the presence of HS components which may not be needed to support personnel tasks. HFE Design Verification is an evaluation to verify that the HSI is designed to accommodate human capabilities and limitations as reflected in HFE guidelines, such as those provided in NUREG-0700. HEDs are identified if the design is inconsistent with HFE guidelines.

Integrated System Validation is an evaluation using performance-based tests to determine whether an integrated system design (i.e., hardware, software, and personnel elements) meets performance requirements and acceptably supports safe operation of the plant. HEDs are identified if performance criteria are not met.

HED Resolution is an evaluation to provide reasonable assurance that the HEDs identified during the V&V activities have been acceptably assessed and resolved. HED Resolution is performed iteratively with V&V.

Figure 5.10-1 shows an overview of the verification and validation activities.

MHI has experience conducting HFE V&V in Japanese PWR plants. The HFE V&V was conducted in two steps: during the development phase and in the actual plant design implementation phase. This experience is described in Appendix B. For the US-APWR plants, both the development phase and design implementation phase, HFE V&V is conducted.

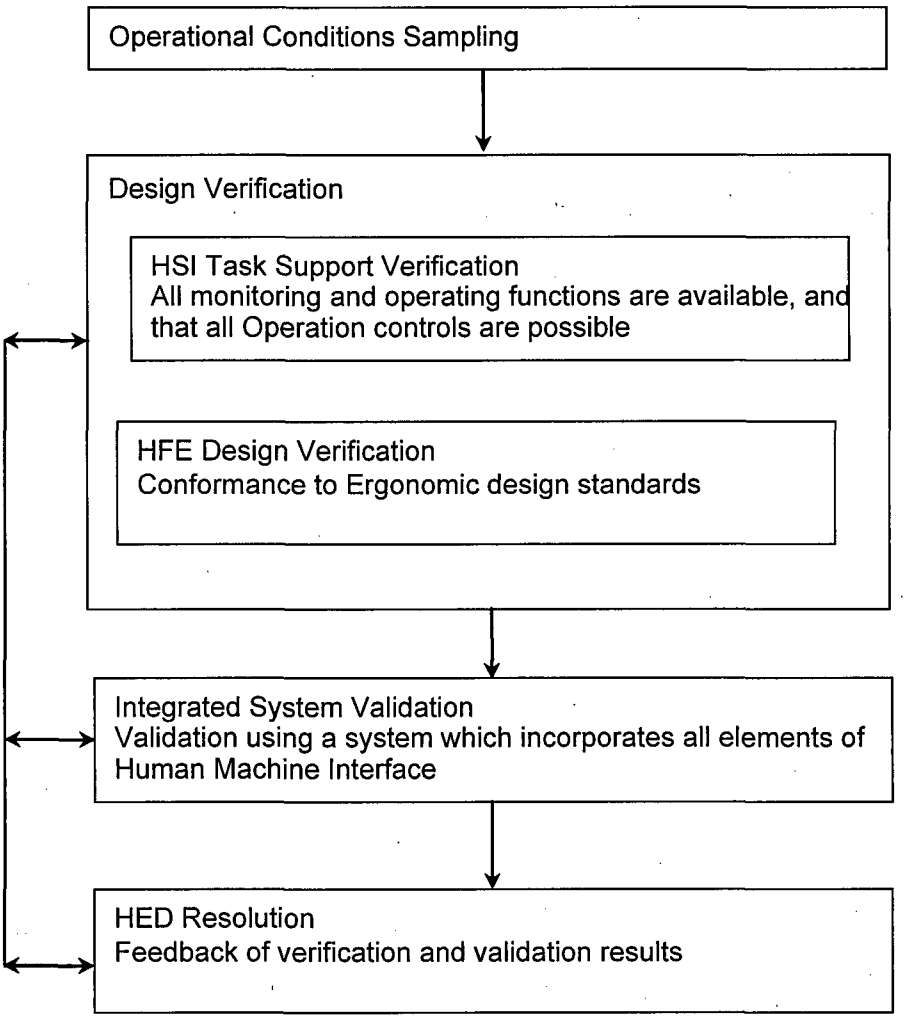


Figure 5.10-1 Overview of Verification and Validation Activities

5.10.2 Implementation Plan for HFE V&V

5.10.2.1 Operational Conditions Sampling

The sampling methodology identifies a range of operational conditions to guide V&V activities. The following sampling dimensions are addressed below: plant conditions, personnel tasks, and situational factors known to challenge personnel performance.

