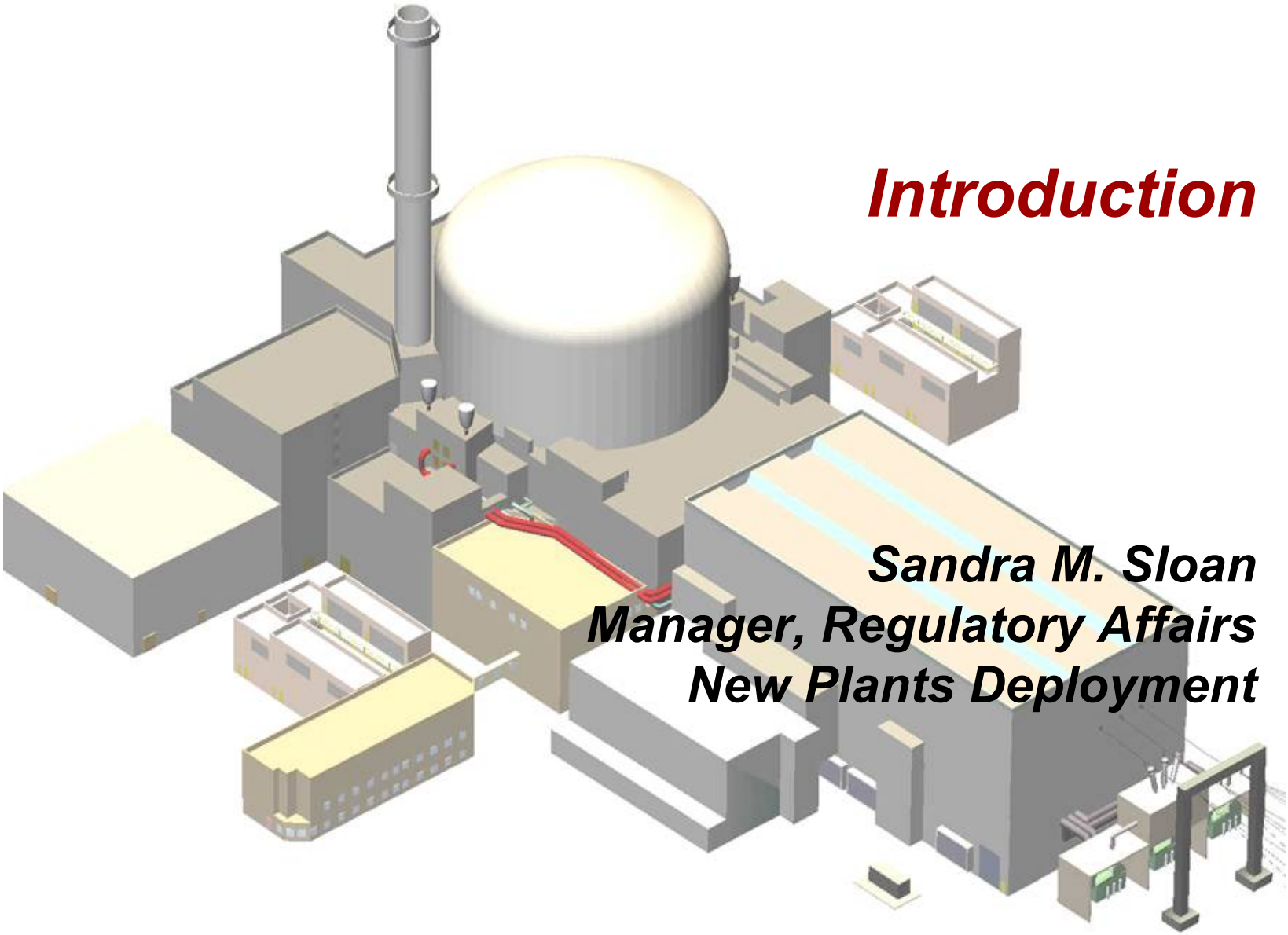
U.S. EPR Pre-Application Review Meeting: I&C Diversity and Defense-in-Depth Methodology Topical Report

AREVA NP Inc. and the NRC
May 3, 2007

AREVA



Introduction

Sandra M. Sloan
Manager, Regulatory Affairs
New Plants Deployment

EPR™

Agenda

- Introduction and meeting objectives (S. Sloan)
- Diversity and Defense-in-Depth (J. Shook)
  - U.S. EPR I&C Architecture
  - Diversity and Defense-In-Depth Methodology
- Summary and next steps (S. Sloan)

