MITSUBISHI NUCLEAR ENERGY SYSTEMS, INC.

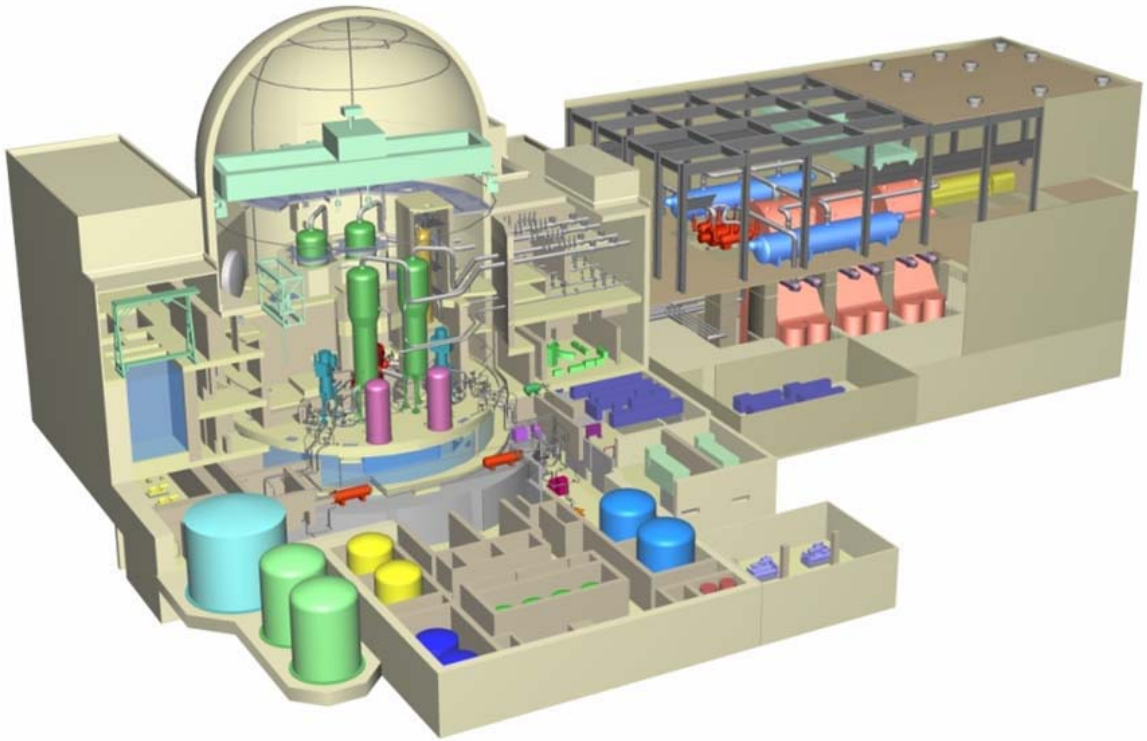
MITSUBISHI HEAVY INDUSTRIES, LTD.

US-APWR

MITSUBISHI

US-APWR

Digital I&C and Electrical System



June 29, 2007

Copyright© 2007 MITSUBISHI HEAVY INDUSTRIES, LTD.

Contents

- **Part 1:**
  - ✓ **I&C System Design**
    - **Operating History and Future Applications**
    - **Key Changes from Current Operating Plants**
    - **Licensing Process**
- **Part 2:**
  - ✓ **Electrical System Design**
    - **Equipment Qualification**
    - **Tech Specs**

- **Our goal is to familiarize DOE personnel with the features and benefits of MHIs digital I&C and Electrical systems**

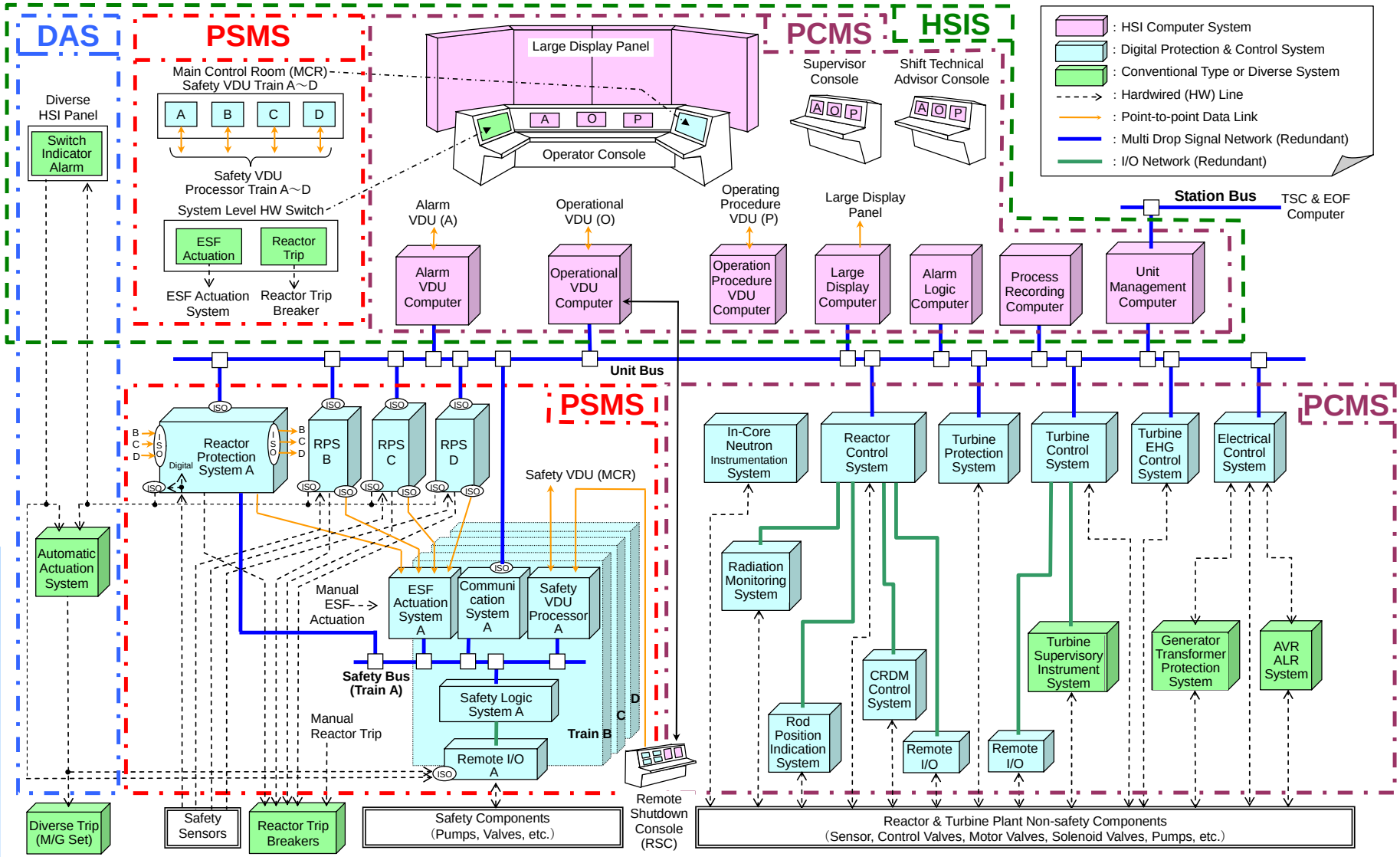
- **Please ask questions at any time**

Copyright© 2007 MITSUBISHI HEAVY INDUSTRIES, LTD.

Part 1:
Digital I&C System Overview

Copyright© 2007 MITSUBISHI HEAVY INDUSTRIES, LTD.