a. The following plant conditions are included:

- Normal operational events including plant startup, plant shutdown or refueling, and significant changes in operating power
- Failure events
- Transients and accidents, including accidents with concurrent Common Cause Failure conditions
- Reasonable, risk-significant, beyond-design-basis events, which are determined from the plant specific PRA
- Consideration of the role of the equipment in achieving plant safety functions (as described in the plant safety analysis report (SAR)) and the degree of interconnection with other plant systems

b. The following types of personnel tasks are included:

- Risk-significant HAs, systems, and accident sequences
- OER-identified difficult tasks
- Range of procedure guided tasks – These are tasks that are well defined by normal, abnormal, emergency, alarm response, and test procedures
- Range of knowledge-based tasks - These are tasks that are not as well defined by detailed procedures
- Range of human cognitive activities
- Range of human interactions
- Tasks that are performed with high frequency

c. The sample reflects a range of situational factors that are known to challenge human performance, such as:

- Operationally difficult tasks
- Error- forcing contexts
- High-workload conditions
- Varying-workload situations
- Fatigue and circadian factors
- Environmental factors

The results of the sampling are combined to identify a set of scenarios to guide subsequent analyses.

5.10.2.2 Design Verification

5.10.2.2.1 Inventory and Characterization

The inventory includes all HSI components associated with the personnel tasks based on the identified operational conditions.
The inventory describes the characteristics of each HSI component. The following is a minimal set of information required for the characterization of each component in the inventory:

- A unique identification code number or name
- Associated plant system and subsystem
- Associated personnel functions/subfunction
- Type of HSI component
  - computer-based control
  - hard-wired control
  - computer-based display
  - hard-wired display
- Display characteristics and functionality
- Control characteristics and functionality
- User-system interaction and dialog types
- Location in data management system
- Physical location in the HSI

5.10.2.2.2 HSI Task Support Verification

HSI task support verification confirms that the HSI provides all alarms, information, and control capabilities required for personnel tasks.

In the HSI task support verification, the HSIs and their characteristics (as defined in the HSI inventory and characterization) are compared to the personnel task requirements identified in the task analysis.

HEDs are identified when:
- An HSI needed for task performance is not available
- HSI characteristics do not match the personnel task requirements
- An HSI is identified as available but is not needed for any task.

HEDs are documented to identify the HSI, the relevant task criterion, and basis for the deficiency.

5.10.2.2.3 HFE Design Verification

HFE design verification is to verify the characteristics of the HSI and environment in which it is used conform to HFE guidelines.

For HFE design verification, a design-specific HFE guideline document is prepared. The design-specific HFE guideline document is compared to the HFE guidelines contained in NUREG-0700 to confirm the guidelines in the design-specific HFE guideline document satisfy the guidelines in NUREG-0700.

The design-specific HFE guideline document includes to following guidelines:
- Display screen format organization
- Font size for each display screen
- Touch size for touch screen operation
- Color coding
- Display Labeling coding
- Ergonomic requirement for display
- Standard of controllers and switches
- Guidelines for display design (guidelines and coding rules for display screen implementation)

5.10.2.2.4 Integrated System Validation

Integrated system validation is the process by which an integrated system design (i.e., hardware, software, and personnel elements) is evaluated using performance-based tests to determine whether it acceptably supports safe operation of the plant.