Meeting Objectives

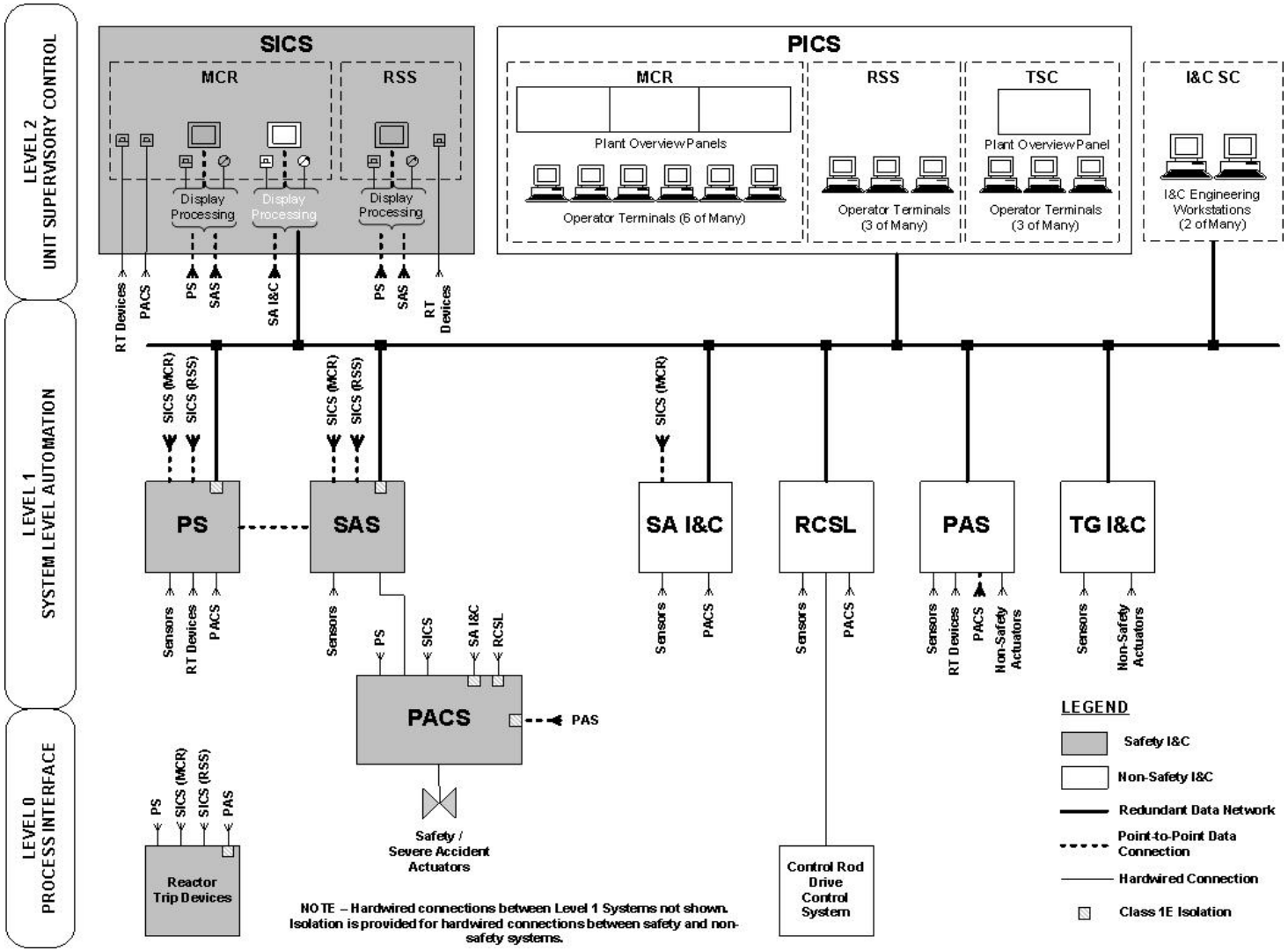
- Provide an overview of the U.S. EPR I&C architecture and the diversity and defense-in-depth design features included
- Provide follow-up to August 31, 2006 meeting on I&C systems overview and special topics
- Provide an overview of the diversity and defense-in-depth methodology
- Provide an opportunity for early NRC feedback on the I&C Diversity and Defense-in-Depth Methodology Topical Report

I&C Diversity and Defense-in-Depth Technical Discussion

Jeremy Shook
I&C Project Engineer

U.S. EPR I&C Architecture

U.S. EPR I&C Architecture



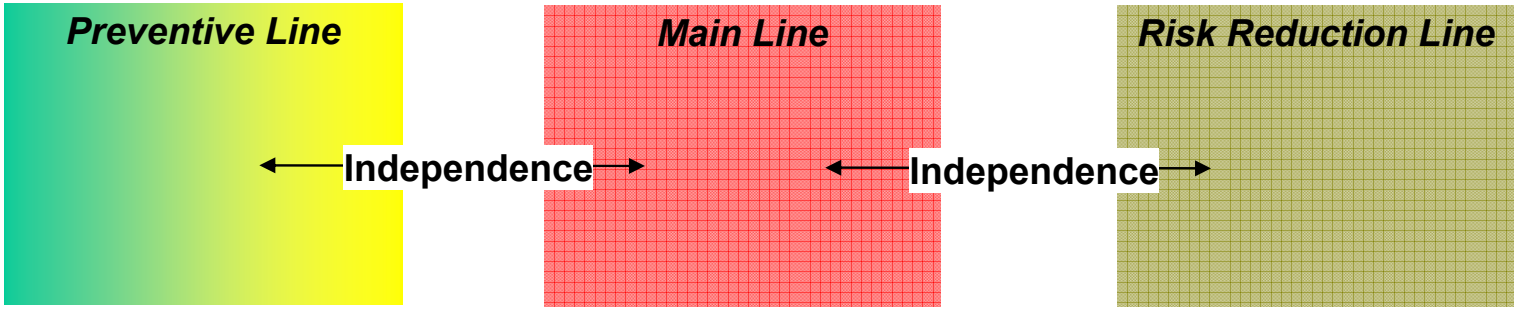
U.S. EPR I&C Defense-In-Depth: Lines of Defense