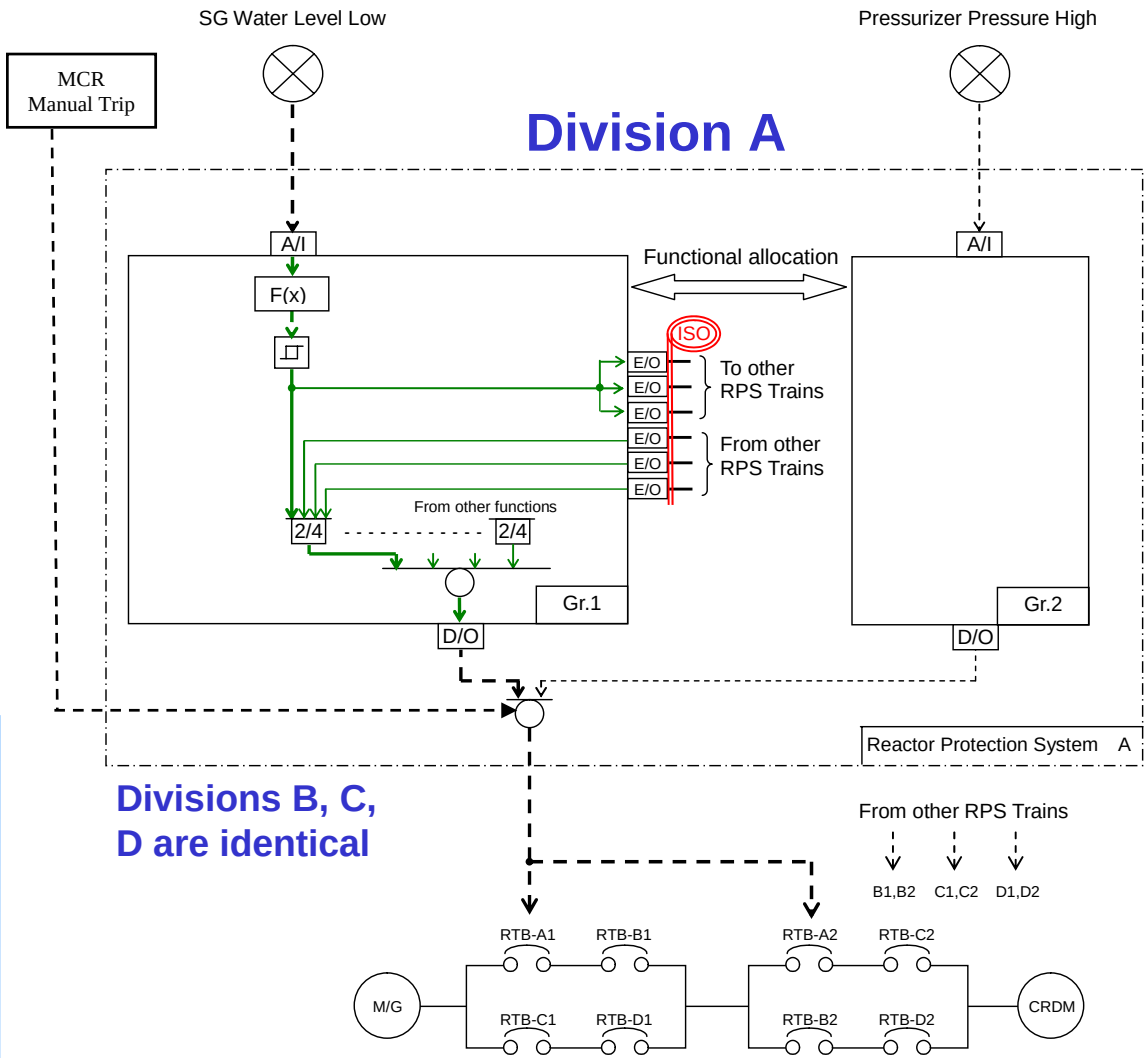
Overall I&C System Architecture



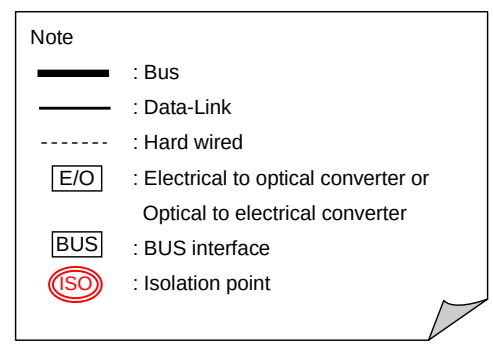
DAS : Diverse Actuation System PSMS : Protection and Safety Monitoring System HSIS : Human System Interface System PCMS : Plant Control and Monitoring System

Copyright© 2007 MITSUBISHI HEAVY INDUSTRIES, LTD.

Reactor Protection System



Two processors in each division provide two functionally diverse trips for each postulated accident.



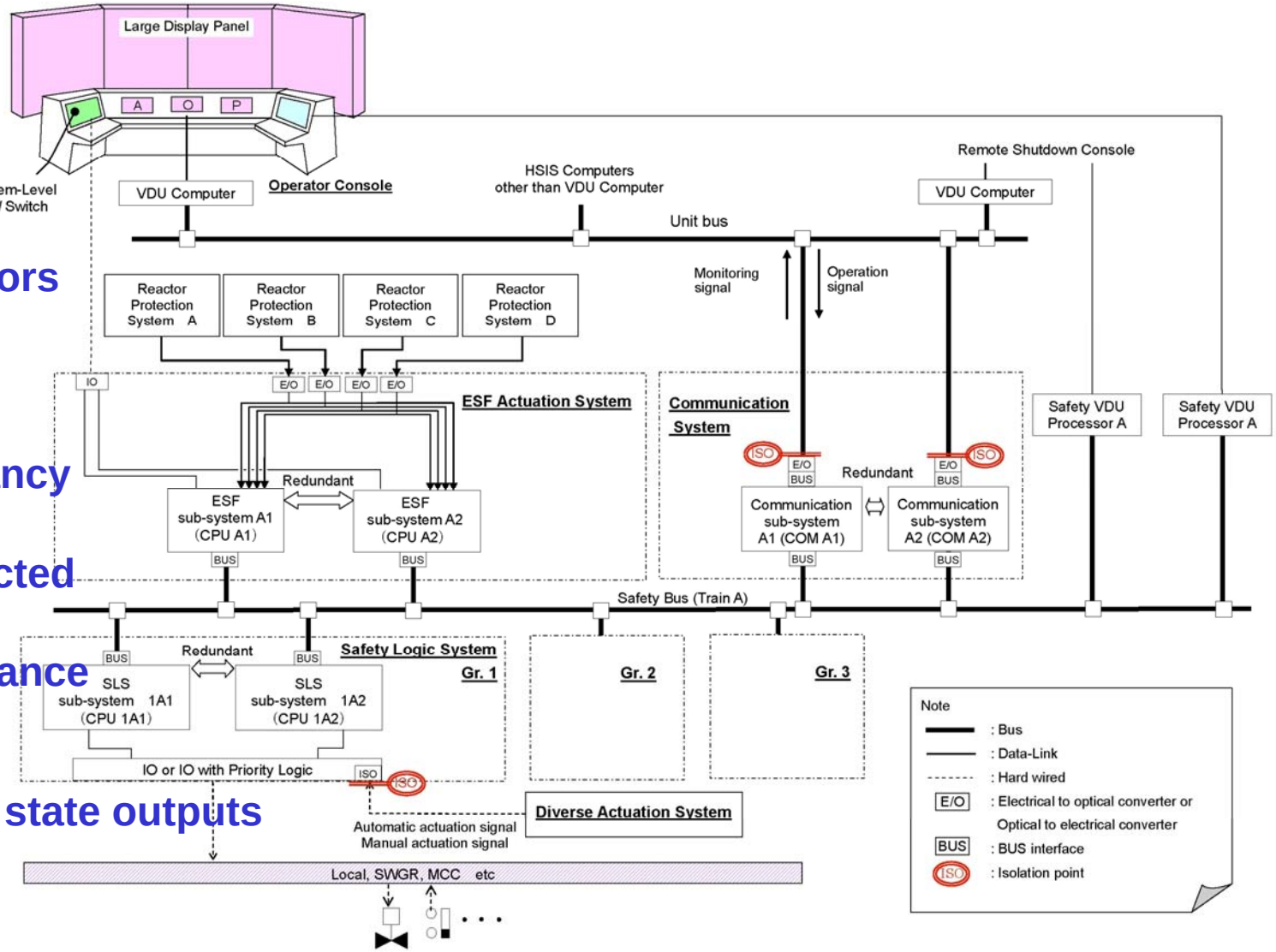
Configuration of Reactor Protection System

Copyright© 2007 MITSUBISHI HEAVY INDUSTRIES, LTD.

ESFAS, Safety Logic System, Safety HSI

Two processors in each division provide redundancy for unrestricted on-line maintenance

All solid state outputs

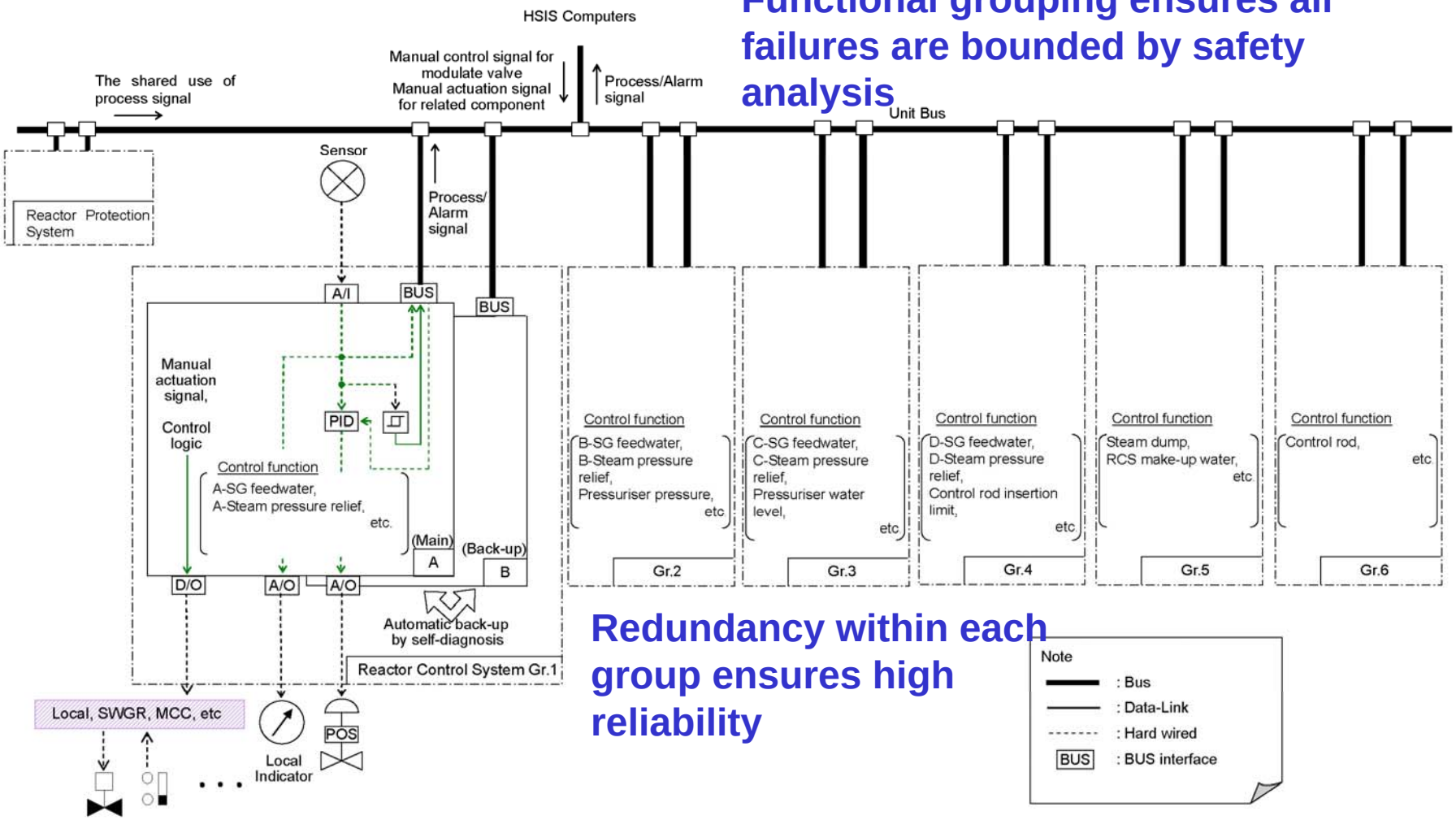


Configuration of Engineered Safety Features Actuation System and Safety Logic System

Copyright© 2007 MITSUBISHI HEAVY INDUSTRIES, LTD.

Reactor Control System

Functional grouping ensures all failures are bounded by safety analysis



Redundancy within each group ensures high reliability

Configuration of Reactor Control System

Copyright© 2007 MITSUBISHI HEAVY INDUSTRIES, LTD.