Integrated system validation is conducted after significant HEDs that are identified in verification reviews are resolved.

a. Test Objectives

Detailed objectives are developed to provide evidence that the integrated system adequately supports plant personnel in the safe operation of the plant.
The objectives are as follows:

- Validate the role of plant personnel.
- Validate that the shift staffing, assignment of tasks to crew members, and crew coordination (both within the control room as well as between the control room and local control stations and support centers) is acceptable.
- Validate that for each human function, the design provides adequate alerting, information, control, and feedback capability for human functions to be performed under normal plant evolutions, transients, design-basis accidents, and selected, risk-significant events that are beyond-design basis.
- Validate that those specific personnel tasks can be accomplished within time and performance criteria, with a high degree of operating crew situation awareness, and with acceptable workload levels that provide a balance between a minimum level of vigilance and operator burden. Validate that the operator interfaces minimize operator error and provide for error detection and recovery capability when errors occur.
- Validate that the crew can make effective transitions between the HSIs and procedures in the accomplishment of their tasks and that interface management tasks such as display configuration and navigation are not a distraction or undue burden.
- Validate that the integrated system performance is tolerant of failures of individual HSI features.
- Identify aspects of the integrated system that may negatively affect integrated system performance.

b. Validation Test Facility

The validation test facility used to perform validation evaluations satisfies the following requirements. The facility used for validation test is consistent with the criteria of the American National Standard "Nuclear power plant simulators for use in operator training" ANSI/ANS 3.5-1998 as a guide. The scope of the plant dynamics is limited to the scope of integrated system validation test. The validation test facility is planned to be constructed at MELCO's factory in the US. The test facility is a full scale HSI mockup with a full-scope simulator.

- Interface Completeness – The test facility completely represents the integrated system. This includes HSIs and procedures not specifically required in the test scenarios. For example, adjacent controls and displays may affect the ways in which personnel use those that are addressed by a particular validation scenario.
- Interface Physical Fidelity –A high degree of physical fidelity in the HSIs and procedures are represented, including accurate presentation of alarms, displays, controls, job aids, procedures, communications, interface management tools, layout and spatial relationships.
- Interface Functional Fidelity –A high degree of functional fidelity in the HSIs and procedures are represented. All HSI functions are available. High functional fidelity includes HSI component modes of operation, i.e., the changes in functionality that can be invoked on the basis of personnel selection and/or plant states.
- Environment Fidelity –A high degree of environment fidelity is represented. The lighting, noise, temperature, and humidity characteristics reasonably reflect those expected. Thus, noise contributed by equipment, such as air handling units and computers are represented in validation tests.
- Data Completeness Fidelity –Information and data provided to personnel should completely represent the plant systems monitored and controlled from that facility.
- Data Content Fidelity – A high degree of data content fidelity are represented. The information and controls presented are based on an underlying model that accurately reflects the reference plant. The model should provide input to the HSI in a manner such that information accurately matches that which is actually presented in the reference plant.
- Data Dynamics Fidelity – A high degree of data dynamics fidelity are represented. The process model are capable of providing input to the HSI in a manner such that information flow and control responses occur accurately and in a correct response time; e.g., information are provided to personnel with the same delays as would occur in the plant.
- For important actions at complex HSIs remote from the main control room, where timely and precise human actions are required, the use of a simulation or mockup are considered to verify that human performance requirements can be achieved. (For less risk-important HAs or where the HSIs are not complex, human performance may be assessed based on analysis such as task analysis rather than simulation.)
- The test facility is verified for conformance to the test facility characteristics identified above before validations are conducted.

c. Plant Personnel

Participants in the validation tests are representative of actual plant personnel who interact with the HSI. They are licensed operators.

To properly account for human variability, a sample of participants is used.

In the selection of personnel, consideration is given to the assembly of minimum and normal crew configurations, including shift supervisors, reactor operators, shift technical advisors, etc., that participate in the test.

To prevent bias in the sample, the following participant characteristics and selection practices are to be avoided:

- Participants who are part of the design organization
- Participants in prior evaluations
- Participants who are selected for some specific characteristic, such as using crews that are identified as good or experienced.

d. Scenario Definition

The operational conditions selected for inclusion in the validation tests are developed in detail so they can be performed on a simulator.