- **Preventive Line of Defense**
  - **Prevent departures from normal operation**
  - **Cope with deviations from normal operation in order to prevent their evolution into accidents**
- **Main Line of Defense**
  - **Mitigate DBE's and prevent their evolution into severe accidents by engineered safety features and reactor trip systems**
- **Risk Reduction Line**
  - **Cope with the complete loss of engineered safety features and protective systems by risk reduction functions**
  - **Preserve the integrity of the containment in the case of severe accidents by special core melt retention and cooling devices**

U.S. EPR I&C Defense-In-Depth: I&C Functions to Support Lines of Defense

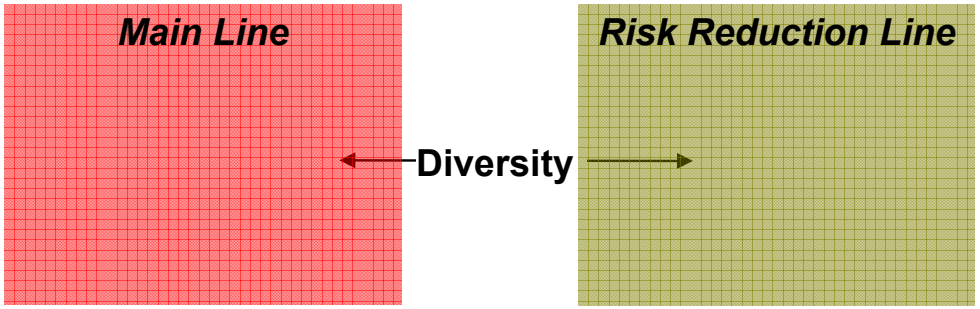
Line of Defense	I&C Functions
Preventive Line	>Operational functions >Limitation functions
Main Line	>Safety functions
Risk Reduction Line	>Risk Reduction functions

U.S. EPR I&C Defense-In-Depth: Independence Between Lines of Defense

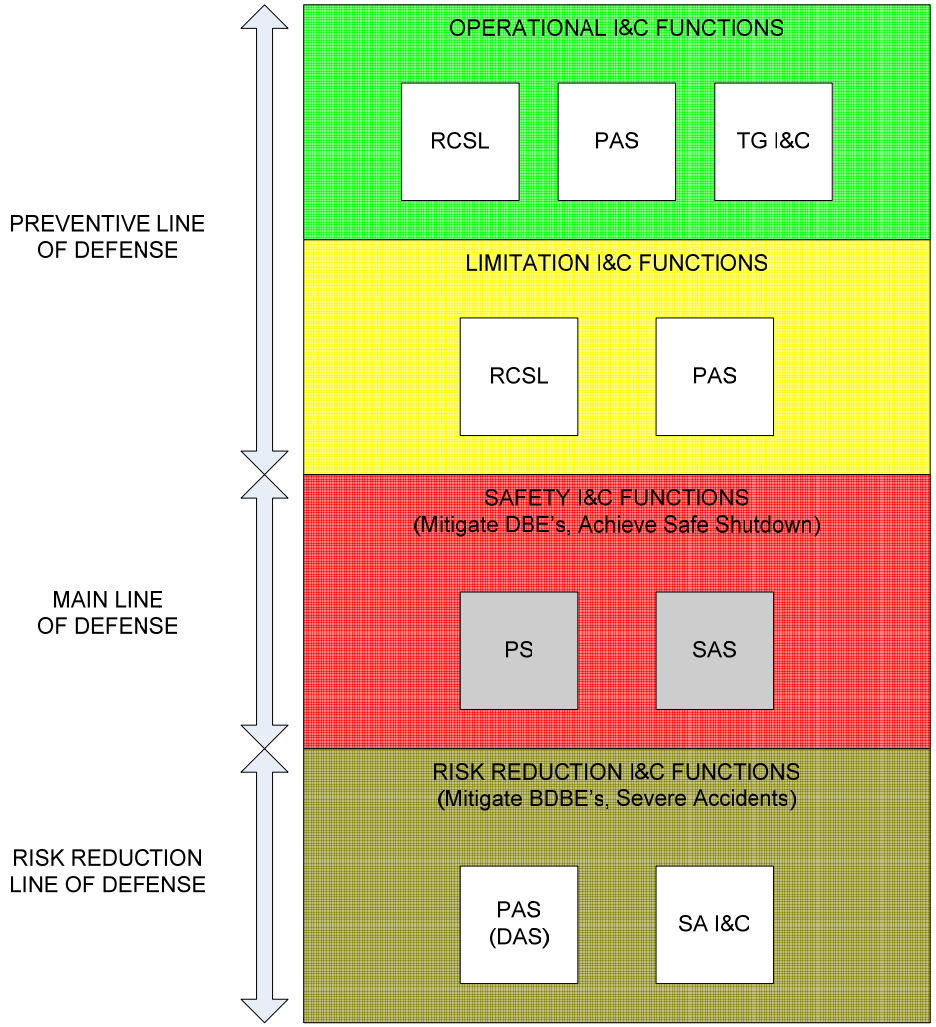


U.S. EPR I&C Defense-In-Depth: Diversity Between Lines of Defense

> **Diversity between Main Line and portion of Risk Reduction Line used to mitigate loss of the Main Line**