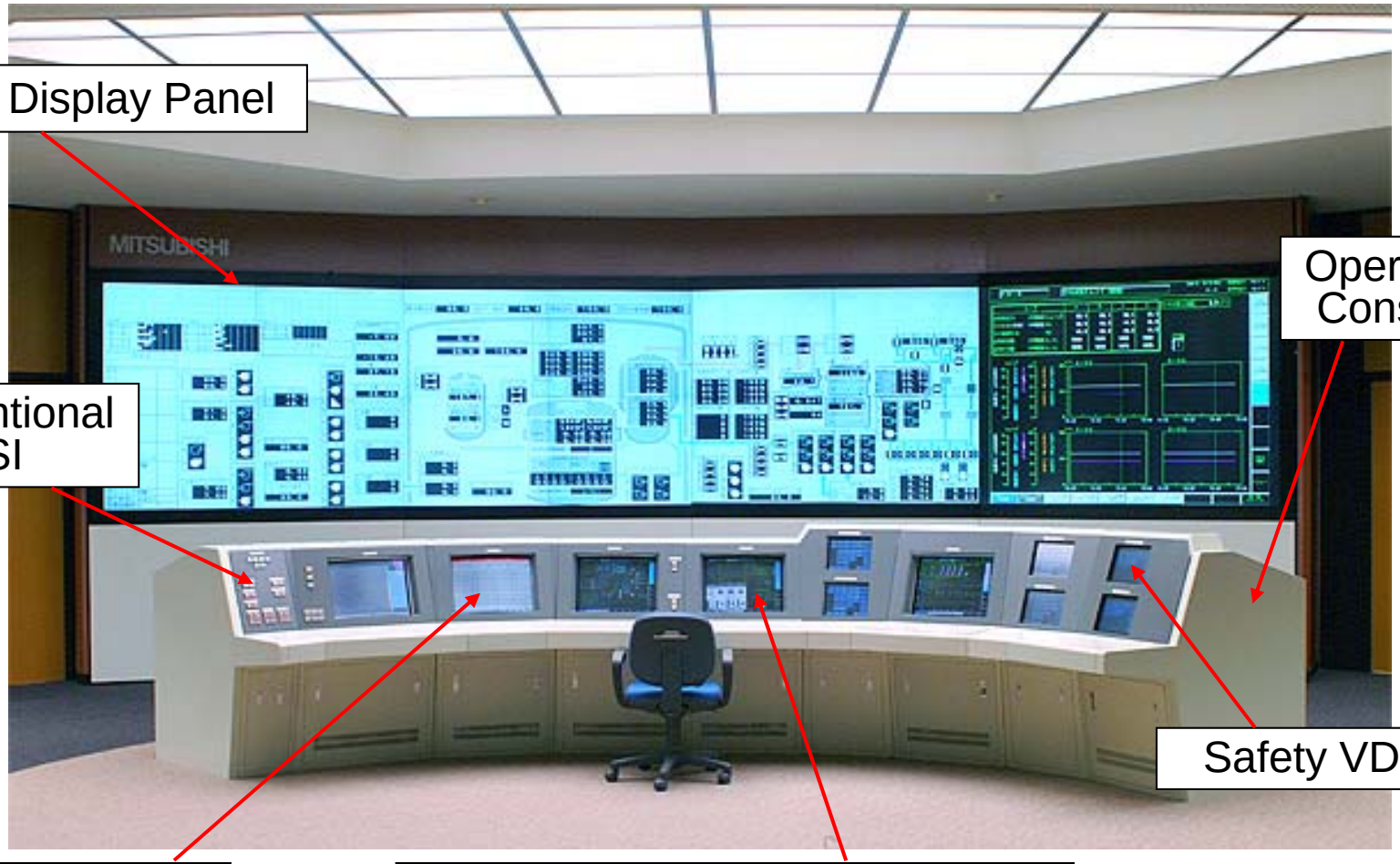
Overall I&C System Architecture

- Microprocessor based digital technology for most plant I&C (no electro-mechanical relays)
- Complete four train redundancy for safety I&C with each division in separate fire zone
- Distributed architecture for non-safety I&C with redundancy
- Fully multiplexed and duplicated signal transmission networks from local areas to I&C equipment rooms and Main Control Room, and between I&C systems
- Common digital platform for Safety and Non-safety I&C
- Diverse Actuation System based on a different technology
- Fully computerized Main Control Room

Copyright© 2007 MITSUBISHI HEAVY INDUSTRIES, LTD.

HSI System Architecture

Computerized Main Control Room



Large Display Panel

Operator Console

Conventional HSI

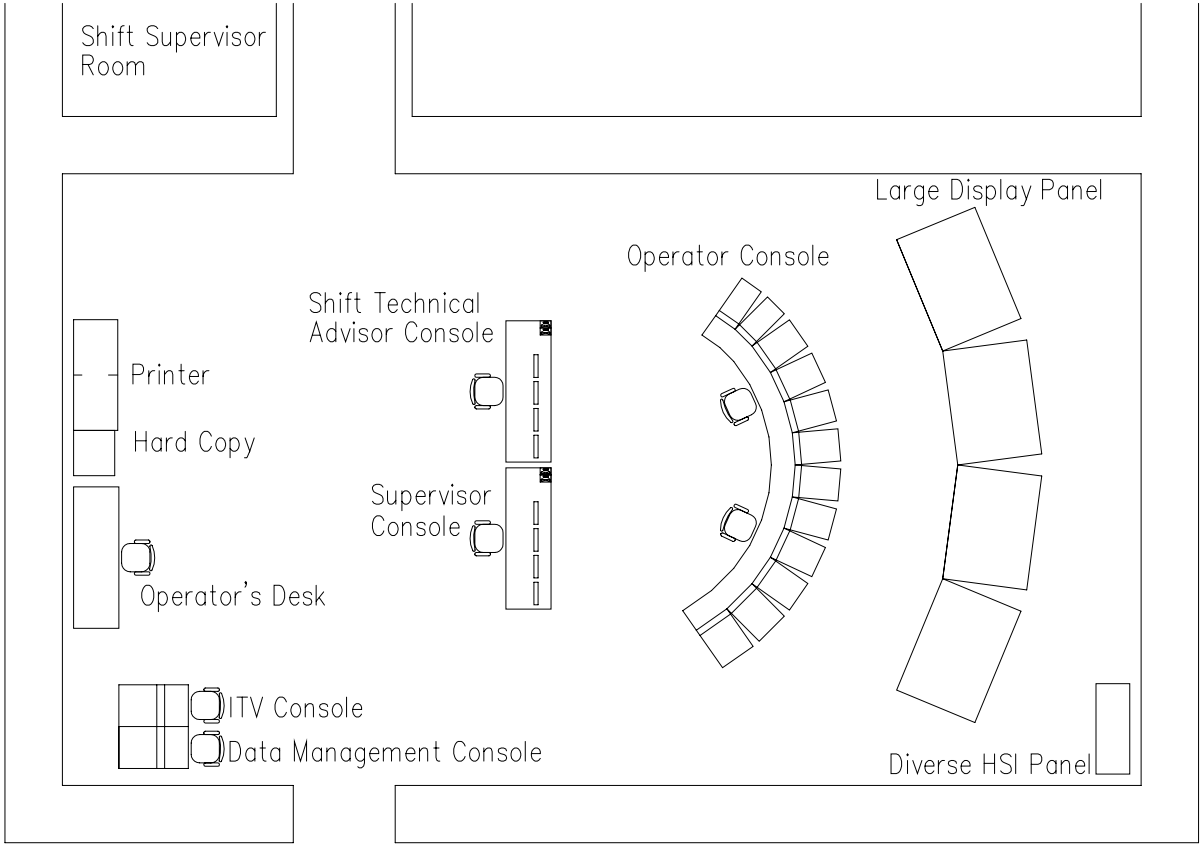
Safety VDU

Alarm VDU

Operation VDU (Non-Safety)

Copyright© 2007 MITSUBISHI HEAVY INDUSTRIES, LTD.

Main Control Room Layout

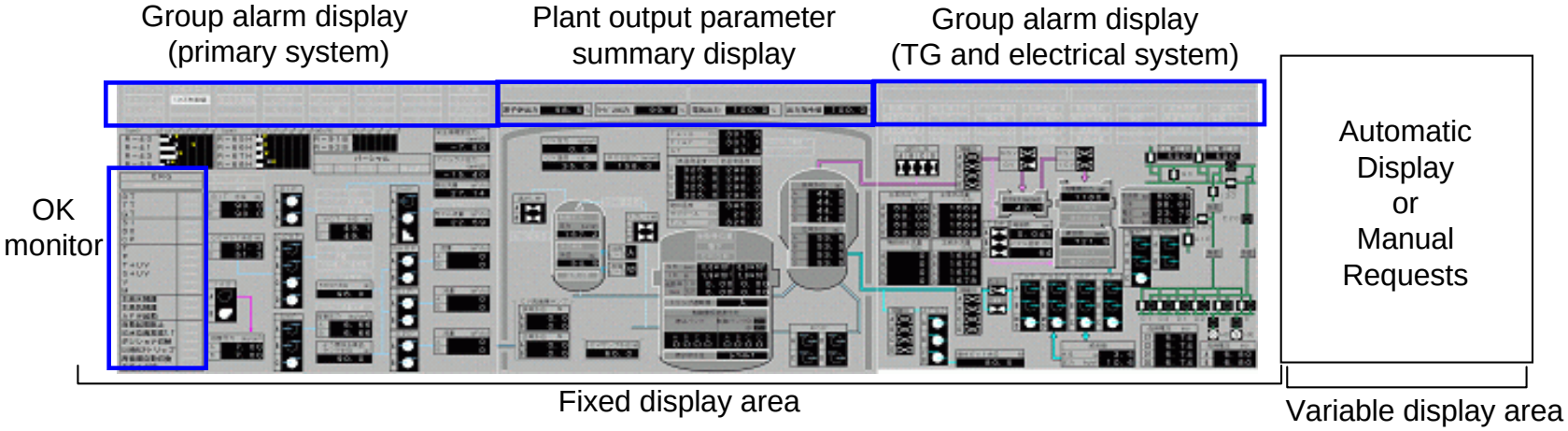


Copyright© 2007 MITSUBISHI HEAVY INDUSTRIES, LTD.