Scenarios have appropriate task fidelity so that realistic task performance is observed in the tests and test results can be generalized to actual plant operations.

When evaluating performance associated with operations remote from the main control room, the effects on crew performance due to a potentially harsh environment (i.e., high radiation) are realistically simulated (i.e., additional time to don protective clothing and access to radiologically controlled areas).

e. Performance measurement

A hierarchal set of performance measures are used that include measures of the performance of the plant and personnel.

- For plant performance, the following measurements are used:
  - Alarm history
  - Event log (plant trip time, ECCS actuation time, etc.)
  - HSIs use history (display screen request history, operational history, etc.)
- Personal task measurement
  For each specific scenario, the tasks that personnel are required to perform are identified and assessed. Two types of personnel tasks are measured: primary (e.g., start a pump), and secondary (e.g., access the pump status display). Following measurements are used:
  - Time
  - Operation and monitoring log
  - Errors (omission and commission)
  - Amount achieved or accomplished
  - Subjective report of participants
  - Behavior categorization by observers
- Situation awareness
  Personnel situation awareness is assessed. Video data and interview to participants are used for analysis of personnel situation awareness.
- Cognitive workload
  Personnel workload is assessed. Video data and interviews of participants are used for analysis of personnel cognitive workload.

f. Test Design

Scenario Assignment – Important characteristics of scenarios are balanced across crews. Normally the same scenario is used for every crew.

The order of presentation of scenario types to crews is carefully balanced to provide reasonable assurance that the same types of scenarios are not always being presented in the same linear position. e.g., the easy scenarios are not always presented first.

Test procedures including the description of NUREG-0711 section 11.4.3.2.6.2 "Test Procedures" are prepared.

Test administration personnel receive training on:
- The use and importance of test procedures
- Experimenter bias and the types of errors that may be introduced into test data through the failure of test conductors to accurately follow test procedures or interact properly with participants
- The importance of accurately documenting problems that arise in the course of testing, even if due to test conductor oversight or error.

Participants are trained to provide reasonable assurance that their knowledge of plant design, plant operations, and use of the HSIs and procedures is representative of experienced plant personnel.

Participants are trained to reach near asymptotic performance (i.e., stable, not significantly changing from trial to trial). One day and half day training is enough for training to use HSIs, based on the experience in Japan.

g. Data Analysis and Interpretation

Validation test data are analyzed through a combination of quantitative and qualitative methods. The relationship between observed performance data and the established performance criteria is clearly established and justified based upon the analyses performed.

For performance measures used as pass/fail indicators, failed indicators are resolved before the design can be validated. Where performance does not meet criteria for the other performance measures, the results are evaluated using the HED evaluation process.

The degree of convergent validity is evaluated, i.e., the convergence or consistency of the measures of performance.

The data analysis is independently verified for correctness of analysis.

The inference from observed performance to estimated real-world performance allows for margin of error.

h. Validation Conclusions

The validation conclusions are clearly documented including the statistical and logical bases for determining that performance of the integrated system is acceptable.

Validation limitations are considered in terms of identifying their possible effects on validation conclusions and impact on design implementation. These include:
- Aspects of the tests that were not well controlled
- Potential differences between the test situation and actual operations, such as absence of productivity-safety conflicts
- Potential differences between the validated design and the plant as built.

5.10.2.2.5 Human Engineering Discrepancy Resolution

HED Resolution is an activity that is performed iteratively with V&V. HED Resolution is performed after design verification and integrated system validation.

5.10.3 Organization of V&V Team

The V&V team includes personnel independent of the designers involved in the HSI initial design.

The V&V team includes personnel who have the following expertise:
- plant operation (maybe operators) and operator training
- Human System Interface design
- Human factor engineering

5.11 Design Implementation Plan

For new plants the ITAAC is used to confirm that the implemented HSI System is consistent with the validated HSI System. Inspections, Tests, Analysis, and Acceptance Criteria (ITAAC) are included in the DCD submittal.

