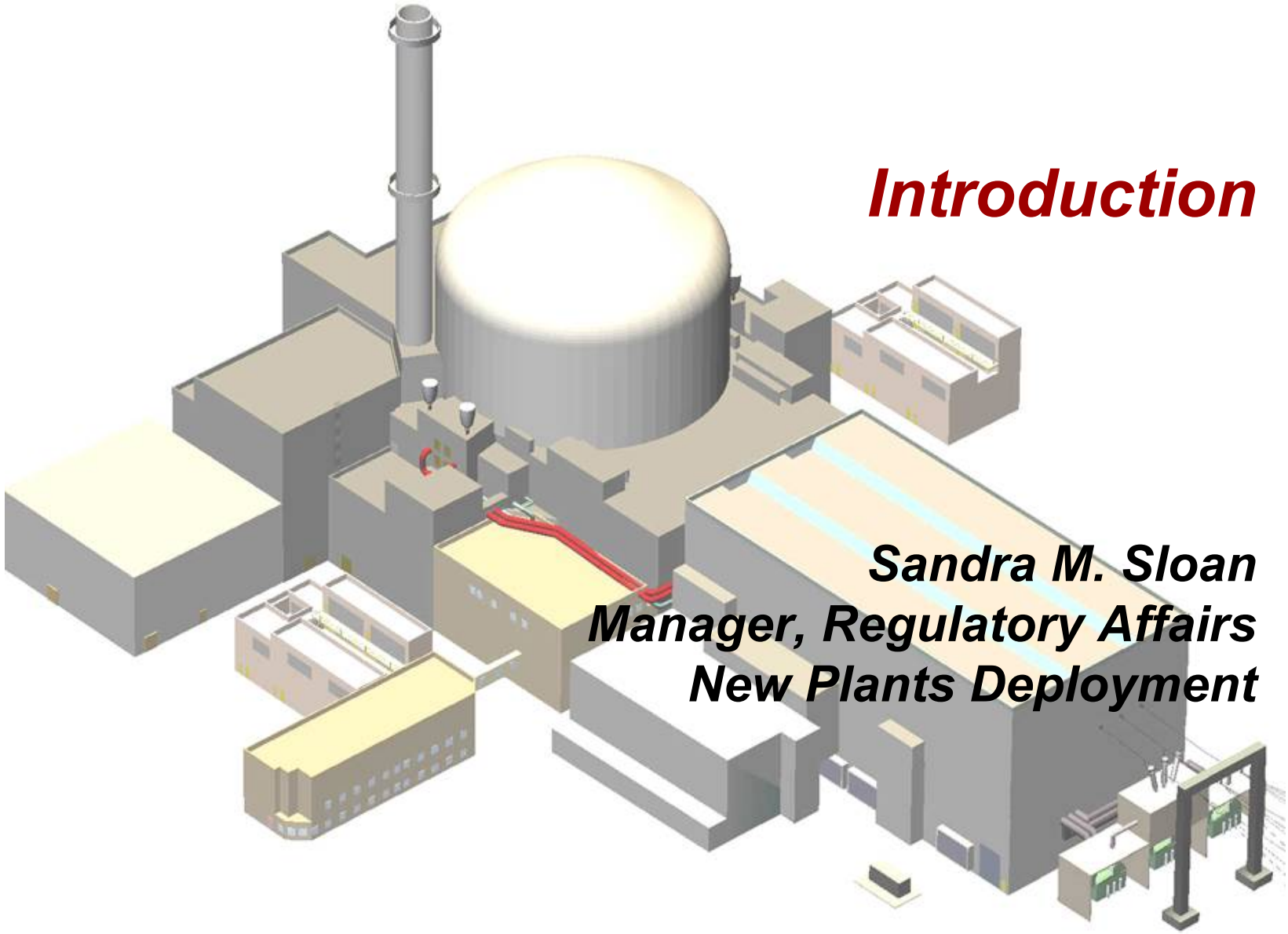
U.S. EPR Pre-Application Review Meeting: I&C Systems Overview and Protection System

AREVA NP Inc., Constellation Energy and the NRC
April 27, 2006

AREVA



Introduction

Sandra M. Sloan
Manager, Regulatory Affairs
New Plants Deployment

EPR

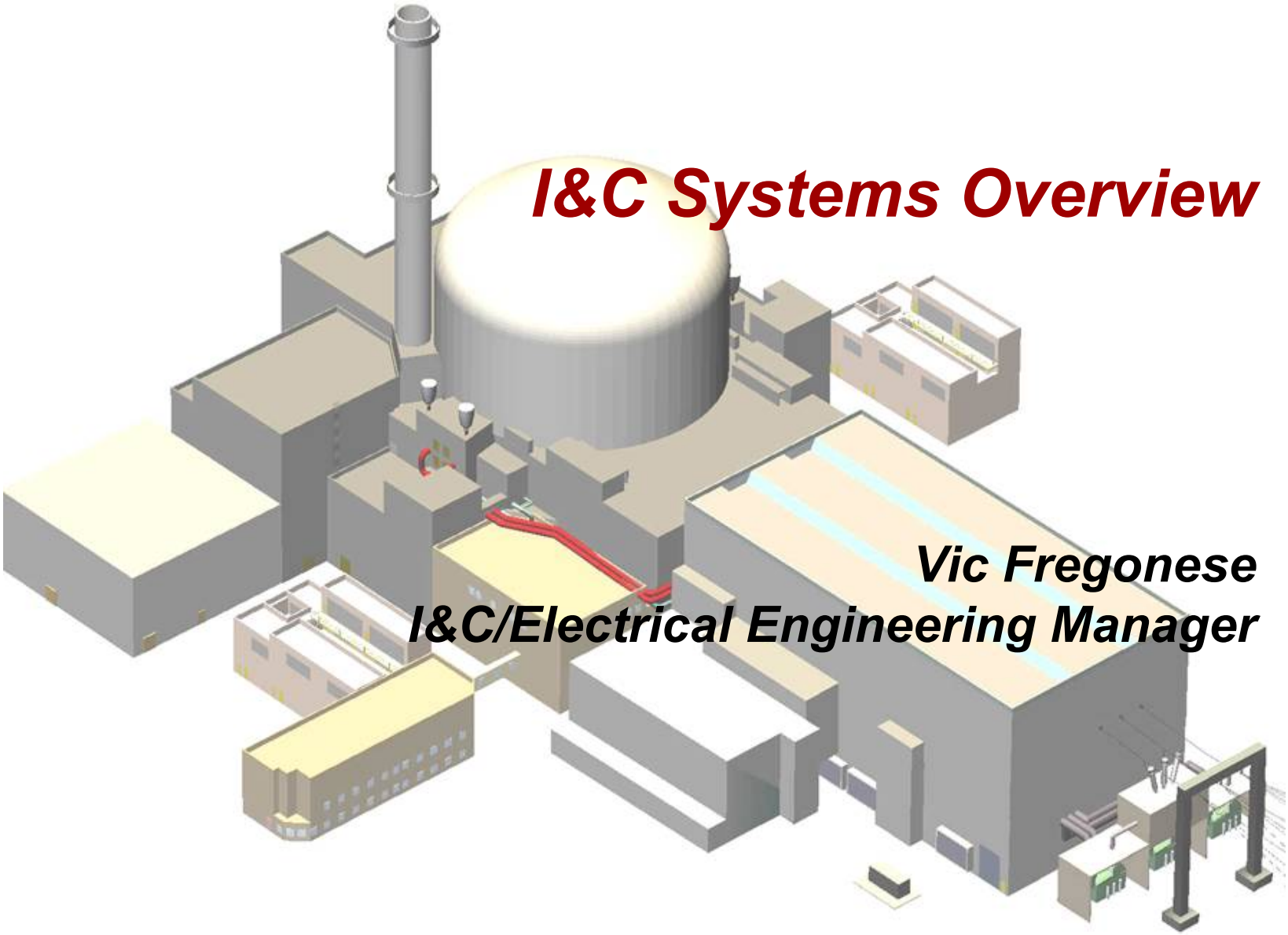
Meeting Objectives

- Describe the approach for the design of I&C systems for the U.S. EPR
- Provide an overview of the design of safety, operational, and diverse I&C systems
- Provide an overview of the approach to U.S. EPR control room design and human factors engineering
- Opportunity for early identification of NRC concerns with the I&C system design strategy

Outline

- Update on the Status of the U.S. EPR Design Certification
- I&C Systems Overview
- Protection System
- Summary and Next Steps

I&C Systems Overview



Vic Fregonese

I&C/Electrical Engineering Manager

Topics

- World-Wide Experience
- I&C Design Approach
- Digital I&C Design Goals and Objectives
- Current Activities and Planned Activities
- Timeline
- I&C Architecture
  - Safety I&C
  - Operational I&C
  - Diverse I&C
- HFE & Control Complex
- Software Development
- Protection System