Large Display Panel

- Purpose of LDP
  - A fixed format display to provide a continuous overview of critical functions for plant power production and plant safety.
  - The apex of the information hierarchy for all plant conditions including upsets
  - A common communications interface to facilitate crew coordination
- LDP fulfills all NRC requirements for Minimum Inventory of SDCV information:
  High Level SPDS / Bypassed or Inoperable Status at System Level /
  Type A, B, C variables / Prompting for credited manual operator actions
- LDP Display Features
  - Information on LDP is readable from Operator Console and Supervisor Console.
  - Variable area selected by operator and Automatic Display shows related displays at Emergency mode (Reactor Trip, ECCS act. etc,.) and Operating Changing mode (Permissive Signal Actuations).

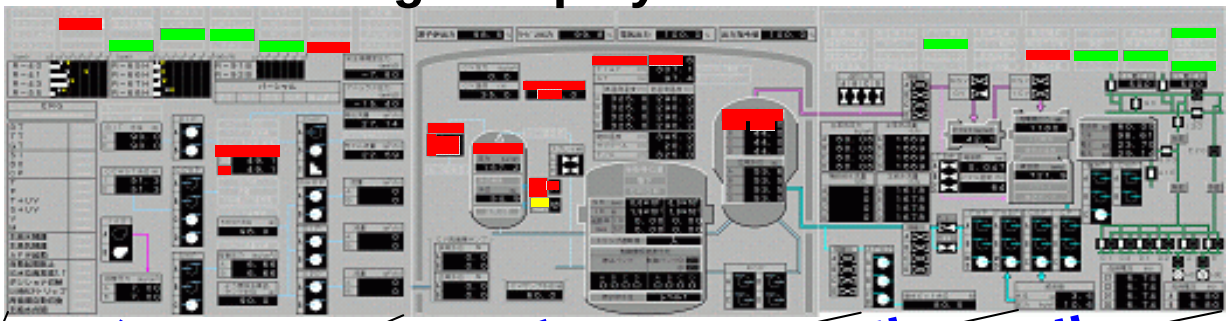
LDP – Large Display Panel SDCV – Spatially Dedicated Continuously Visible
SPDS – Safety Parameter Display System

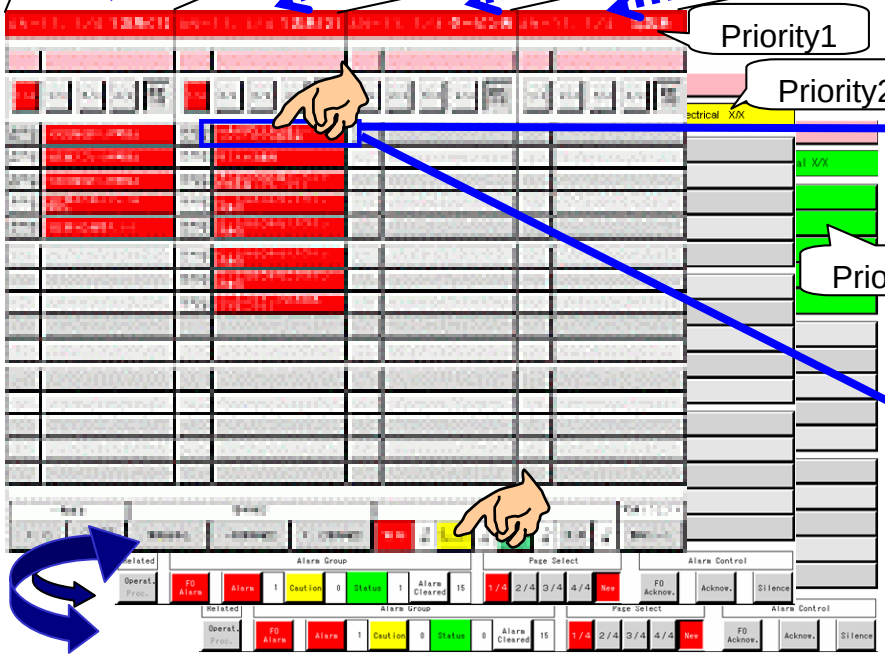


Copyright© 2007 MITSUBISHI HEAVY INDUSTRIES, LTD.

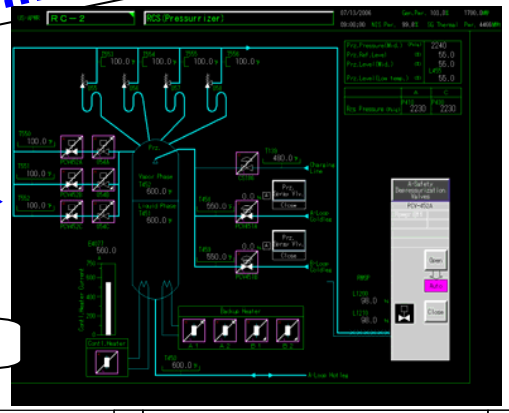
Alarm System

Large Display Panel

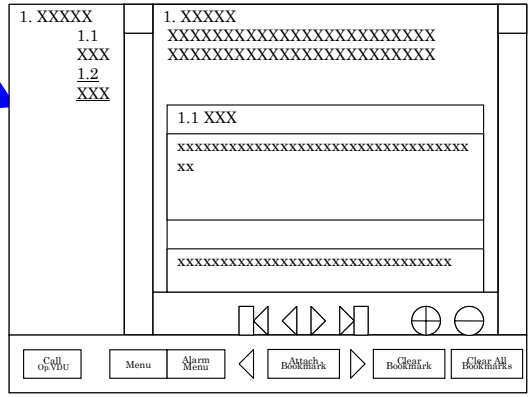




Alarm Display



Operational Display

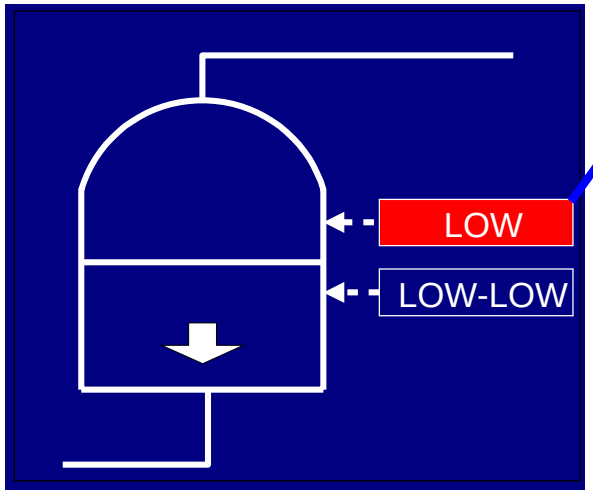


Operating Procedure Display

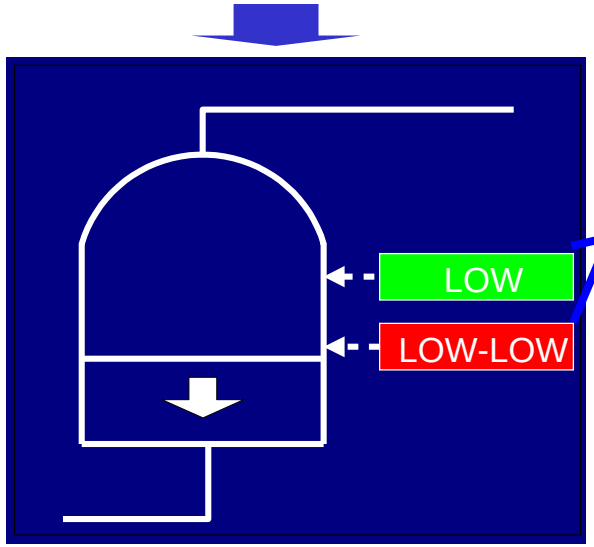
Copyright© 2007 MITSUBISHI HEAVY INDUSTRIES, LTD.

Dynamic Alarm Priorities (1/3)

1. Higher prioritization rule



Low alarm is displayed as Priority 1 (alarm information) until the tank level reaches the Low-Low alarm setpoint.

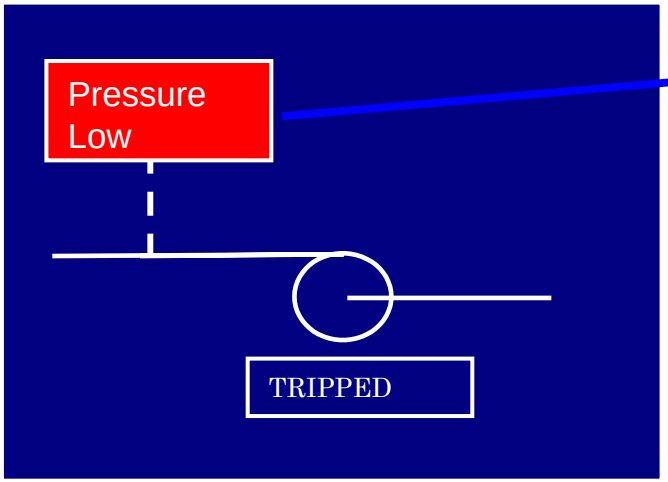


When the level reaches the Low-Low alarm setpoint, the Low-Low alarm is displayed as Priority 1 and the Low alarm is changed to Priority 3 (status information).

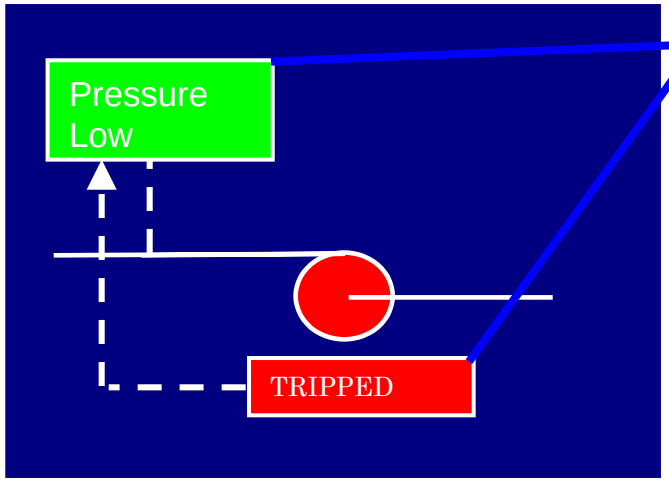
Copyright© 2007 MITSUBISHI HEAVY INDUSTRIES, LTD.

Dynamic Alarm Priorities (2/3)

2. Cause-consequence rule



A low discharge pressure alarm is displayed at priority 1 if there is no cause alarm.