The Design Implementation Plan element of the HFE Program Model also applies to operating plant modernization. It would also apply to HSI changes to the US-APWR after COL approval.

For any HSI change to a licensed design the potential impact on Human Actions is assessed and a risk significance level is assigned in accordance with the criteria in NUREG-1764. The risk significance considers the scope of the change as well as the potential impact on plant safety functions. Based on the risk significance some or all of the previous elements described in the HFE Program Plan are executed for the new design. The scope for each element is limited to the HSI change and any interfaces that may be affected by the change.

5.12 Human Performance Monitoring Plan

The goal of this element is to ensure that plant personnel have maintained the skills necessary to accomplish human actions within the time and performance criteria confirmed during the HSI validation program. The Human Performance Monitoring Plan ensures that no significant safety degradation occurs because of any changes that are made in the plant, including changes to HSI designs, procedures and training.

The plan requires periodic monitoring and documentation of human performance in actual or simulated plant conditions. Trends are maintained so that degraded performance is identified prior to reaching unacceptable levels. Corrective actions are tracked to resolution.

6.0 REFERENCES

This section lists the references cited in this topical report, except for applicable codes and standards and regulatory guidance in section 3.

1. MUAP-07004,"Safety I&C System Description and Design Process"
2. MUAP-07005,"Safety System Digital Platform-MELTAC"
3. MUAP-07006,"Defense-in-Depth Diversity"
4. PQD-HD-19005,"Quality Assurance Program(QAP) Description for Design Certification of US-APWR"
5. "Cyber Security Program for Nuclear Power Reactors", NEI 04-04, February 2005.
6. "Technical Report on Template for an Industry Training Program Description", NEI 06-13
7. System 80+ Design Certification Document (DCD)
8. Card, S.K, et al, "The Psychology of Human-Computer Interaction", Hillsdale, NJ: Lawrence Erlbaum Associates, (1983)"
9. ANSI/ANS-3.5 -1998 Nuclear Power Plant Simulators for Use in Operator Training
10. ANSI/ANS 5.8 -1994 Time Response Design Criteria for Safety-Related Operator Actions
11. EPRI NP-3659 Human Factors Guide for Nuclear Power Plant Control Room Development
12. NUREG/CR-1278, Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications
13. NUREG/CR-3371 Task Analysis of Nuclear Power Plant Control Room Crews
14. NUREG/CR-2623 The Allocation of Functions in Man-Machine Systems: A Perspective and Literature Review
15. NUREG/CR-3331 A Methodology for Allocation of Nuclear Power Plant Control Functions to Human and Automated Control Functions to Human and Automated Control
16. NUREG/CR-6400 HFE Insights For Advanced Reactors Based Upon Operating Experience
17. NUREG/CR-6393 Integrated System Validation: Methodology and Review Criteria
18. NUREG/CR-6633 Advanced Information Systems: Technical Basis and Human Factors Review Guidance

19. NUREG/CR-6634 Computer-Based Procedure Systems: Technical Basis and Human Factors Review Guidance

20. NUREG/CR-6635 Soft Controls: Technical Basis and Human Factors Review Guidance

21. NUREG/CR-6636 Maintenance of Digital Systems: Technical Basis and Human Factors Review Guidance

22. NUREG/CR-6637 Human-System Interface and Plant Modernization Process: Technical Basis and Human Factors Review Guidance

23. NUREG/CR-6689 Proposed Approach for Reviewing Changes to Risk-Important Human Actions

24. IEC 60964-1989 Design for control rooms of nuclear power plants

25. IEC 60960-1988 Functional Design Criteria for a Safety Parameter Display System for Nuclear Power Stations First Edition

26. IEC 60965-1989 Supplementary control points for reactor shutdown without access to the main control room

27. IEC 61227-1993 Nuclear power plants—control rooms—operator controls

28. IEC 61771-1995 Nuclear power plants — main control room — verification and validation of design

29. IEC 61772-1995 Nuclear power plants — main control room — Visual display unit (VDU) application to main control room in nuclear plants