U.S. EPR I&C Defense-In-Depth: I&C Systems Support Defense-in-Depth

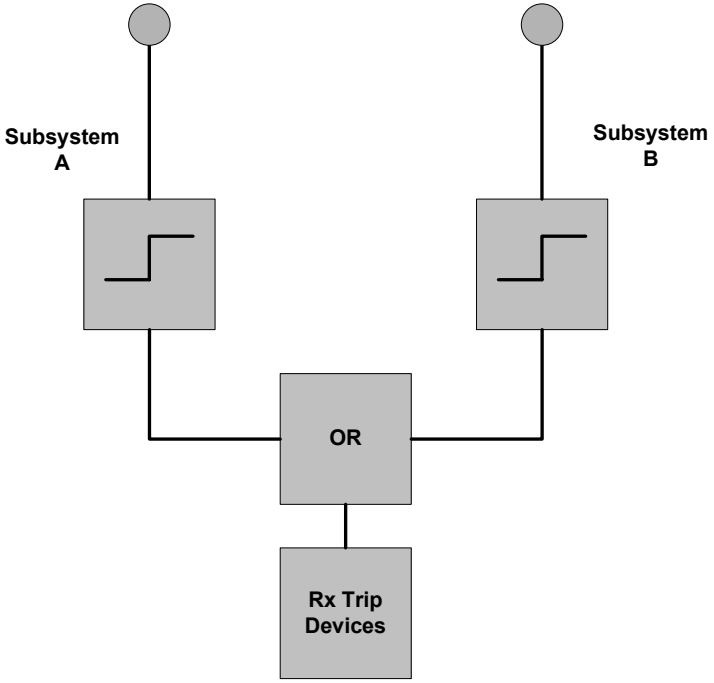


U.S. EPR I&C Diversity

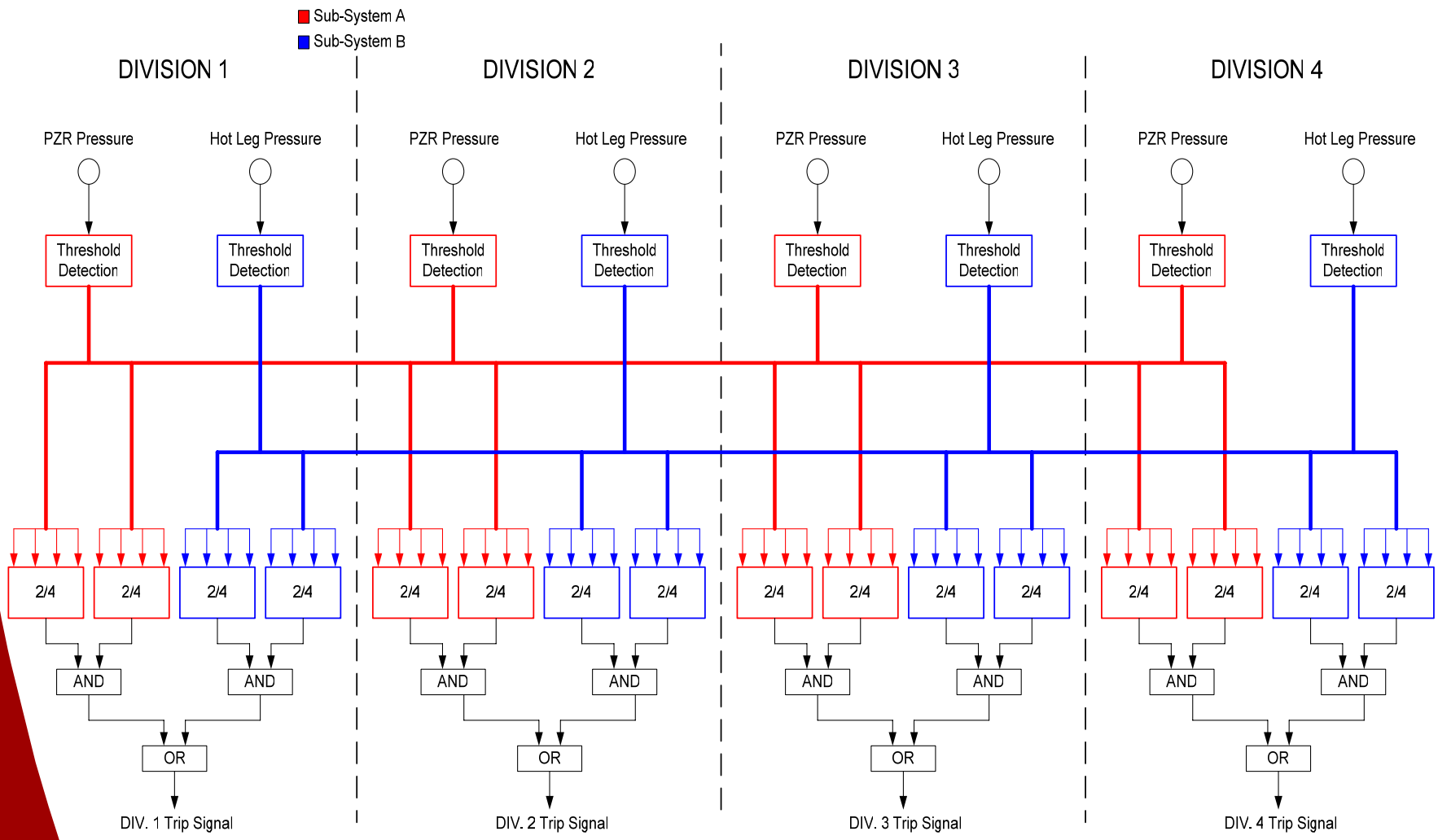
- **Functional diversity**
  - **Minimizes probability of CCF within the PS**
- **Equipment diversity**
  - **Mitigates effects of CCF of the PS**