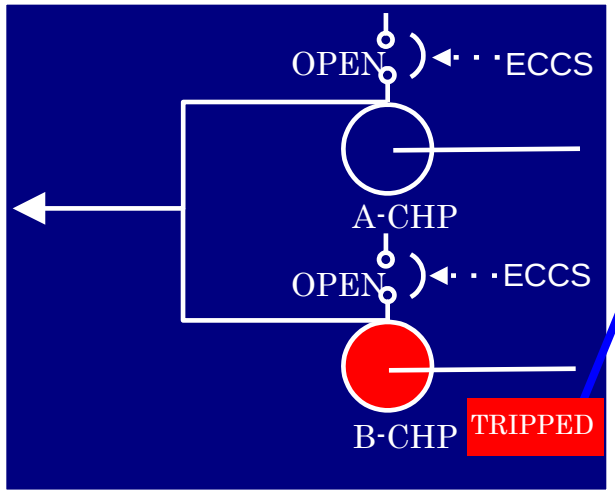


However, the low pressure alarm (“result” alarm) is regarded as Priority 3 when the pump is stopped by the interlock alarm (“cause” alarm) which is displayed as Priority 1.

Copyright© 2007 MITSUBISHI HEAVY INDUSTRIES, LTD.

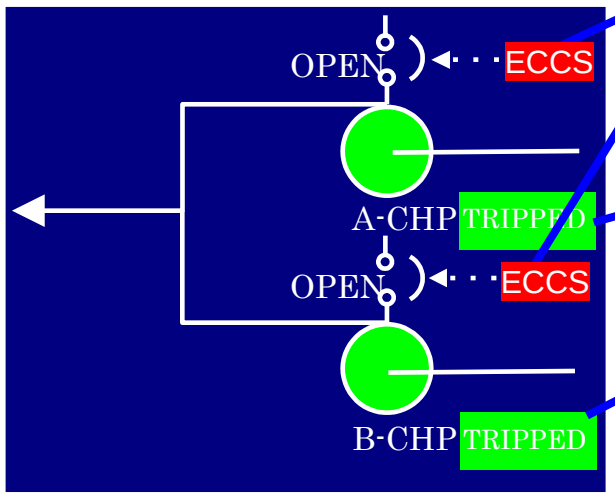
Dynamic Alarm Priorities (3/3)

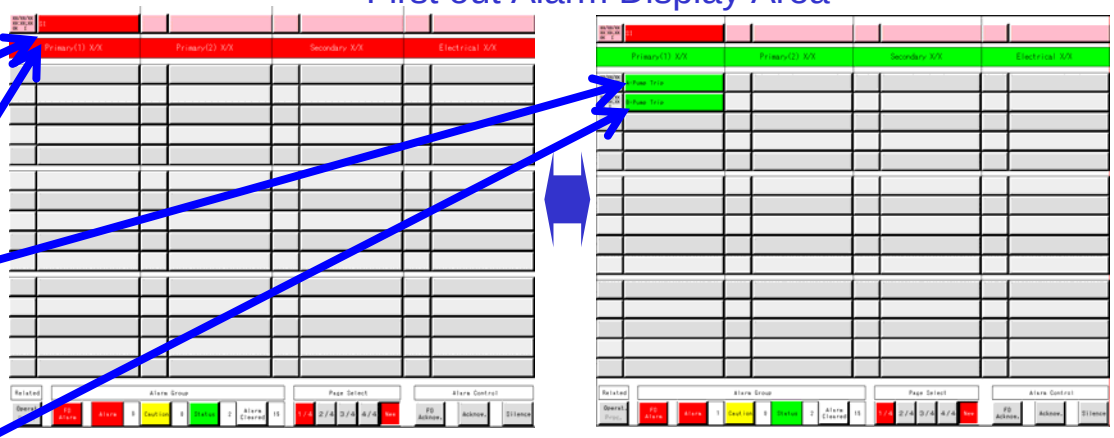
3. Mode Rule



A charging pump trip is displayed at priority 1 if there is no cause alarm.

First out Alarm Display Area





Charging pump trip alarms are regarded as Priority 3 (status information) when an ECCS signal is actuated.

Copyright© 2007 MITSUBISHI HEAVY INDUSTRIES, LTD.

Operating History and Future Applications

Copyright© 2007 MITSUBISHI HEAVY INDUSTRIES, LTD.

MELTAC Platform

- **Mitsubishi Electric Total Advanced Controller**

- **Simple Design**
  - ✓ Modular and Structured Architecture
  - ✓ Single Task execution
  - ✓ Cyclical Processing with No Interrupts

- **Quality Assurance and Control**
  - ✓ Designed specifically for Nuclear Applications
  - ✓ Under control of Nuclear QA/QC
  - ✓ Fully owned and life cycle management by MHI

Copyright© 2007 MITSUBISHI HEAVY INDUSTRIES, LTD.

History of MHI Digital Application

➢ Non-safety Application History

- ✓ Development began in 1985 with initial goal of non-safety applications and long term goal of safety applications
- ✓ Platform originally developed in compliance with US standards, including communications independence (cyber security)
- ✓ First installation for non-safety in 1991
- ✓ Average 10 years operation for five operating plants
- ✓ Applied to all non-safety I&C, 50 applications per plant
- ✓ Over 20 million hours total operating experience
- ✓ No un-expected shut down caused by I&C since 1992
- ✓ No system malfunction caused by S/W or H/W failure

Copyright© 2007 MITSUBISHI HEAVY INDUSTRIES, LTD.

History of MHI Digital Application

- **The same MELTAC digital platform is currently being applied to safety systems**
- **Current application for Reactor Protection and ESF Actuation System in Japan**
  - ✓Tomari #3 (Under construction, C/O 2009)
  - ✓Tsuruga #3/4 (APWR) (Under licensing, C/O 2015)
  - ✓Ikata #1/2 (Digital Upgrade 2009)
  - ✓Takahama #1/2/3/4 (Digital Upgrade 2009 – 2012)
  - ✓Ohi #1/2/3/4 (Digital Upgrade 2009 – 2013)

Note: Above RPS/ESFAS basic architecture are same as US-APWR

Copyright© 2007 MITSUBISHI HEAVY INDUSTRIES, LTD.

Development of Computerized MCR

- **Computerized Main Control Room Developed with Japanese Operators**
  - ✓ Development began in 1987
  - ✓ V&V tests (3 times) with Japanese PWR utilities shift operators (from12 sites) 1998-2001
    - Full-Scale Simulator
    - Performance Check
    - Review and Comment
  - ✓ Established Standard Design Specification for New PWR, APWR and Plant Modernization
- **Current applications in Japan**
  - ✓ Tomari #3 (Under construction, C/O 2009)
  - ✓ Tsuruga #3/4 (APWR) (Under licensing, C/O 2015)
  - ✓ Ikata #1/2 (Modernization 2009)

Copyright© 2007 MITSUBISHI HEAVY INDUSTRIES, LTD.

Lifetime and Local Support

➢ Lifetime & maintenance/replacement period

- ✓ Guarantee complete maintenance service for 30 years from delivery
- ✓ Digital platform will be replaced just one time during 60 year life

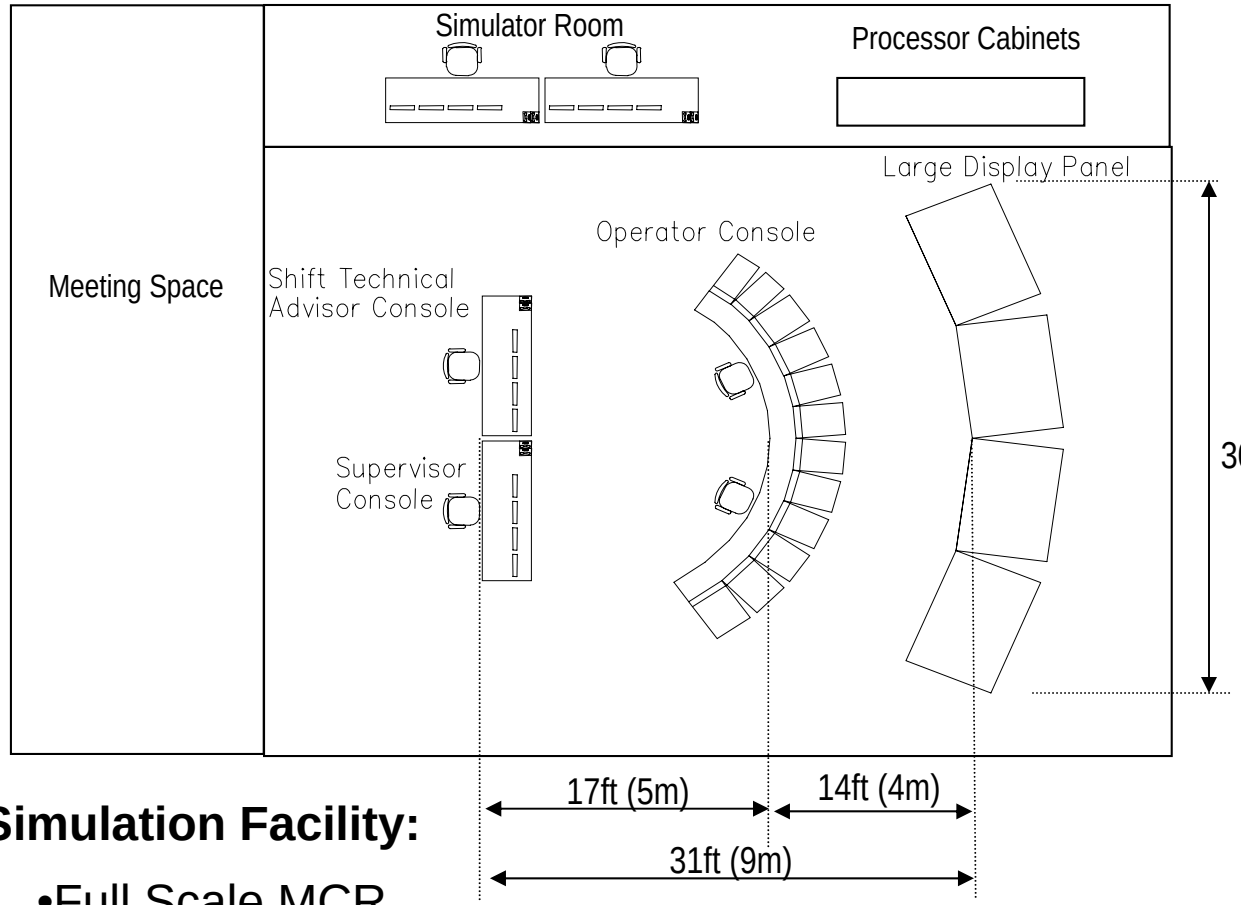
➢ Local support in United States

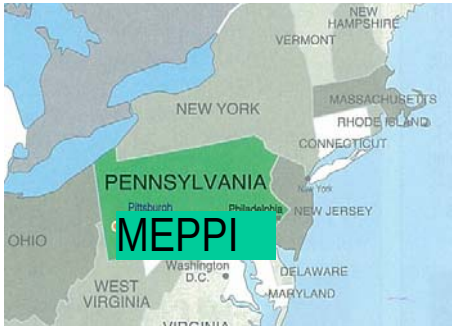
- ✓ Great experience in maintaining high reliability of 23 PWRs in Japan
- ✓ MELCO owns a 100%-subsidiary company in Pennsylvania (MEPPI: Mitsubishi Electric Power Product Inc.)
- ✓ Serves North American power systems, etc. with products & services
- ✓ This US company handles all technical & commercial communications
- ✓ Well-established service knowledge & organization
- ✓ Experience will provide effective maintenance support team for nuclear I&C in US, including 10CFR50 Appendix B

Copyright© 2007 MITSUBISHI HEAVY INDUSTRIES, LTD.