30. IEC 61839-2000 Nuclear power plants — Design control rooms — Functional analysis and assignment

31. IEC 62096-2001 Instrumentation and Control: Guidance for the Decision on Modernization

32. IEC 60911-1987 Measurement requirements for reactor core sub cooling monitoring

33. IEC 62241-2004 Nuclear power plants — main control room —Alarm Functions and Presentation

34. ISO 11064-1-2000 Ergonomic Design of Control Centres — Part 1: Principles for the Design of Control Centres

35. ISO 11064-2-2000 Ergonomic Design of Control Centres — Part 2: Principles for the Arrangement of Control Suites

36. ISO 11064-3-1999 Ergonomic Design of Control Centres — Part 3 Control Room Layout

37. ISO 11064-4:2004 Ergonomic Design of Control Centres — Part 4: Layout and Dimensions of Workstations

38. ISO 11064-6:2005 Ergonomic Design of Control Centres — Part 6: Environmental Requirements for Control Centres

39. IEEE Std. 845-1999 IEEE Guide to the Evaluation of Human-System Performance in Nuclear Power Generating Stations

40. IEEE Std. 1023-1988 IEEE Guide to the Application of Human Factors Engineering to Systems, Equipment, and Facilities of Nuclear Power Generating Stations

41. IEEE Std. 1082-1997 A Guide for Incorporating Human Action Reliability Analysis for Nuclear Power Generating Stations

42. IAEA-TECDOC-1057 Experience in the Use of Systematic Approach to Training for Nuclear Power Plant Personnel

Appendix A History of Development of Japanese PWR Main Control Room by Mitsubishi and Japanese PWR Power Utilities

	Period	Objectives	HFE V&V
1. Development of advanced main control room	1996.10-2003.3	Establishment of total HSI design ●Large display panel(Alarm display) ●VDU for operation and monitoring ●Decision support system	Static validation test: 12 crews, 36 persons Dynamic validation test: #1 12 crews, 39 persons #2 12 crews, 37 persons #3 12 crews, 37 persons
2. Development of advanced alarm information display system	1994.10-1996.10	Development of alarm processing and display design	Static validation test: 12 crews, 24 persons Dynamic validation test: 12 crews, 34 persons
3. Development of emergency operation support system	1993.8-1996.3	Development of plant status diagnosis and operation guidance system	Dynamic validation test: 46 crews, 138 persons
4. Development of advanced main control board	1987.4 - 1991.3	Establishment of basic design ● VDU based monitoring and operation ●Compact operation console	Static validation test: 12 crews, 24 persons Dynamic validation test: #1 13 crews, 43 persons #2 13 crews, 44 persons #3 12 crews, 39 persons

Appendix B HFE V&V Experience in Japan

a. Verification and Validation in the Development Phase

Before applying the Advanced Main Control Board to an actual plant, design verification and validation of the standard specification were carried out and completed in the development phase of the control board. In verifying the standard specification, international standards IEC-60964, IEC-61171, and the US guideline NUREG-0711 were used for HSI design verification criteria for the Main Control Boards (MCBs).

The verification and validation were performed in two steps, step I and step II, as shown in Figure B-1. Step I or the "Static Verification" consists of design inspection and design verification of the standard specification. In step II, "Dynamic Validation", a mockup control board was setup and actual plant situations were simulated iteratively using the plant simulator. Both steps I and II were conducted by experienced plant operators, more than one hundred operators participated in the dynamic validation, which enabled operation practices to be implemented in the design from the development phase.
The validation facility used for validation test of the computerized main control board (DIATOM: Diamond Atomic Touch Operation and Monitoring system) is shown in Figure B-2, and Figure B-3