AREVA Worldwide Experience

Digital Safety I&C
Worldwide Orders/Installations

- **50 NPP units worldwide**
- **Located in 11 countries**
- **9 different reactor OEMs**
- **More than 8000 years of processor modules operation time**

AREVA Supports the Entire I&C System Design Life Cycle

- Research and Development
- Application Software
- Detailed Design
- Manufacturing
- Factory and Site Acceptance Testing
- Training and Simulator Development
- Implementation
- Configuration Management
- Operational Support

U.S. EPR I&C Systems – Design Approach

- OL3 is the base plant design
- Systematic process to prepare the design for U.S. deployment
- Conversion to U.S. design codes & standards
- Address compliance with NRC regulations and QA requirements
- Operating experience addressed through regulatory compliance assessment process
- Use of Global Competence Team to develop and implement worldwide EPR I&C design concepts --> standardization
- Loan U.S. employees for OL3 electrical, I&C, and control room design team

Digital I&C – Goals and Objectives

Improved I&C Safety, Performance and Reliability

- Improved safety/reliability
  - Actuate trips when needed
  - Avoid spurious actuation
- Improved maintainability
  - On-line testing and diagnostics
  - On-line maintenance without impact to plant operation or system operability
- Improved automation
  - Automatic limitation functions to avoid protection system actuation
- Improved information management for operators
- Support advanced plant PRA goals
- Support advanced plant staffing goals
- World-wide standardization to maximum extent possible
- Acceptance by international regulatory authorities

Digital I&C – Design Team Core Focus Areas

> **Reactor Safety**
  - Understand the technology of the facility and maintain design conservatism
  - Protect the design basis - understand and maintain the design basis

> **Configuration Control**
  - Ensure that changes to design configuration conform to design requirements and are accurately reflected in the facility configuration information
  - Ensure that alignment of in-service equipment is consistent with the design
  - Ensure that equipment is procured and maintained in accordance with the design

> **Plant Operations**
  - Ensure plant operators understand the functions, characteristics, and operating limits of the equipment, in order to safely control it
  - Ensure human factors integration with design and configuration control

> **Plant Maintenance**
  - Ensure plant maintenance staff understands the equipment to support successful execution and control of maintenance required to keep the equipment within operating parameters

Current Activities

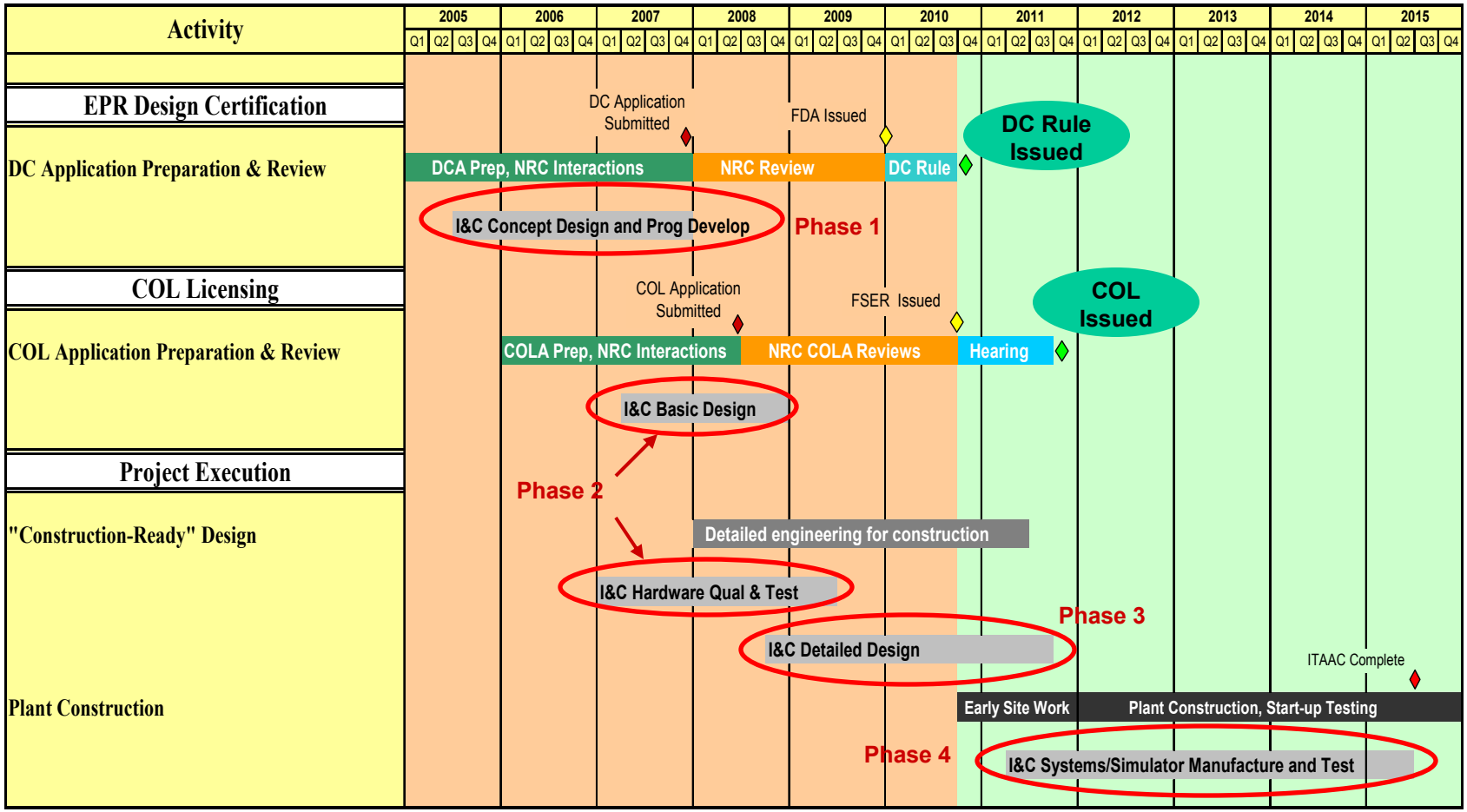
- OL3 reference plant
  - Under construction in Finland
  - 2009 commercial operation
  - I&C systems in design freeze process
  - I&C manufacturing started
  - HSI design in progress
  - Simulator development in progress

- U.S. EPR deployment
  - DCD development for December 2007 submittal
  - COLA development for June 2008 submittal
  - Design continuum development
  - I&C licensing and design basis reconciliation
  - I&C Global Competence Team oversight

Planned Activities

- I&C Design Process
  - Phase 1 – Conceptual Design
  - Phase 2 – Basic Design
  - Phase 3 – Detailed Design
  - Phase 4 – Manufacturing/Testing/Installation