HSI Simulator Facility

HSI Simulation Facility at MEPPI site – Pittsburgh (April 2008)





Existing simulation Facility in Japan, MELCO ESC in Kobe

Simulation Facility:

- Full Scale MCR
- Interactive, full functionality VDUs
- High fidelity dynamic plant model

(MEPPI: Mitsubishi Electric Power Products, Inc.)

Copyright© 2007 MITSUBISHI HEAVY INDUSTRIES, LTD.

Purpose HSI Simulator Facility

- **The HSI Simulation Facility will fulfill three key needs:**
  1. **For Design Certification Application**
     - HSI Simulator allows NRC reviewers to fully understand HSI design and planned validation process
  2. **For Combined Operational Licensing Application**
     - Validation with US Operating Crews
       - All displays and computerized procedures
       - Operation with minimum staffing
       - Operation under degraded I&C/HSI conditions
  3. **For ITAAC Closure (ie. final operating license approval)**
     - Validation of operator and technician training programs
     - Train instructors
- **The HSI Simulator may also be used to bridge schedule gap for availability of site specific training simulators**

Copyright© 2007 MITSUBISHI HEAVY INDUSTRIES, LTD.

Key Changes
Compared to Operating Plants

Copyright© 2007 MITSUBISHI HEAVY INDUSTRIES, LTD.

Plant Availability

- **Well proven digital platform with complete redundancy**
  - No single failure in non-safety systems can cause spurious plant trips
  - No single failure in safety systems can cause plant trips even during on-line test configurations
  - ✓ Reduced unplanned upset conditions

Copyright© 2007 MITSUBISHI HEAVY INDUSTRIES, LTD.

Maintenance

- **Common digital platform used plant-wide for almost all safety and non-safety applications**
  - ✓ Reduced training for technicians, engineers, operators, other support staff
  - ✓ Reduced support staff
  - ✓ Reduced spare parts
- **Fully credited self-testing**
  - ✓ Reduced manual Tech Spec surveillances
  - ✓ Manual calibration and test extended to 24 months
- **Four divisions of all I&C and most mechanical systems**
  - ✓ Allows extended bypass and inoperable conditions for on-line maintenance and Tech Spec surveillance without threat of spurious plant trip
  - ✓ Unlimited bypass for RPS/ESFAS instrumentation and other functions with 4 divisions

Copyright© 2007 MITSUBISHI HEAVY INDUSTRIES, LTD.

Operations

➢ Advanced HSI

- multi-channel soft controls
- alarm filtering and prioritization
- fully integrated computerized procedures
- self-testing credited for Tech Spec surveillances

✓ Reduced operator training

✓ Reduced operations staff

- One SRO and one RO in MCR
- One SRO (Shift Supervisor) and one RO in Plant
- Reduced Auxiliary operators
  - Complete isolated fire zones with all MCR functionality at RSR
  - Distributed I/O allows more instrumentation for continuous on-line monitoring

Copyright© 2007 MITSUBISHI HEAVY INDUSTRIES, LTD.

Licensing Process in US

- **Four Topical Reports have been submitted for NRC approval**
  - Safety System Digital Platform - MELTAC
  - Safety I&C System Design Process and Description
  - HSI System Description and HFE Process
  - Defense-in-Depth and Diversity
- **Topical Reports address key technical issues that are likely to require in depth review by the NRC**
- **Topical Reports will be referenced in US-APWR Design Certification and COL Applications**
- **Also expected to be referenced in operating plant License Amendments**
- **MHI actively participates in all NEI Digital I&C/HFE Working Group and all related NRC meetings**

Copyright© 2007 MITSUBISHI HEAVY INDUSTRIES, LTD.

Key US Licensing Challenges

- **Level of detail for software and HFE design process submittals**
  - ✓ MHI goal is to minimize Design Acceptance Criteria
- **Acceptance of QA for previously developed software**
- **Multi-channel non-safety VDUs**
- **Common digital platform for safety and non-safety**

Copyright© 2007 MITSUBISHI HEAVY INDUSTRIES, LTD.

Multi-channel HSI

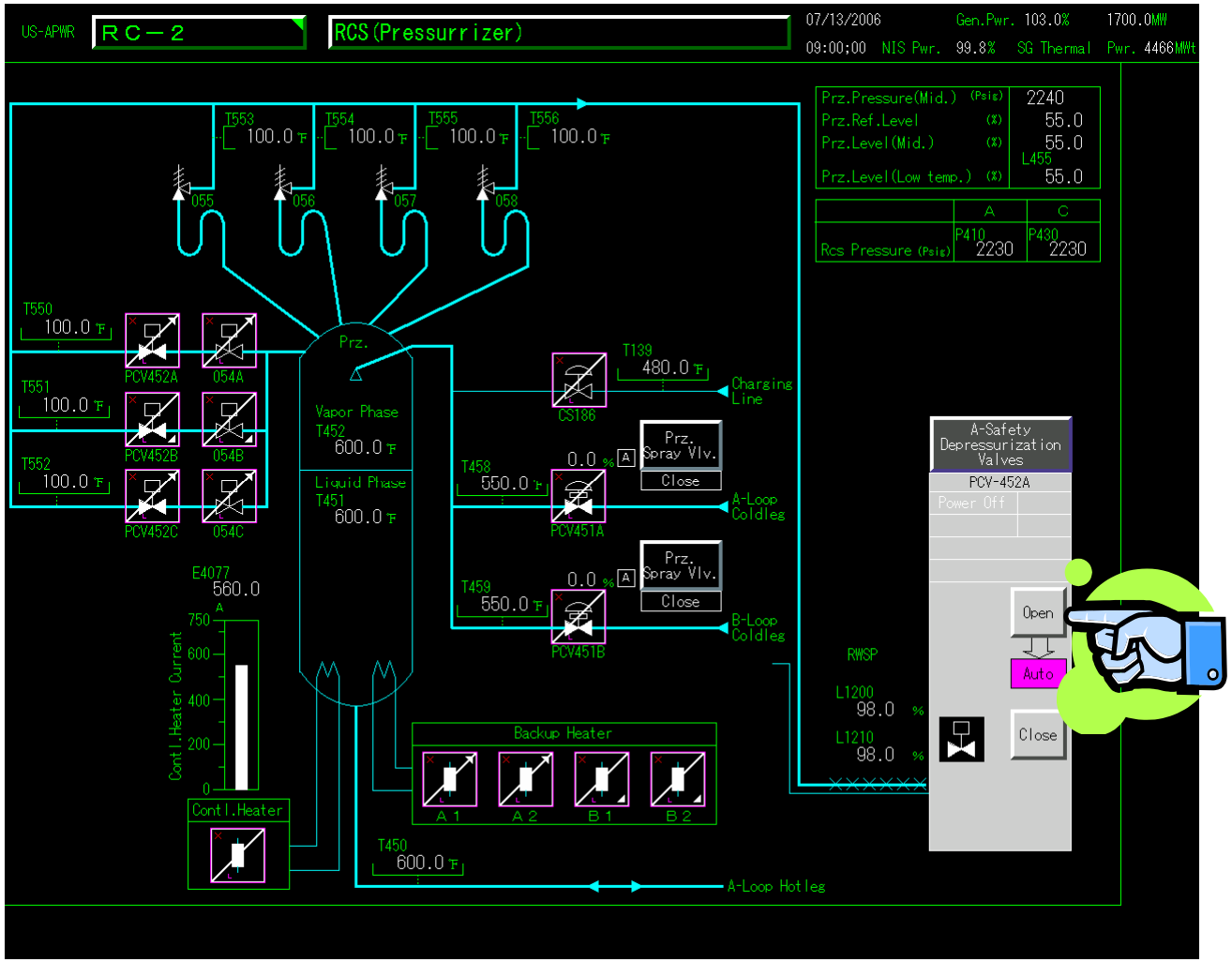
- **For all plant conditions, including DBA and safe shutdown, the primary operator interface is provided by**
  - ✓ Non-safety Multi-channel LDP
    - SDCV information and alarms significant to safety and power production
  - ✓ Non-Safety Multi-channel VDUs
    - Selectable interface for all other information, alarms and controls
  - ✓ Conventional Class 1E switches
    - SDCV controls for system level actuation of safety functions
- **Safety VDUs provide required Class 1E information and control for all safety functions (ie. backup)**

LDP – Large Display Panel
SDCV – spatially dedicated, continuously visible

Copyright© 2007 MITSUBISHI HEAVY INDUSTRIES, LTD.

Integrated Operation

- **Safety and Non-safety components can be operated from same screen**



Copyright© 2007 MITSUBISHI HEAVY INDUSTRIES, LTD.