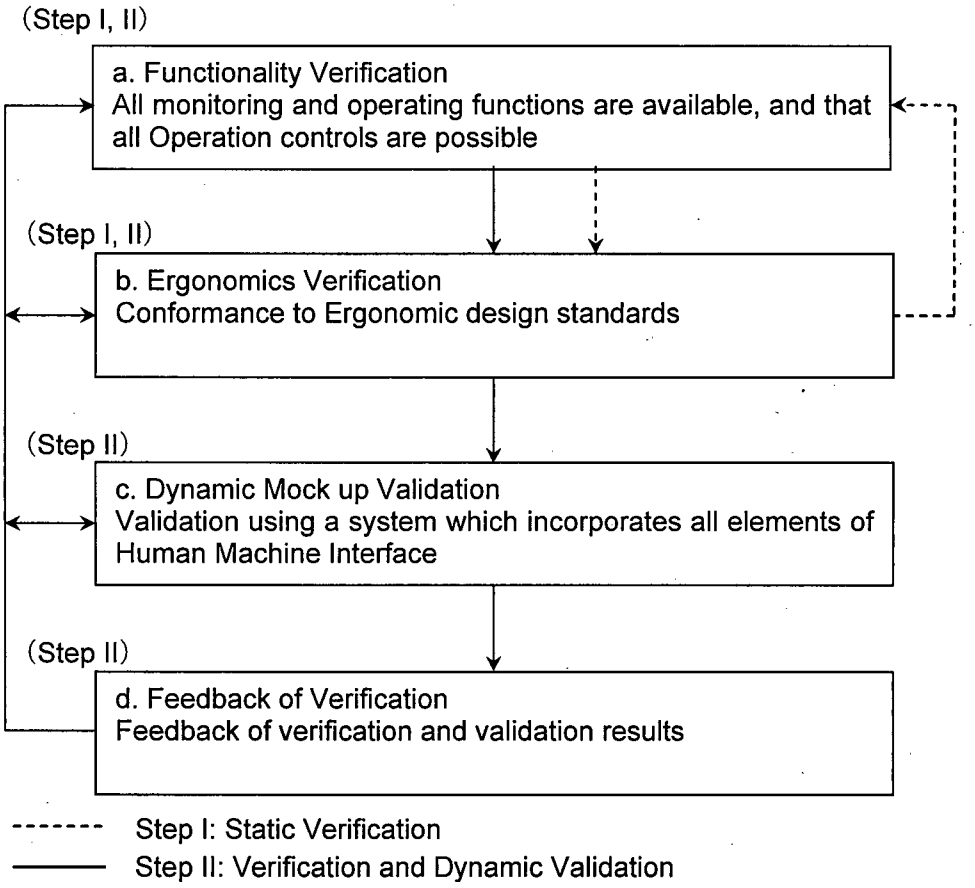


Figure B-1 HFE Verification and Validation Flow in the Development Phase

b. Verification and Validation in the Design Implementation Phase

Verification and validation in the Design Implementation Phase was conducted for the deviations from the standard design developed by the development phase.

Because, the deviations from the standard design were small, V&V in the implementation phase was conducted using a static method as follows.

- Full scale mockup test: - layout in the main control room was confirmed using plant specified full scale static mockup facility.
- Scenario based validation - Plant specified VDU formats verified by scenario based validation method using PC based static VDU format navigation system.

Details of HSI verification and validation in Japan are described in the following documents.

"The Development and Validation of Standardized Main Control Boards for full digital PWR I & C system", Trans. At. Energy Soc. Japan, Vol.2, No.3, pp. 307 ~ 35. (2003)

"The advanced main control console for next Japanese PWR plants", Proc. ICONE-9, Nice, (2001)