Planned Activities - Timeline

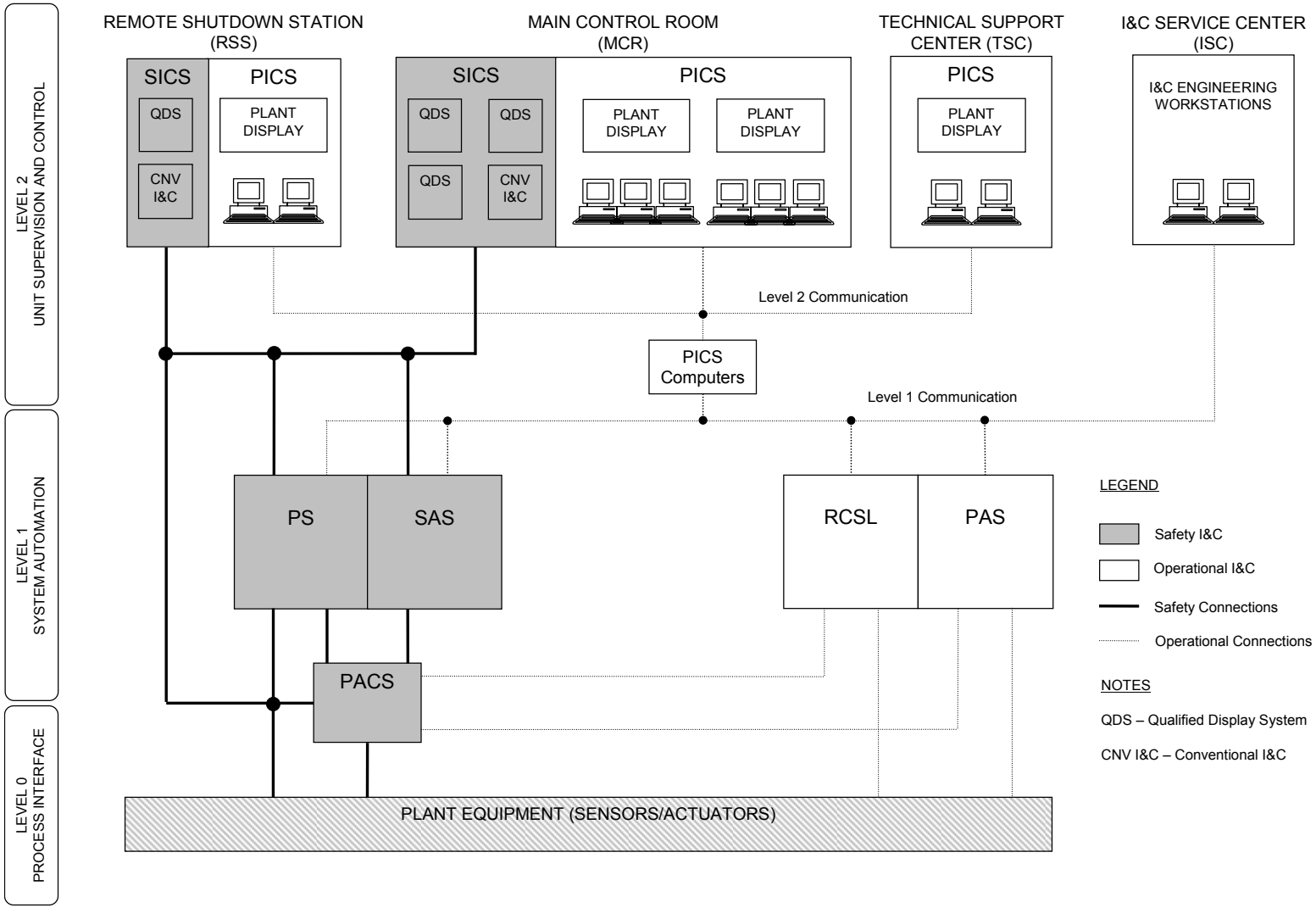


EPR I&C Systems

- **Safety I&C**
  - Protection System (PS)
  - Safety Automation System (SAS)
  - Priority Actuation and Control Systems (PACS)
  - Safety Information and Control System (SICS)
- **Operational I&C**
  - Reactor Control, Surveillance, and Limitation (RCSL)
  - Process Automation System (PAS)
  - Process Information and Control System (PICS)
  - Diverse I&C
- **System alignment to SRP* sections**
  - 7.2 – PS
  - 7.3 – PS, PACS
  - 7.4 – SAS, PACS
  - 7.5 – SICS
  - 7.6 – PS
  - 7.7 – RCSL, PAS, PICS
  - 7.8 – Operational I&C
  - 7.9 – ALL

*Revision 4, June 1997

I&C Systems Architecture



Safety I&C Systems

- Protection System (PS)
  - Reactor trip
  - ESFAS
  - Safety permissives (interlocks)
- Safety Automation System (SAS)
  - Safe shutdown functions
- Priority Actuation and Control System (PACS)
  - Prioritization between safety and operational inputs
- Safety Information and Control System (SICS)
  - Post accident/safety parameter monitoring (QDS)
  - Manual controls of safety system functions and actuators

Operational I&C Systems

- Reactor Control, Surveillance, and Limitation (RCSL)
  - Reactor control functions (i.e. Rods, Boron)
  - Primary plant control functions (i.e. Pzr. Pressure, Pzr. Level)
  - S/G Level
  - Limitation functions – reduce challenges to PS
- Process Automation System (PAS)
  - Balance of plant controls
  - Turbine controls
- Process Information and Control System (PICS)
  - Operator display and interface with all plant systems

Diverse I&C

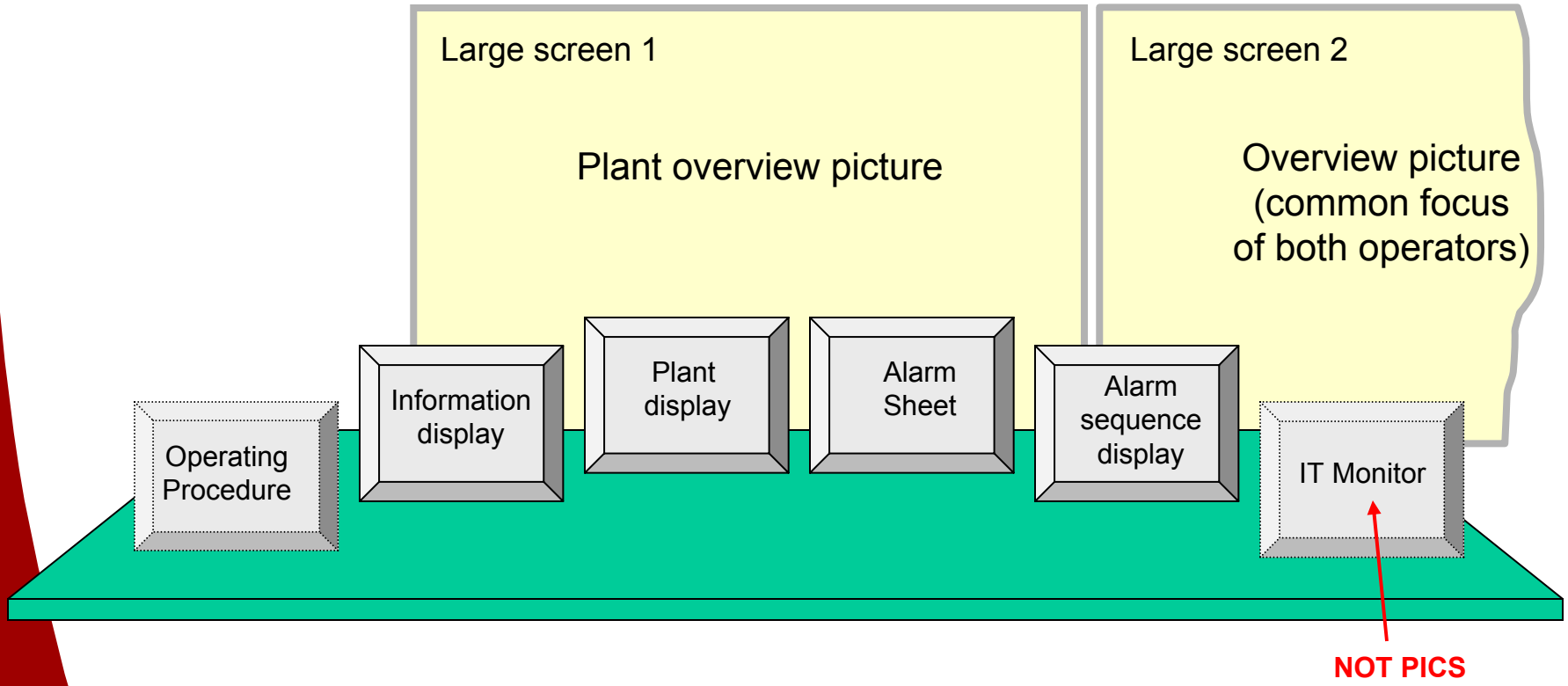
- Diversity for common mode failure of protection system (Branch Technical Position 19) and ATWS
  - ATWS mitigation functions per 10 CFR 50.62
  - Automatic actuation of safety systems via system diverse from PS
  - Manual actuation of safety systems that bypasses the PS is used for accidents not requiring automatic action (with associated diverse indication)