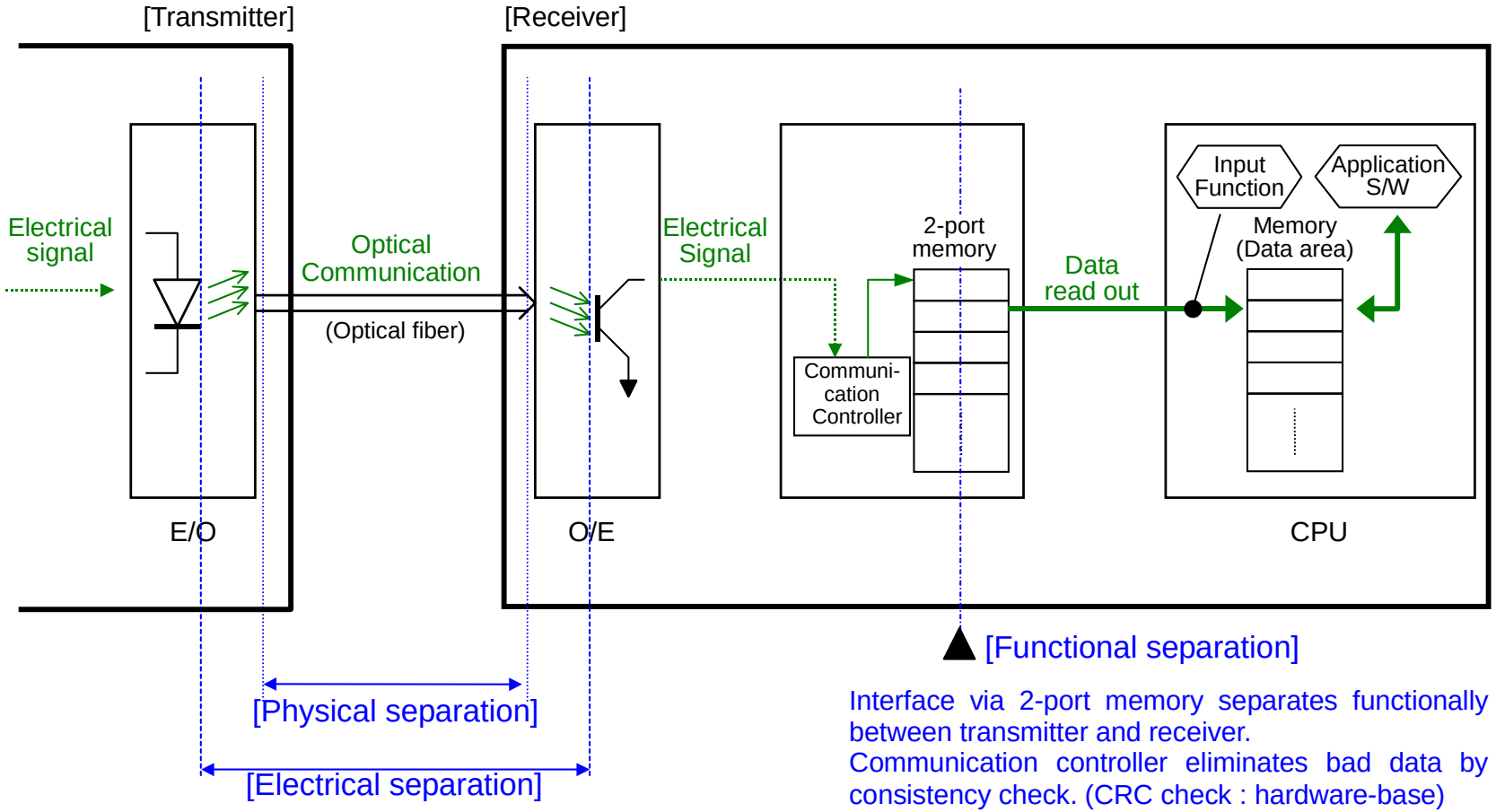
Multi-channel HSI Benefits

- **Integrated safety and non-safety monitoring and control 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 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 via hyperlinks.
  - ✓ Minimizes operator transitions between safety and non-safety VDUs, thereby reducing operator workload during critical plant situations
- **Benefits reduce operator task burden, reduce potential for human error**

Copyright© 2007 MITSUBISHI HEAVY INDUSTRIES, LTD.

Communication Isolation Features

- All intra-division or inter-division data communication uses the same method
- The communication method ensures no disruption to deterministic processing of safety functions



Interface via 2-port memory separates functionally between transmitter and receiver.
Communication controller eliminates bad data by consistency check. (CRC check : hardware-base)

Copyright© 2007 MITSUBISHI HEAVY INDUSTRIES, LTD.

Basis of DAS HSI/Automation

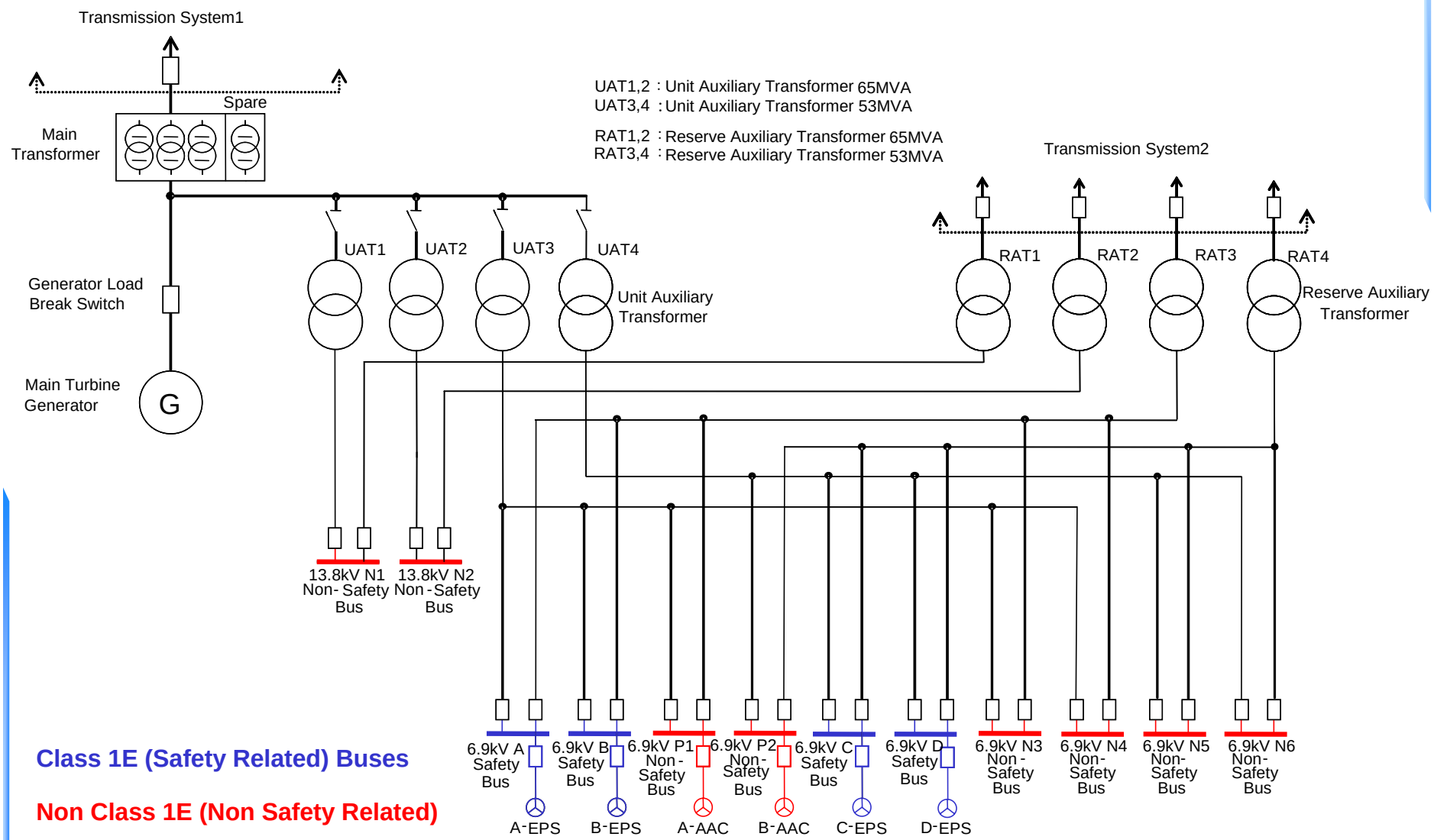
- **A "best estimate" thermal hydraulic analysis determines the time at which mitigation actions are required to meet the acceptance criteria of BTP-19**
  - ✓ Need action within 10 minutes
    - DAS automation is provided with alarms
  - ✓ Need action within 30 minutes
    - Indications, alarms and manual controls are provided on the Diverse HSI Panel (DHP)
    - Justification based on available HSI inventory and HFE analysis (otherwise function is also automated)
  - ✓ Need action after 30 minutes
    - Indications and manual controls are provided outside the MCR
    - Justification based on available HSI inventory
- **Indications and Manual Controls are provided for each critical safety function**

Copyright© 2007 MITSUBISHI HEAVY INDUSTRIES, LTD.

Part 2:
Electrical System Overview

Copyright© 2007 MITSUBISHI HEAVY INDUSTRIES, LTD.

AC Power System Configuration



Class 1E (Safety Related) Buses

Non Class 1E (Non Safety Related) Buses

Copyright© 2007 MITSUBISHI HEAVY INDUSTRIES, LTD.

Offsite Power System

➢ Design Features

- ✓ The two (2) sources of offsite power provided
  - a) Main Transformer through Unit Auxiliary Transformers (UAT)
  - b) Reserve Auxiliary Transformer (RAT)
- ✓ The two (2) offsite power supply circuits are independent and physically separated
- ✓ Both offsite power supply circuits have enough capacity to achieve their safety related function during a Design Basis Event (DBE) and meet the requirement of the applicable GDC's

Copyright© 2007 MITSUBISHI HEAVY INDUSTRIES, LTD.