U.S. EPR I&C Functional Diversity: Basis and Concept

- In general, digital I&C systems contain:
  - Hardware
  - Operating system
  - Application software
- AREVA experience (>20 years) shows majority of failures in application software layer
- Functional diversity is used to reduce probability of CCF due to application software functional specification errors (dominant error mode)
- Implementation of functional diversity:
  - Diverse Reactor Trip functions in each subsystem
  - ESF actuation functions allocated to each subsystem

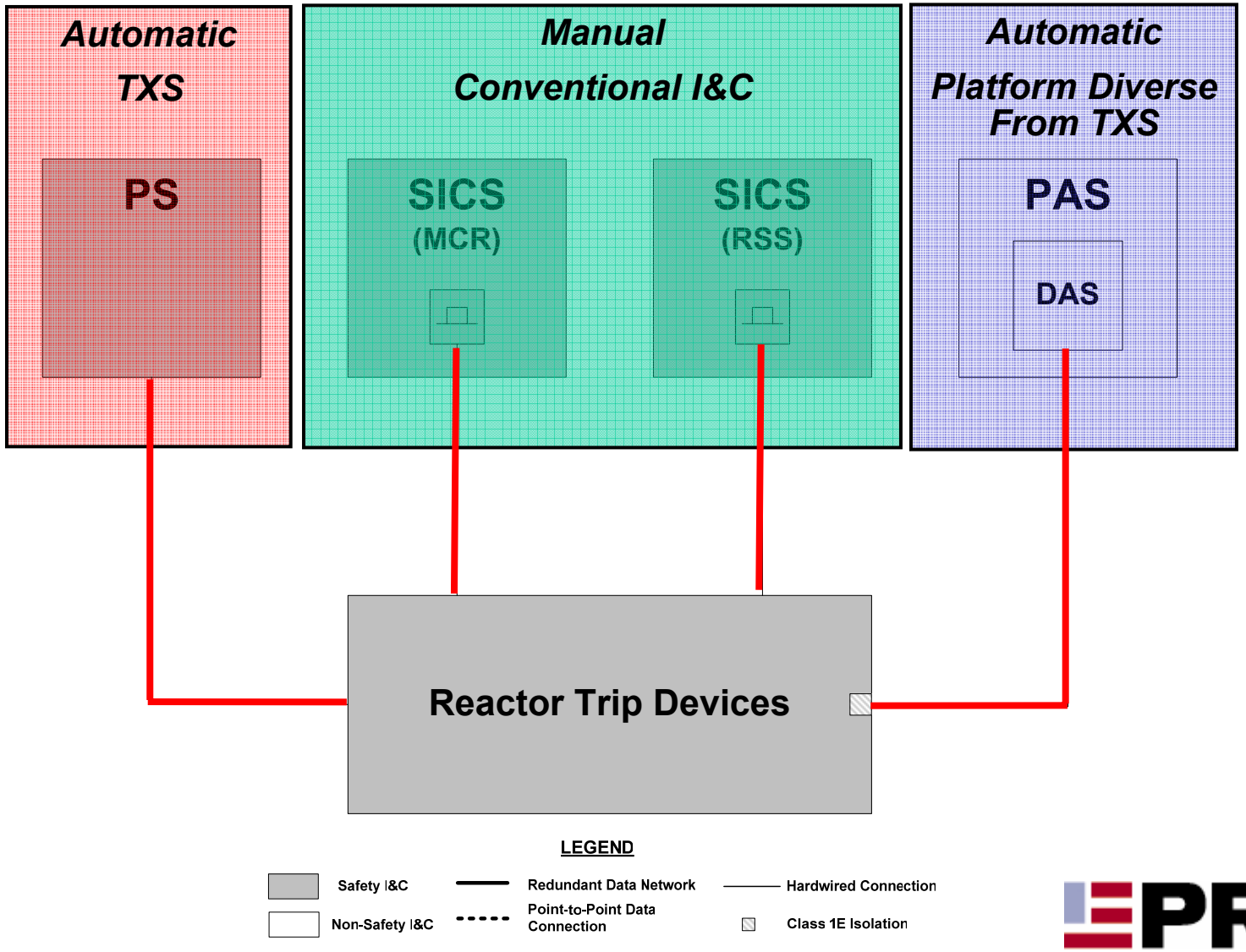


U.S. EPR I&C Functional Diversity: Example

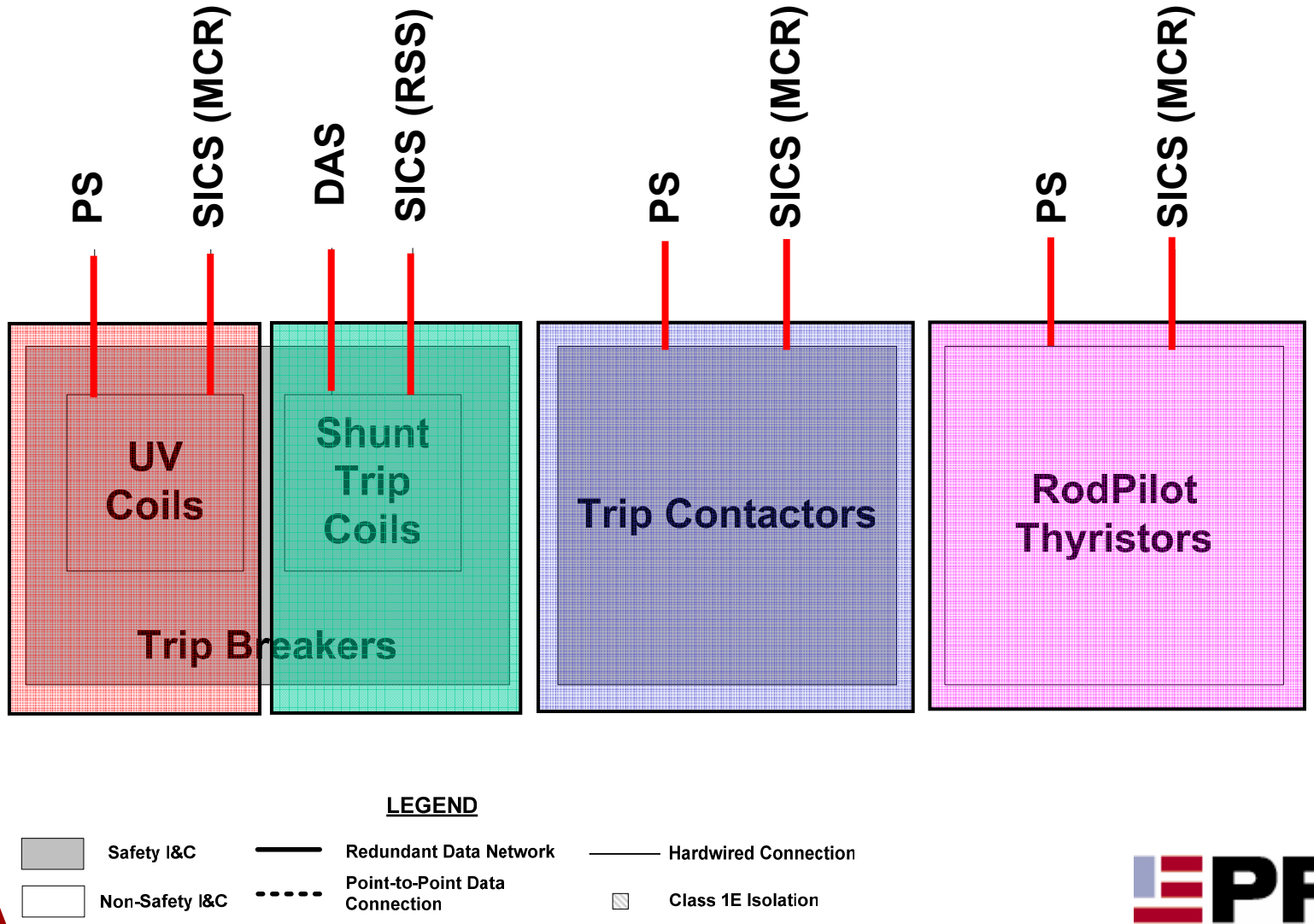


Benefits of functional diversity is demonstrated in PRA