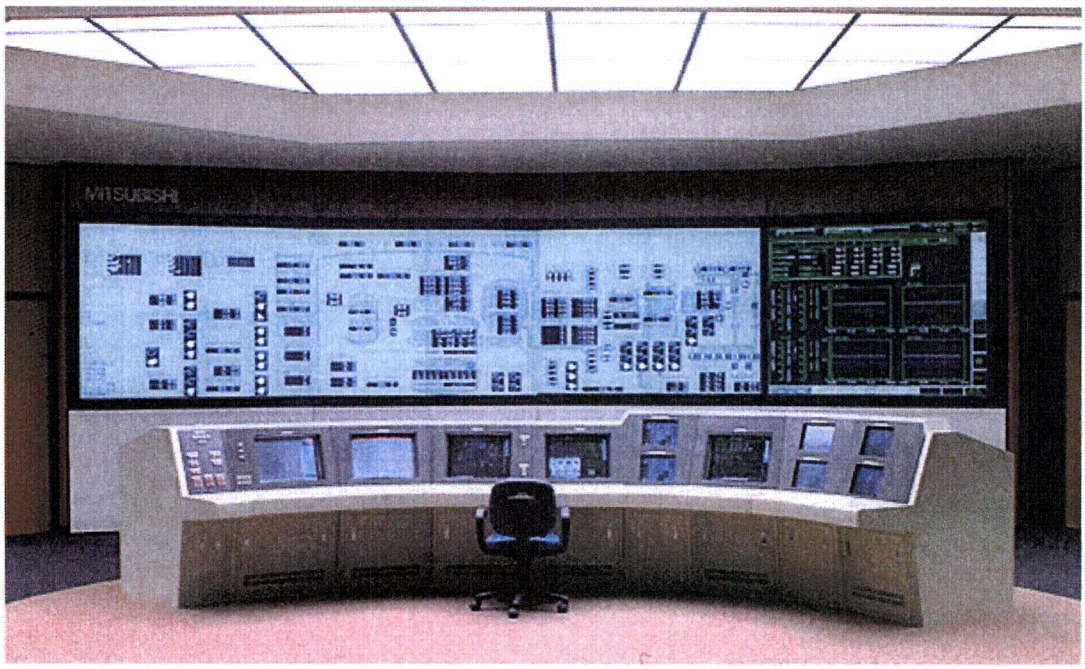
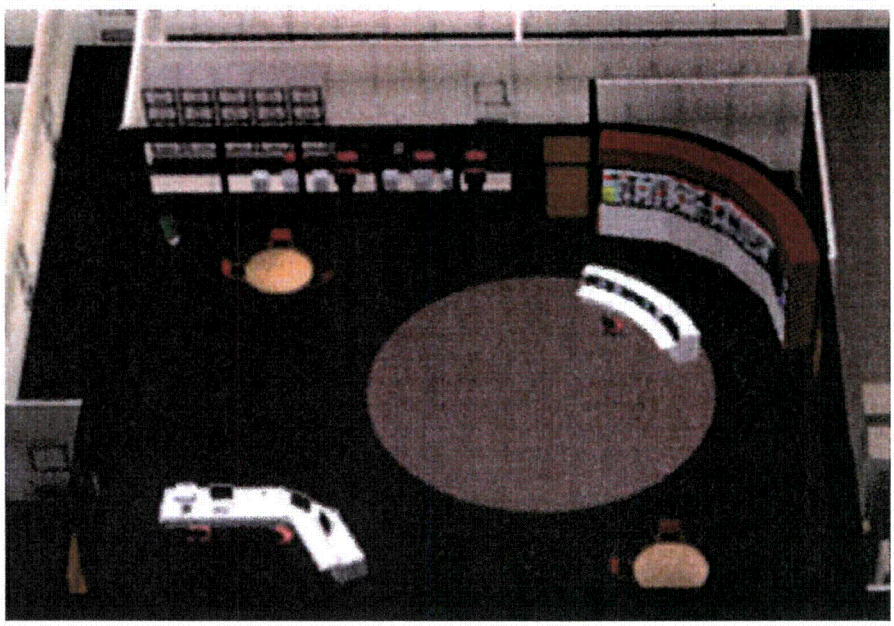


Figure B-2 The Facility Used in Development Phase



Note: Equivalent Facility is planned to be build in U.S.

Figure B-3 The Facility Image Used in Development Phase