PICS Concept of Operations

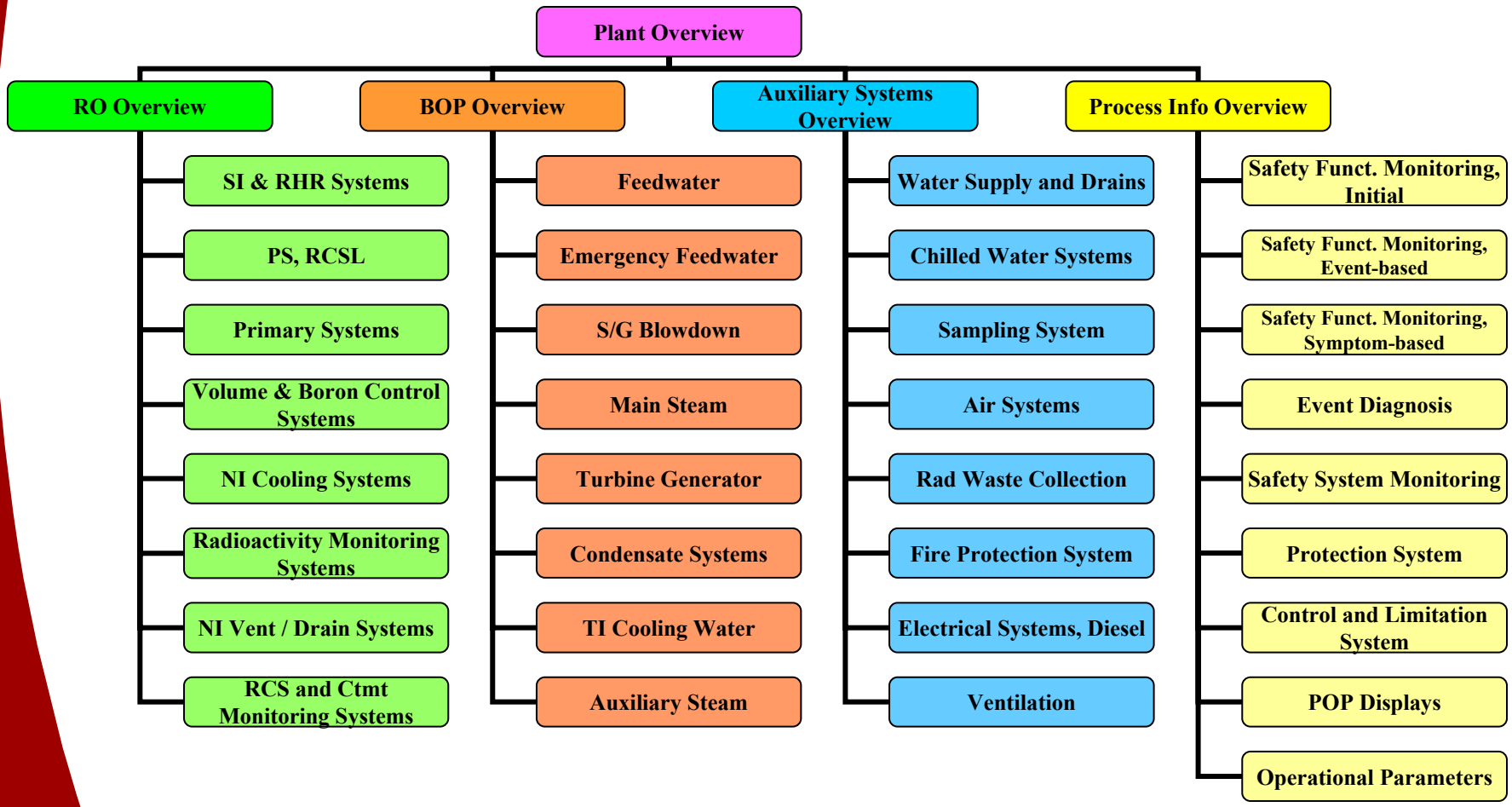
- Essentially all operations are performed using PICS, including emergency operations, as long as PICS is available
- SICS is intended for use in the unlikely event of total unavailability of PICS
- Administrative controls drive the recovery of PICS or require shutdown via SICS

PICS Displays

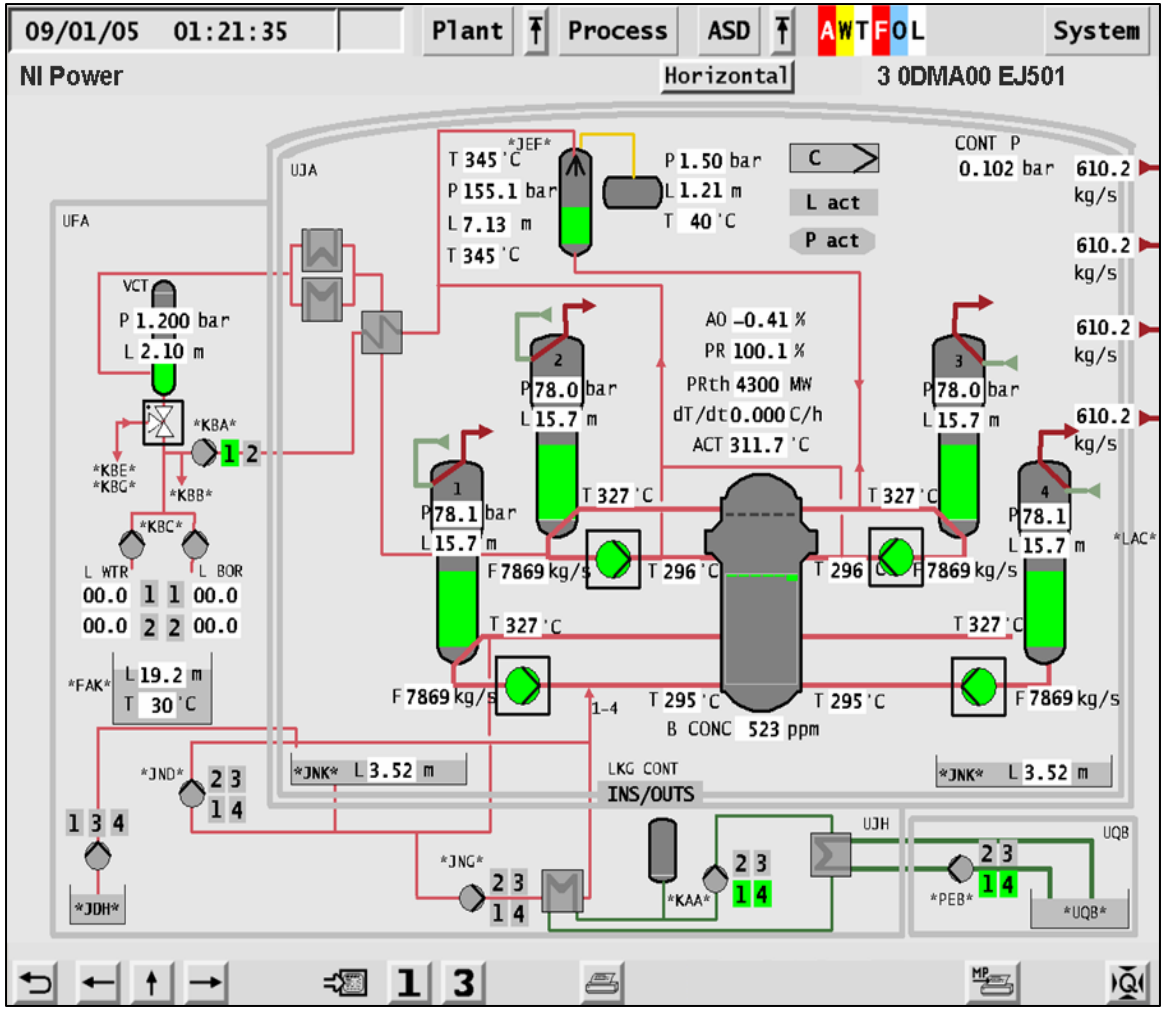
Workstation - Typical Assignment of Screens



PICS Screen Navigation

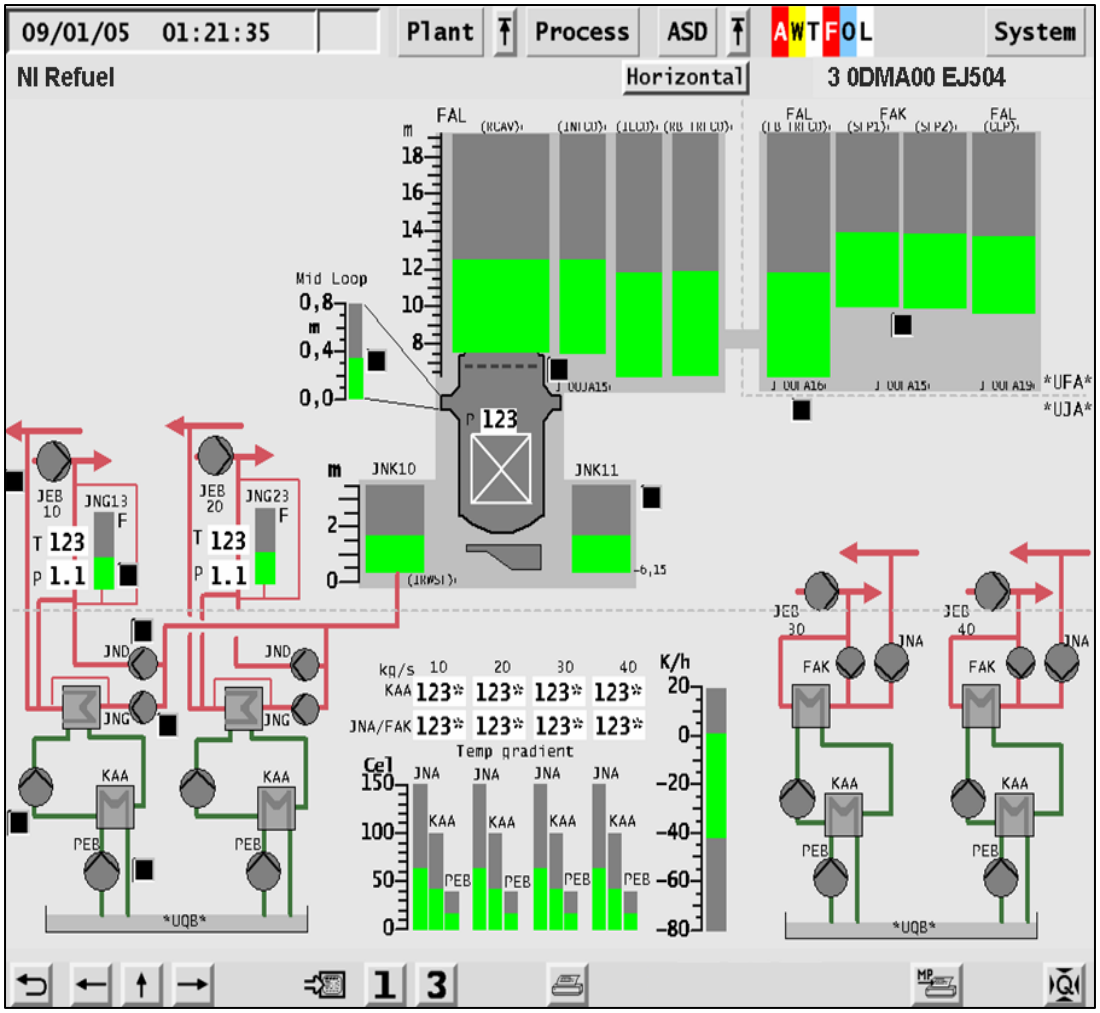


Plant Overview Displays (OL3)