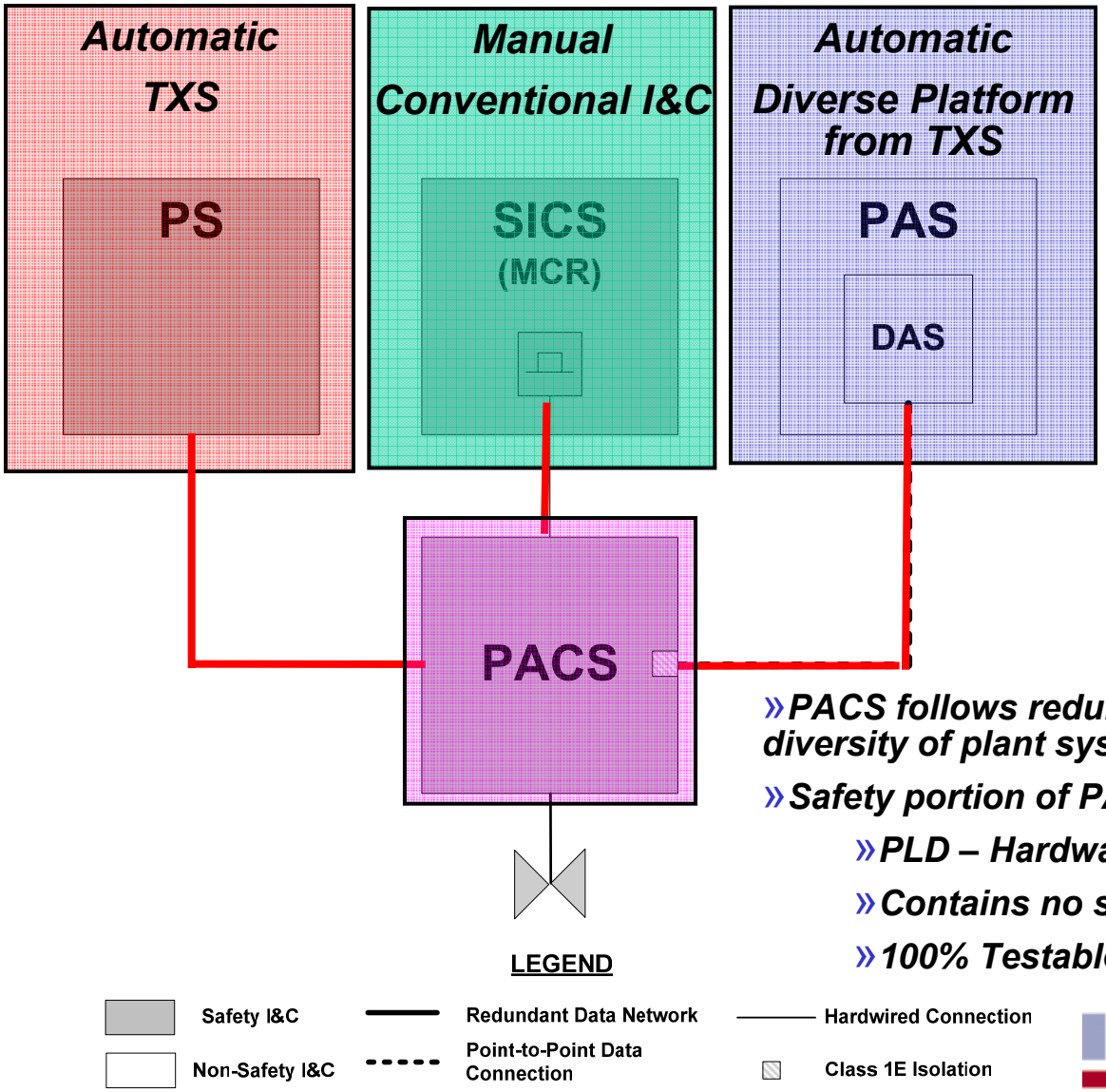
U.S. EPR I&C Equipment Diversity: Three Diverse Means of Initiating Reactor Trip



U.S. EPR I&C Equipment Diversity: Four Diverse Means of Executing Reactor Trip

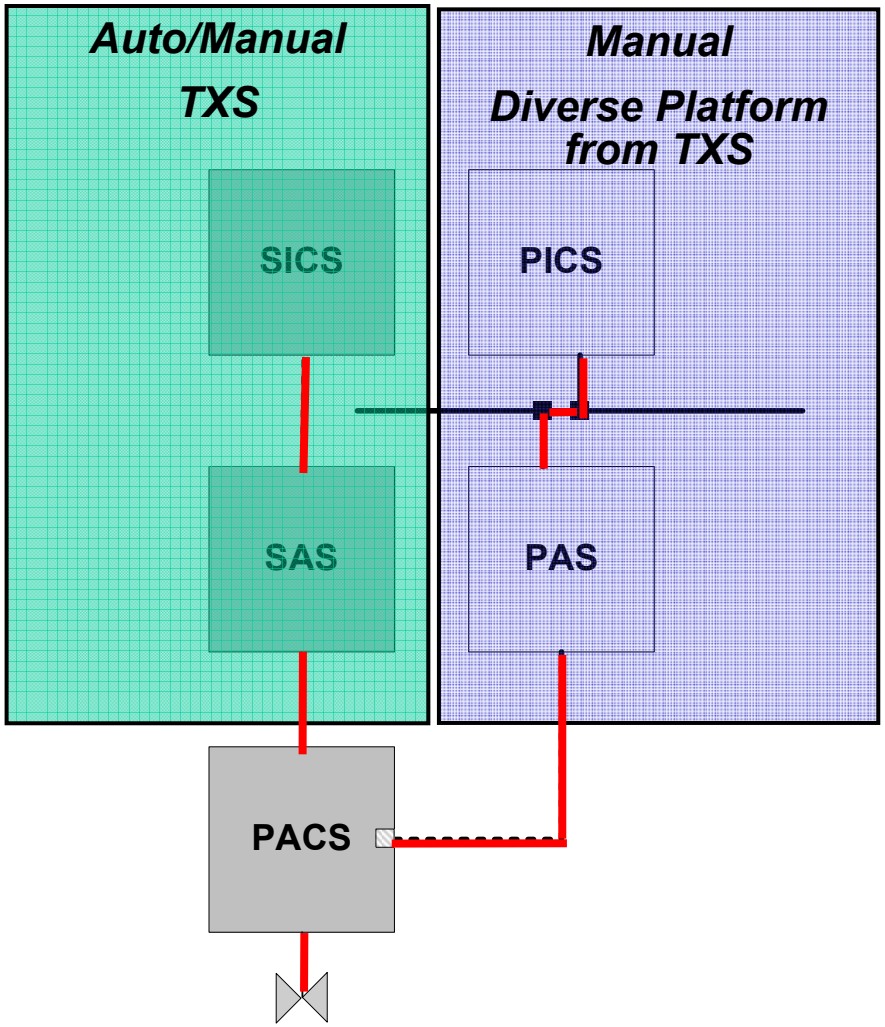


U.S. EPR I&C Equipment Diversity: Three Diverse Means of Initiating ESF Actuation