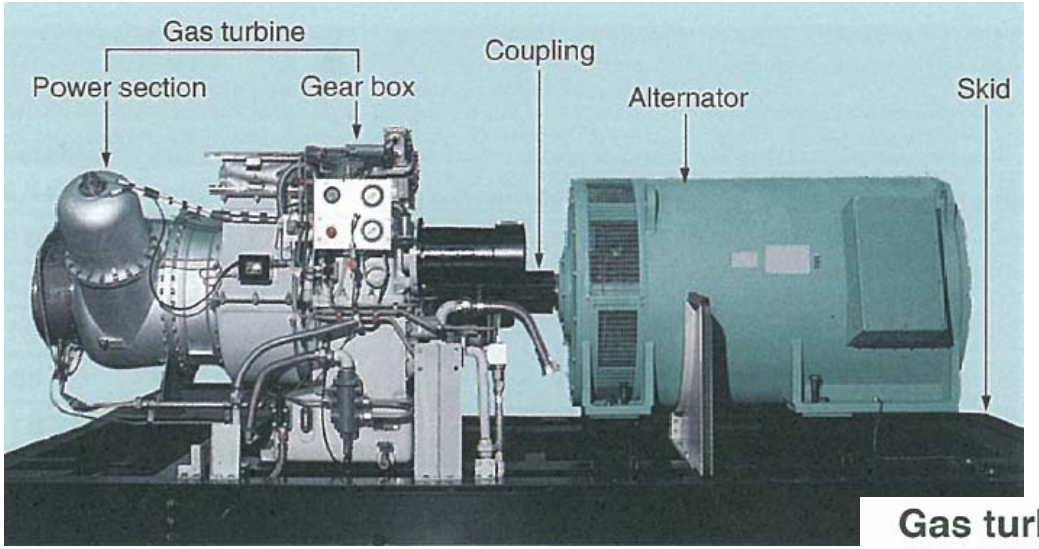
Onsite AC Power System

➢Design Features

- ✓ Class 1E AC electrical power system consists of four (4) separate trains. Each train includes one Class 1E Emergency Power Source (EPS)
- ✓ On-Line Maintenance of any EPS is allowed with Single-Failure Criterion remaining satisfied
- ✓ "Permanent" buses supplied from Alternate AC Power Source (AAC) are provided
- ✓ Non-safety related loads are not supplied from class 1E buses. Required non-safety related loads are supplied from AAC in LOOP condition

Copyright© 2007 MITSUBISHI HEAVY INDUSTRIES, LTD.

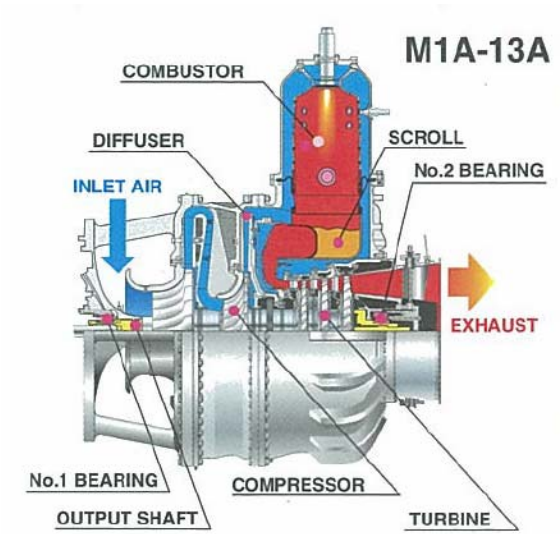
Gas Turbine Generator



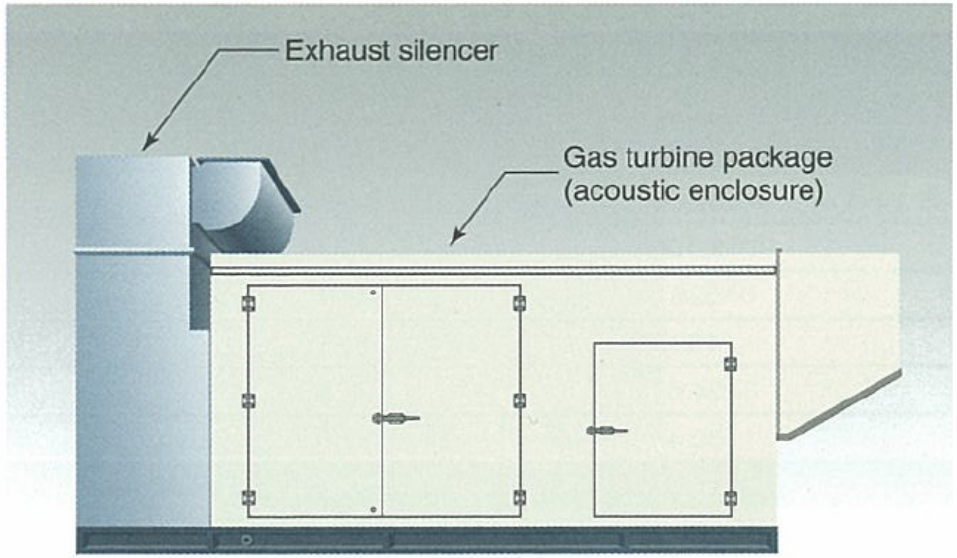
MHI selected

Gas Turbine Generators

for EPS and ACC



Gas turbine package with exhaust silencer



Copyright© 2007 MITSUBISHI HEAVY INDUSTRIES, LTD.

Why Gas Turbine Generators

✓GT/G has been selected based on reliability and maintainability improvements when compared to DG

	Gas Turbine Generator	Diesel Generator
Space	Compact	Large
Cooling Water	Not Required	Required
Routine Maintainability	1/3 the parts of a DG	Complex
Large Scale Overhaul	Once or twice during plant life	Periodic Overhaul Required
Reliability (failure/demand)	10^{-3} based on Japanese experience	10^{-2}
Starting Time	40 sec	10 sec

✓Longer start time of GT/G is accommodated by the Advanced Accumulator design of US-APWR which allows 100 sec

Copyright© 2007 MITSUBISHI HEAVY INDUSTRIES, LTD.

EPS GT/G Class 1E Qualification

- → **The EPS GT/G will meet the same requirements as the Emergency Diesel Generator**
  - → Testing per Regulatory Guide 1.9 and IEEE-387
  - → Seismic Qualification per IEEE344
- ✓ **The Qualification procedure will use the Commercial Grade Item (CGI) dedication process, per EPRI NP 5652 endorsed by NRC GL 91-05**
- ➢ **Mitsubishi plans to start the Class 1E qualification of Gas-Turbine Generator soon and will complete it by 06/2009**
- ➢ **Mitsubishi will perform the qualification program with two partner companies**
  - ✓ One has many years of experience of supplying commercial grade GT/G
  - ✓ The other has extensive experiences of supplying Class 1E DGs to US conventional NPPs, as well as Commercial Grade Dedication per EPRI NP5652

Copyright© 2007 MITSUBISHI HEAVY INDUSTRIES, LTD.

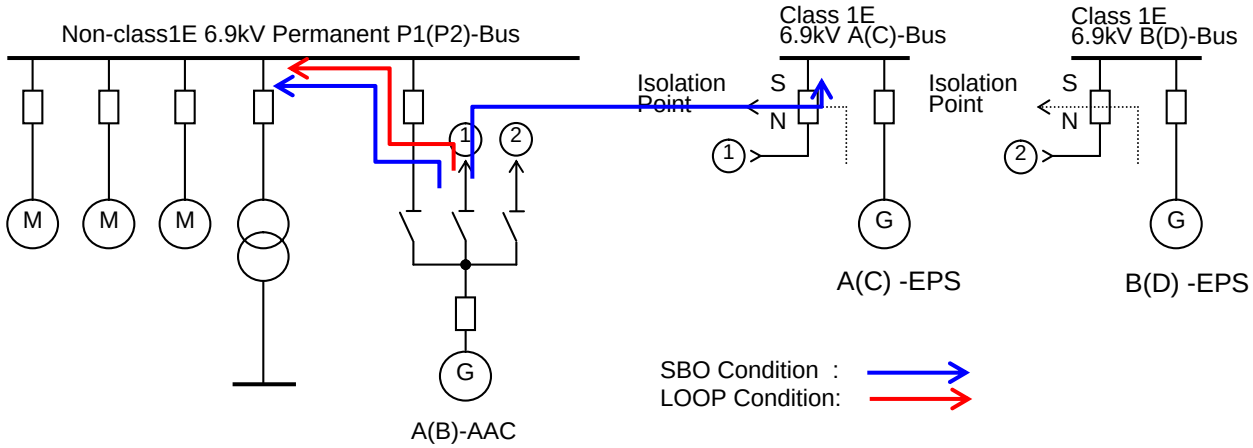
Countermeasures against SBO

➢ Alternate AC Power Source Design Basis

- ✓ The AAC is a non-class 1E gas turbine-generator package connected to a 6.9kV AC “permanent” bus
- ✓ Diverse design from EPS
  - ✓ Starting System, Capacity, etc.
- ✓ Different design and different connections minimize the potential for common mode failure with either the offsite power or the EPS system
- ✓ The AAC supplies power to loads of a class 1E bus through the tie line circuit during SBO
- ✓ The AAC supplies power to loads for 8 hours during SBO

Copyright© 2007 MITSUBISHI HEAVY INDUSTRIES, LTD.

Power supply from AACs



When a LOOP occurs, the AAC supplies to “permanent” bus automatically

Each ACC can be manually aligned to one Class 1E bus for SBO

Interlocks will prevent the AAC and EPS to be operated in parallel on same bus

Copyright© 2007 MITSUBISHI HEAVY INDUSTRIES, LTD.

Technical Specifications for Four Train Safety Systems

- **Applicable to**
  - ✓ **RPS, EPS**
  - ✓ **Safety Injection System, Containment Spray System, Containment Spray System, Residual Heat Removal System, Emergency Feedwater System, Emergency Service Water System, and corresponding portions of ESFAS/SLS**
- **Operability Requirements**
  - ✓ **2 trains required for operation**
  - ✓ **1 additional train required to meet single failure criterion**
  - ✓ **1 train available for On Line Maintenance (no Tech Spec limitation)**
- **Limiting Condition for Operation**
  - ✓ **When less than 3 independent trains operable**
  - ✓ **Allowed Outage Time (AOT) based on Configuration Risk Management Program (CRMP) which manages the increase in risk that may result from maintenance work**

Copyright© 2007 MITSUBISHI HEAVY INDUSTRIES, LTD.

Summary

- **MHI I&C and Electrical Systems provide significant advancements to**
  - ✓ improve plant safety and availability
  - ✓ reduce operations and maintenance costs
- **The systems employ proven designs with many years of demonstrated reliability**
- **MHI is working closely with NRC and NEI to achieve US licensing for the US-APWR and for operating plant modernization**

Copyright© 2007 MITSUBISHI HEAVY INDUSTRIES, LTD.