Power Operation

Plant Overview Displays (OL3)



Refueling Operation

HFE Program

- DCD Chapter 18 to be completed to the level of detail required by SRP chapters 14.3.9 and 18 consistent with NUREG-0711 and precedent
- U.S. EPR HFE topical report to be submitted in 1QCY 2007 for early review and issue resolution
- DCD submittal to include implementation plans for:
  - Operating Experience Review (HFE)
  - Functional Requirements Analysis
  - Functional Allocation
  - Task Analyses
  - HSI Design
  - V&V
  - Design Implementation
  - Human Performance Monitoring
- Documentation of assumptions related to staffing and training in process
- Operating manual being developed in conjunction with COL applicant – drives procedure development

Software Development Plan

> The AREVA software life-cycle design approach meets BTP-14 requirements and addresses:

- Software Quality Assurance
- Software Configuration Management
- Software Verification and Validation
- Software Operations and Maintenance
- Documentation
- Problem Reporting and Corrective Actions

Potential for early submittal of a software program manual via topical report

Protection System

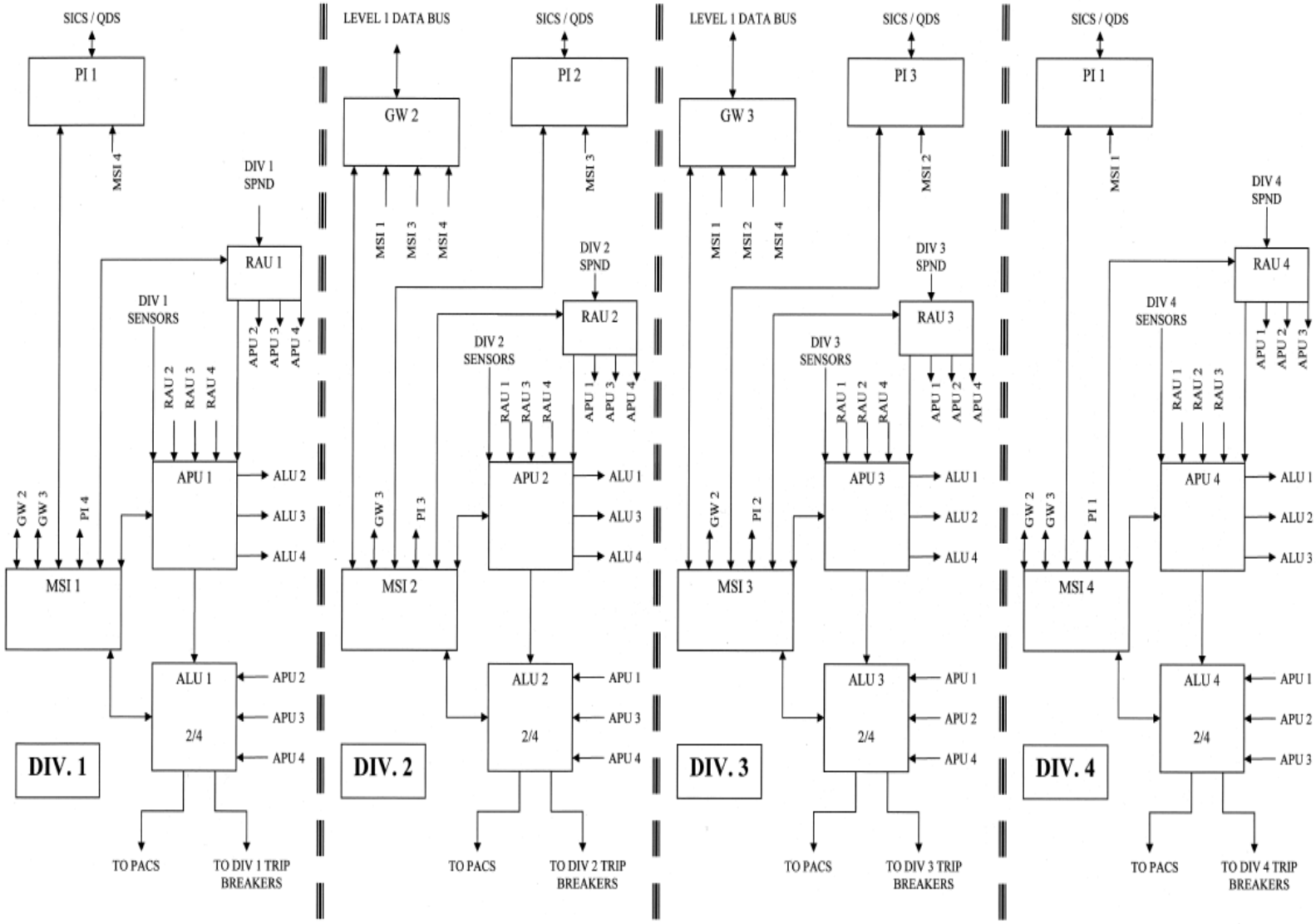
Protection System - Design Features

- **Functionality**
  - Performs reactor trip, ESF functions, safety permissives
  - Each division generates a trip decision per parameter
  - Each division votes 2/4 on trip decisions from all 4 divisions
  - In case of failure of one division, other divisions vote 2/3
- **Redundancy**
  - 4 redundant divisions
  - Redundant voting within each sub-system
- **Functional diversity for reactor trips**
  - 2 functionally diverse sub-systems per division
- **Reliability and availability**
  - Protection against spurious trips
  - Protection against unavailability of ESF functions

Protection System - Function Block Definitions

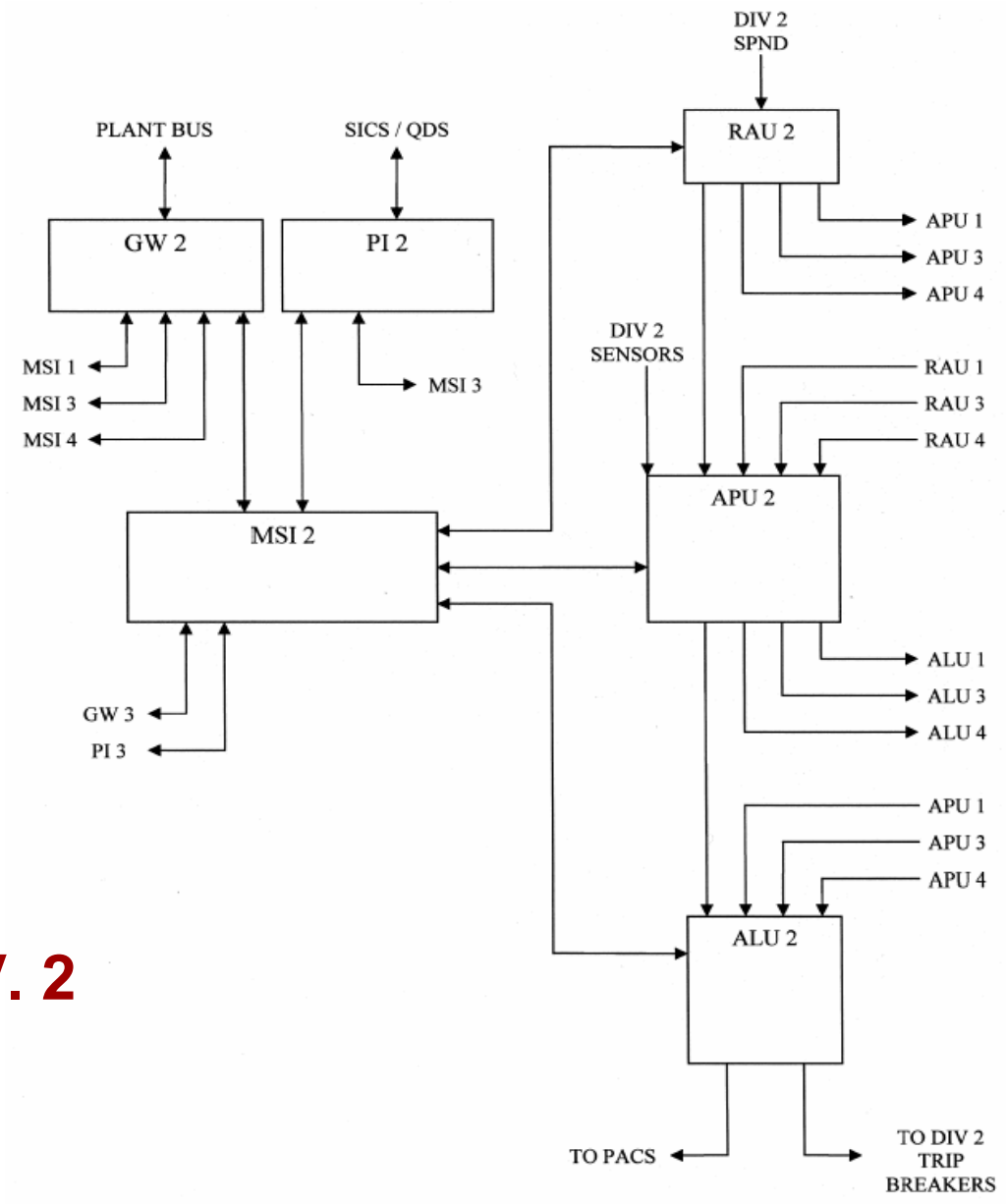
- RAU: *Remote Acquisition Unit*
  - Acquires in-core instrumentation, distributes to APUs
- APU: *Acquisition and Processing Unit*
  - Acquires process sensors, performs threshold detection and processing functions, distributes to ALUs
- ALU: *Actuation Logic Unit*
  - Performs voting of trip decisions from APUs, issues actuation orders to trip devices and PAC modules
- MSI: *Monitoring and Service Interface*
  - Provides 1E / non-1E isolation, performs data transfer and monitoring functions
- PI: *Panel Interface*
  - Provides 1E interface to safety displays
- GW: *Gateway*
  - Provides interface to operational I&C

Protection System Block Diagram



4 Divisions – Increased Safety and Reliability

Protection System Block Diagram



DIV. 2

Protection System - Reactor Trip Logic

APU*X Y*

X= Division

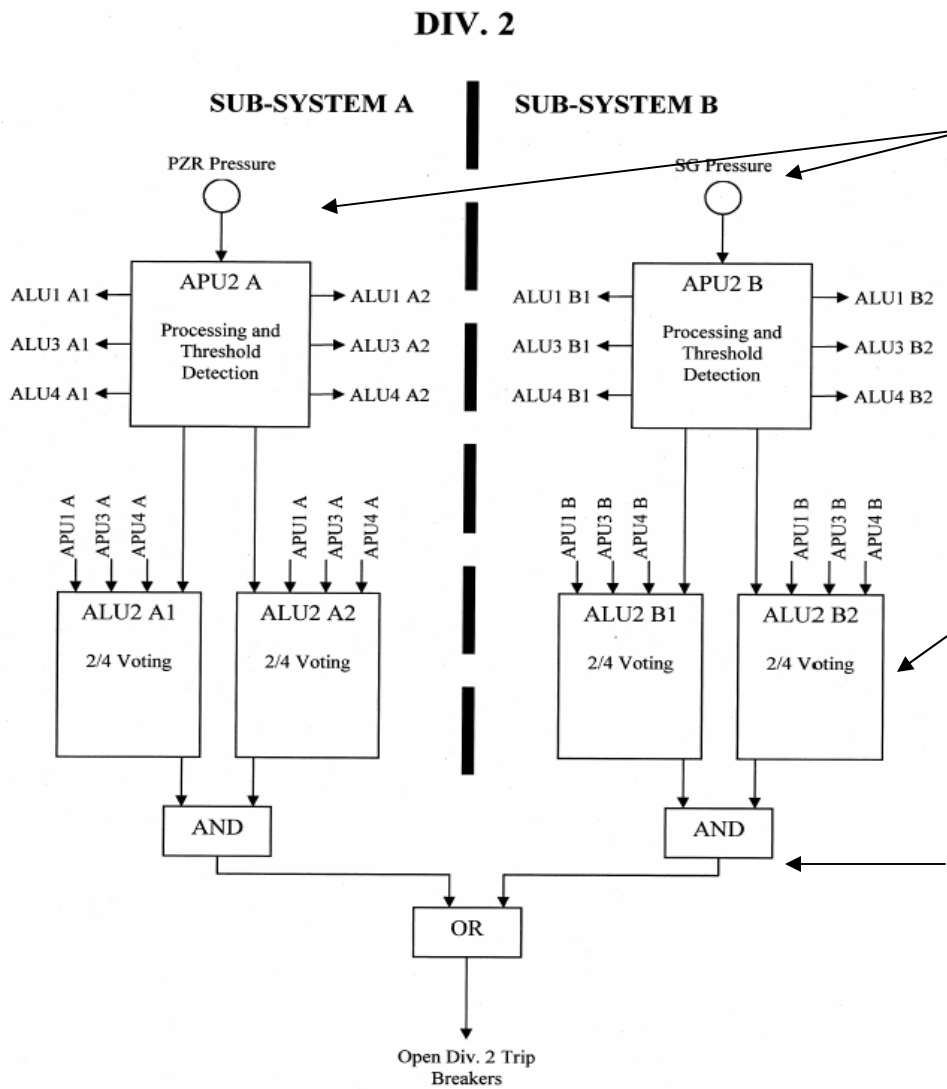
Y= Sub-system

ALU*X YZ*

X= Division

Y= Sub-system

Z= Redundancy



Functional diversity

Redundant voting per sub-system

Protection against spurious trip

Safe & Reliable - 2 Sub-Systems and Redundant Voting

Protection System – ESF Logic

APU*X Y*

X **= Division**

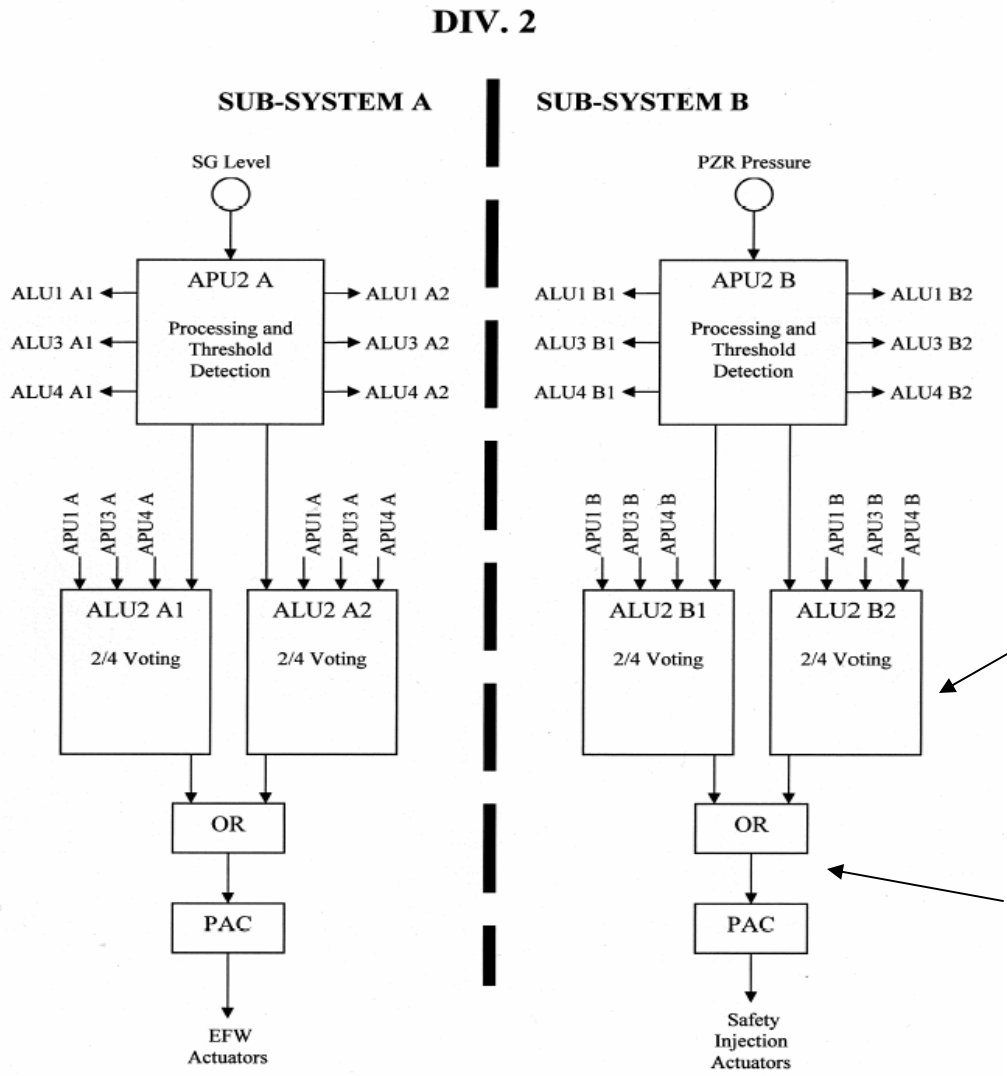
Y **= Sub-system**

ALU*X YZ*

X **= Division**

Y **= Sub-system**

Z **= Redundancy**

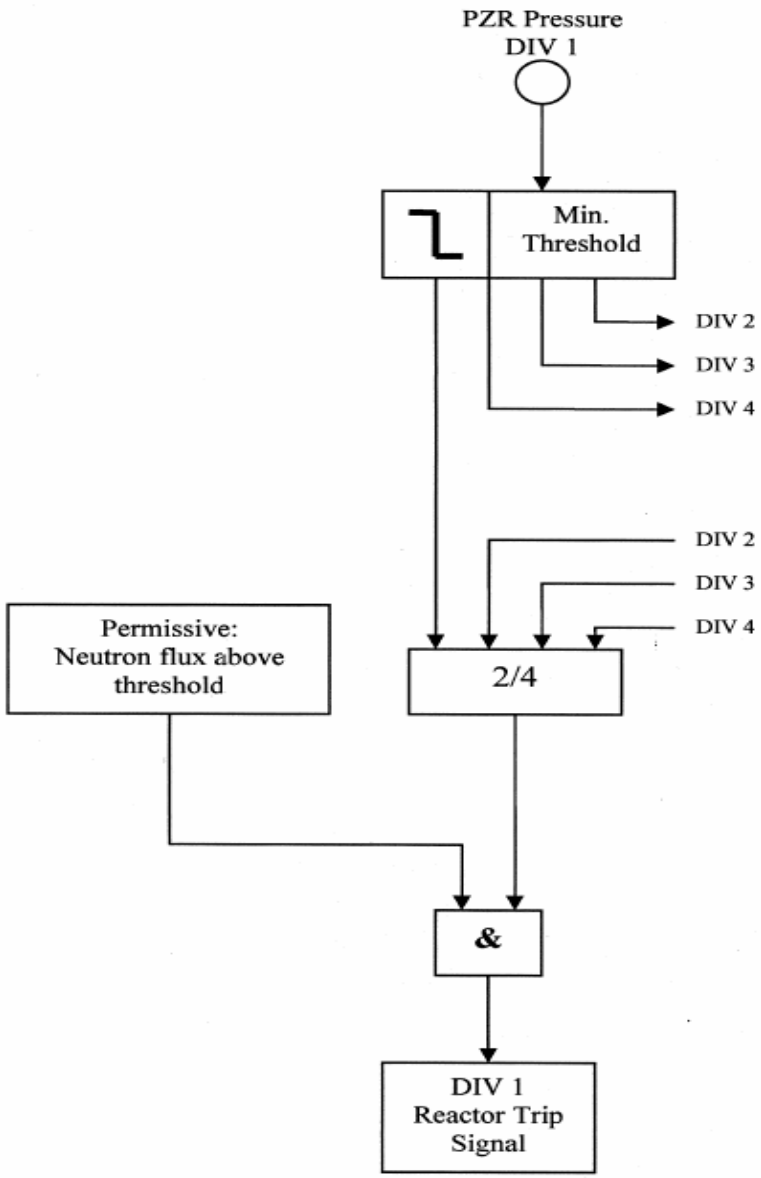


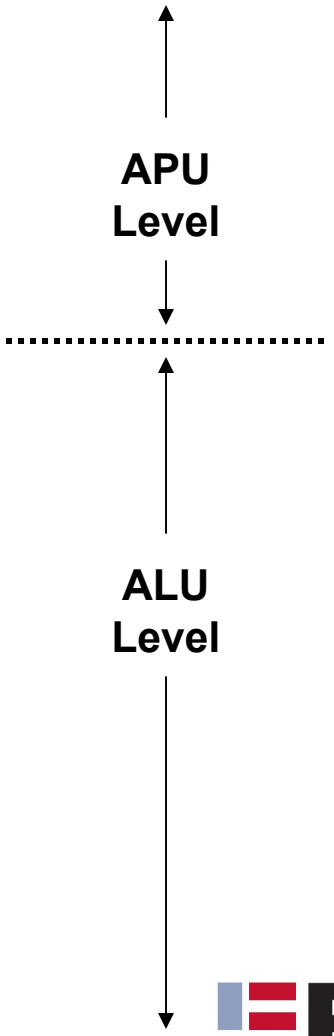
Redundant voting per sub-system

Protection against ESF unavailability

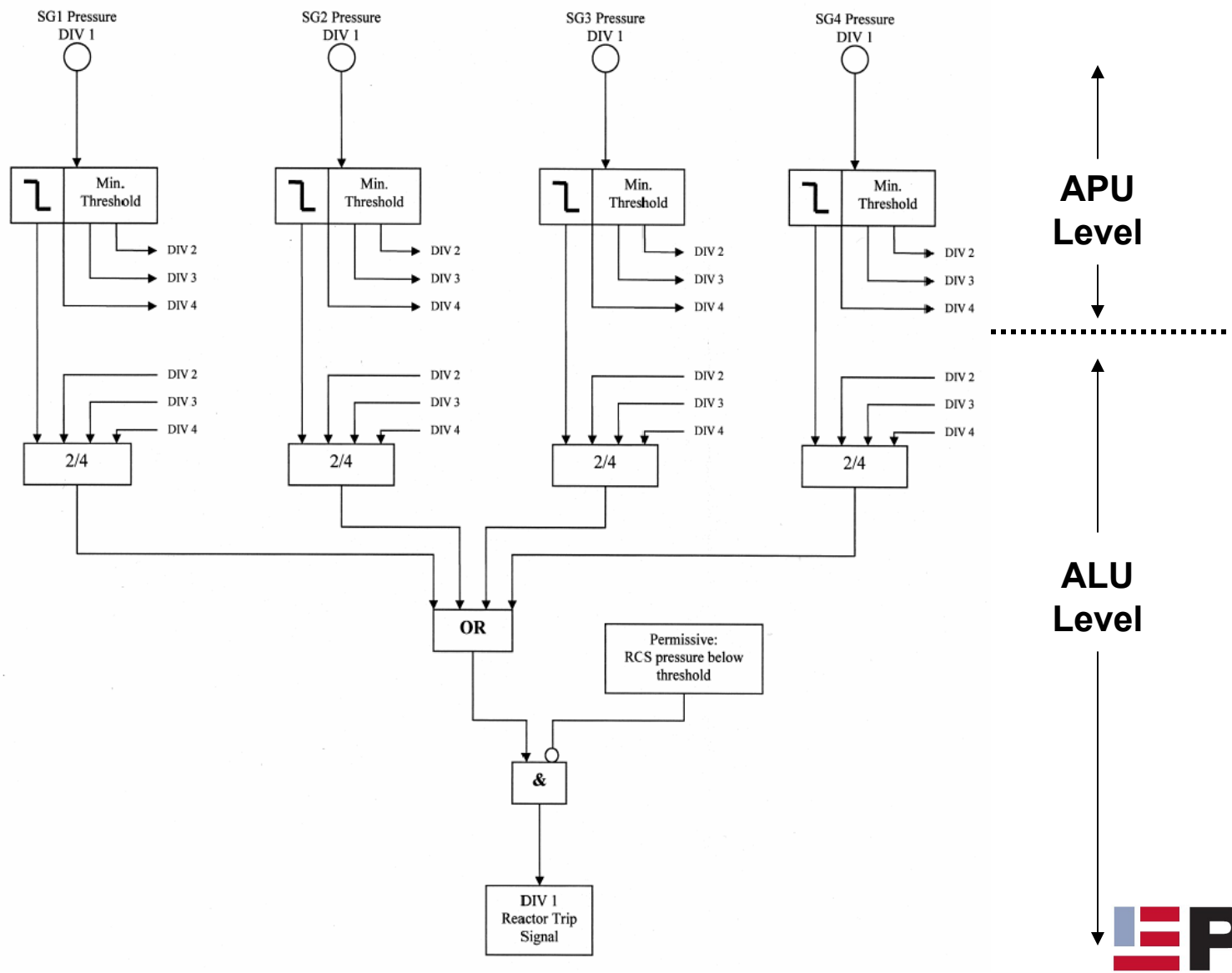
Safe & Reliable - 2 Sub-Systems and Redundant Voting

Pressurizer Pressure Trip Logic Example

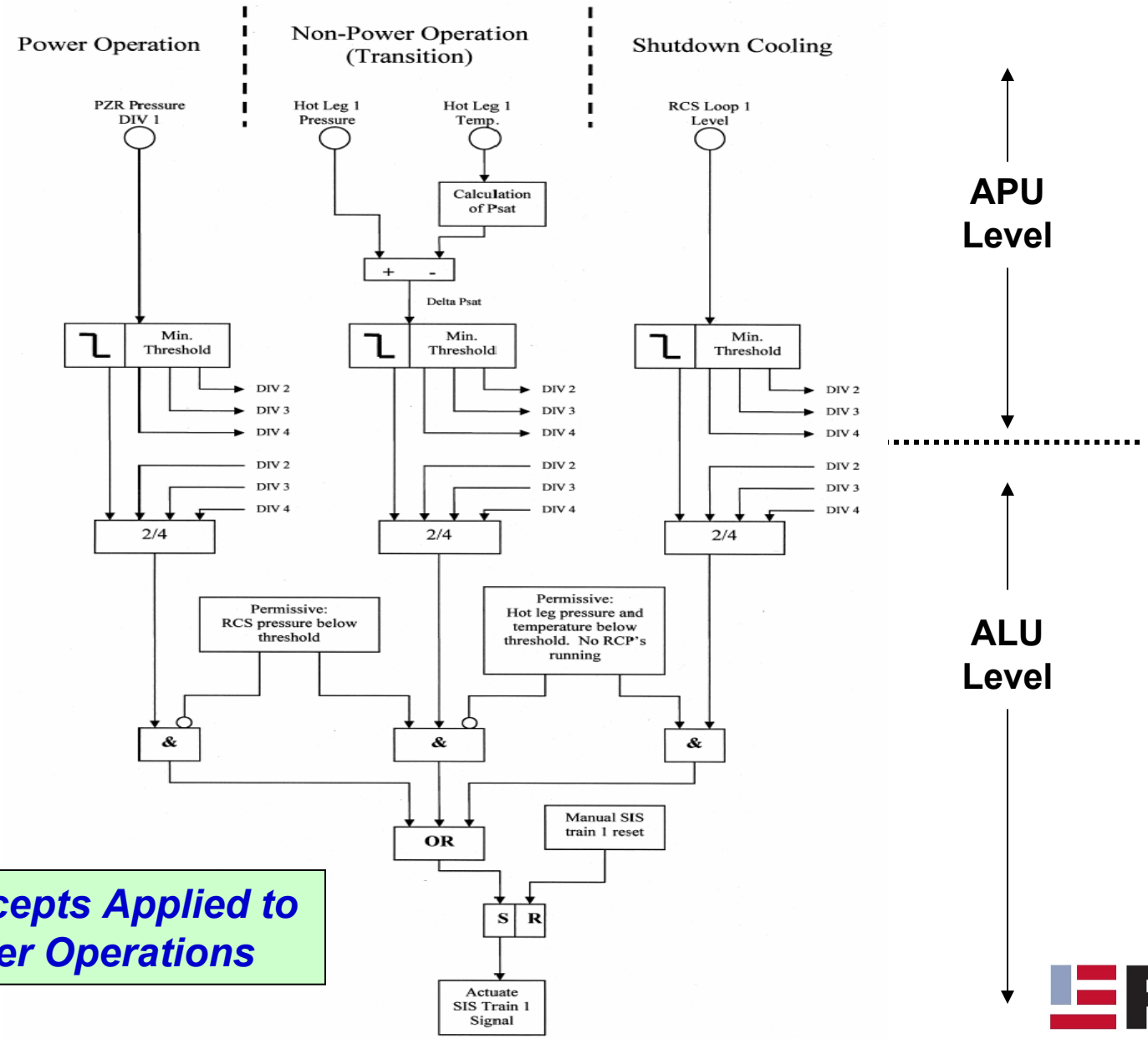




Steam Generator Pressure Logic Example

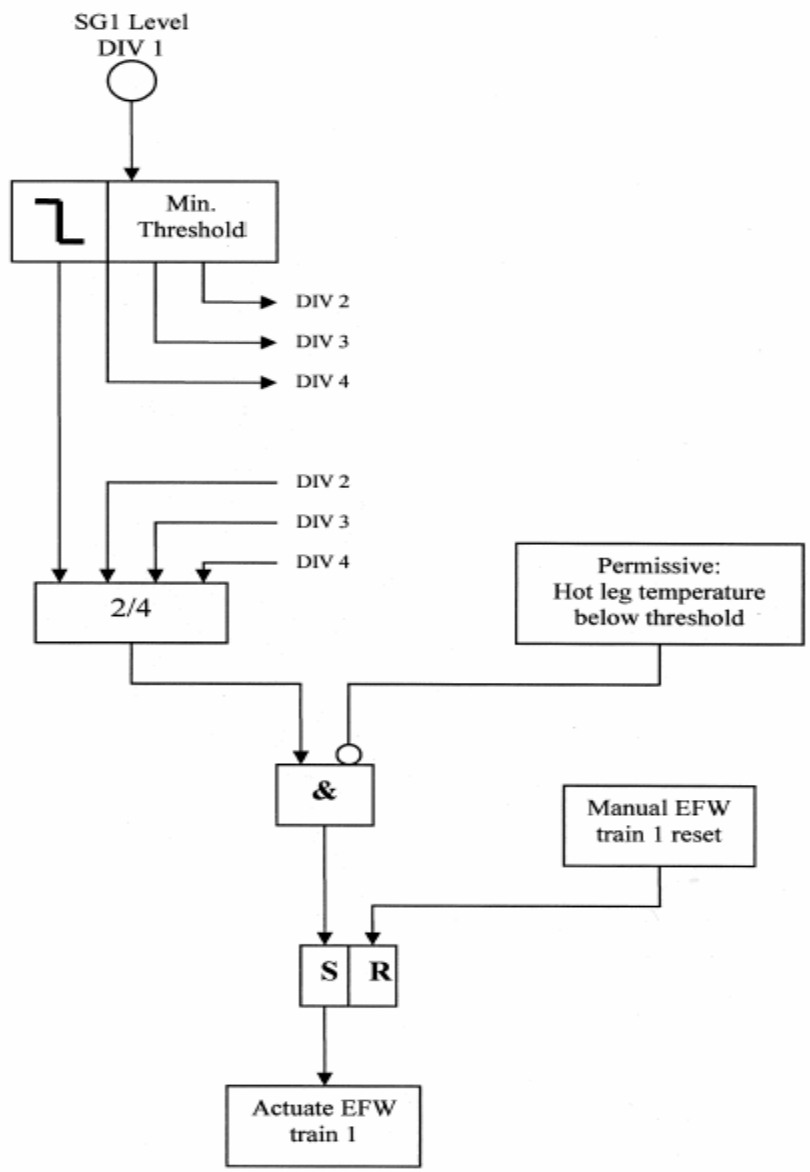


Safety Injection Logic Example



Safety Concepts Applied to Non-Power Operations

Emergency Feedwater Logic Example



APU Level

ALU Level

Summary

- U.S. EPR I&C systems design and control room/HFE design will use insights gained from the design of OL3
- U.S. EPR I&C systems design will address applicable NRC standards and requirements and will incorporate insights gained from operating experience
- U.S. EPR I&C system design will use proven technology
- AREVA supports the entire system design life cycle

The U.S. EPR I&C system design will offer improved safety, performance and reliability.

Engineering and Maintenance Training

Next Steps

Planned I&C Meetings	Date
I&C System Architecture	August 2006

Planned I&C Submittals	Date
Incore and nuclear instrumentation design report	4Q CY 2006
Human factors report	1Q CY 2007
Digital protection system design report	1Q CY 2007
Instrument setpoint methodology report	1Q CY 2007
I&C diversity and defense-in-depth report	2Q CY 2007

AREVA support of key industry activities:

> NEI I&C Working Group Meeting – May, 2006

> NRC SRP Ch. 7 Update – September, 2006 (2 sections & 2 BTPs)

> DG-1145 Workshops – Date for Chapter 7 TBD

Handouts

Acronyms

PS: Protection System

SAS: Safety Automation System

PACS: Priority Actuation & Control System

SICS: Safety Information & Control System

RCSL: Reactor Control, Surveillance, & Limitation System

PAS: Process Automation System

PICS: Process Information & Control System

QDS: Qualified Display System

RAU: Remote Acquisition Unit

APU: Acquisition & Processing Unit

ALU: Actuation Logic Unit

MSI: Monitoring & Service Interface

PI: Panel Interface

GW: Gateway