- PACS follows redundancy and diversity of plant systems
- Safety portion of PAC module
  - PLD – Hardware Device
  - Contains no software
  - 100% Testable

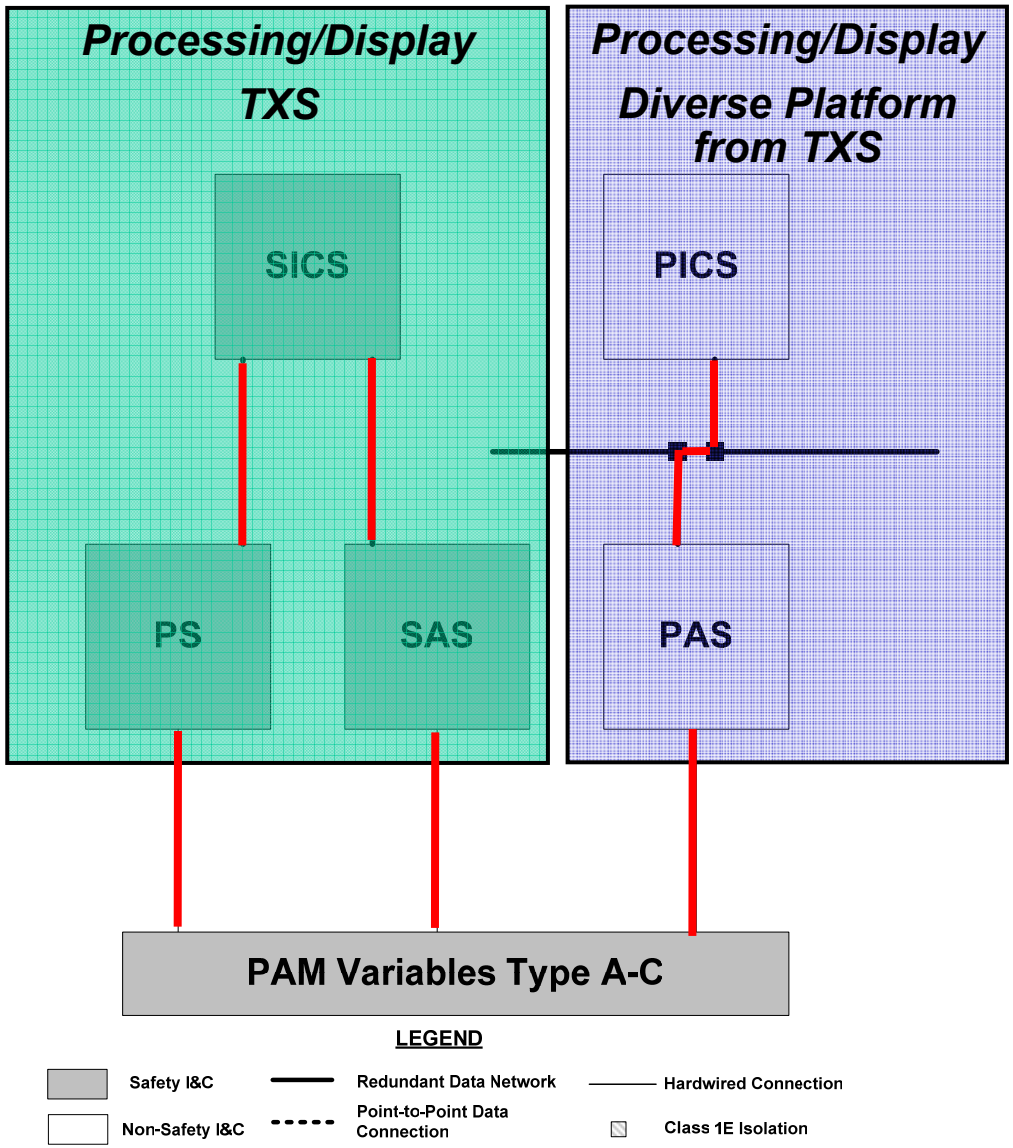
U.S. EPR I&C Equipment Diversity: Two Diverse Means of Executing Safety Controls



LEGEND

- Safety I&C
- Non-Safety I&C
- Redundant Data Network
- Point-to-Point Data Connection
- Hardwired Connection
- Class 1E Isolation

U.S. EPR I&C Equipment Diversity: Architecture Addresses RG 1.97 Rev 4



Robust I&C Platform and Software Design Processes

- **Teleperm XS Features**
  - Simple operating system
  - Static memory allocation
  - Cyclic processing
  - Asynchronous operation
  - No process driven interrupts
  - Constant bus loading
  - Watchdog monitoring
  - Function block programming
  - 10 Years/62 million processor hours of operating experience
  - Approved by SER, May 2000
- **Software Program Manual**
  - Structured lifecycle processes
  - Topical report currently in review

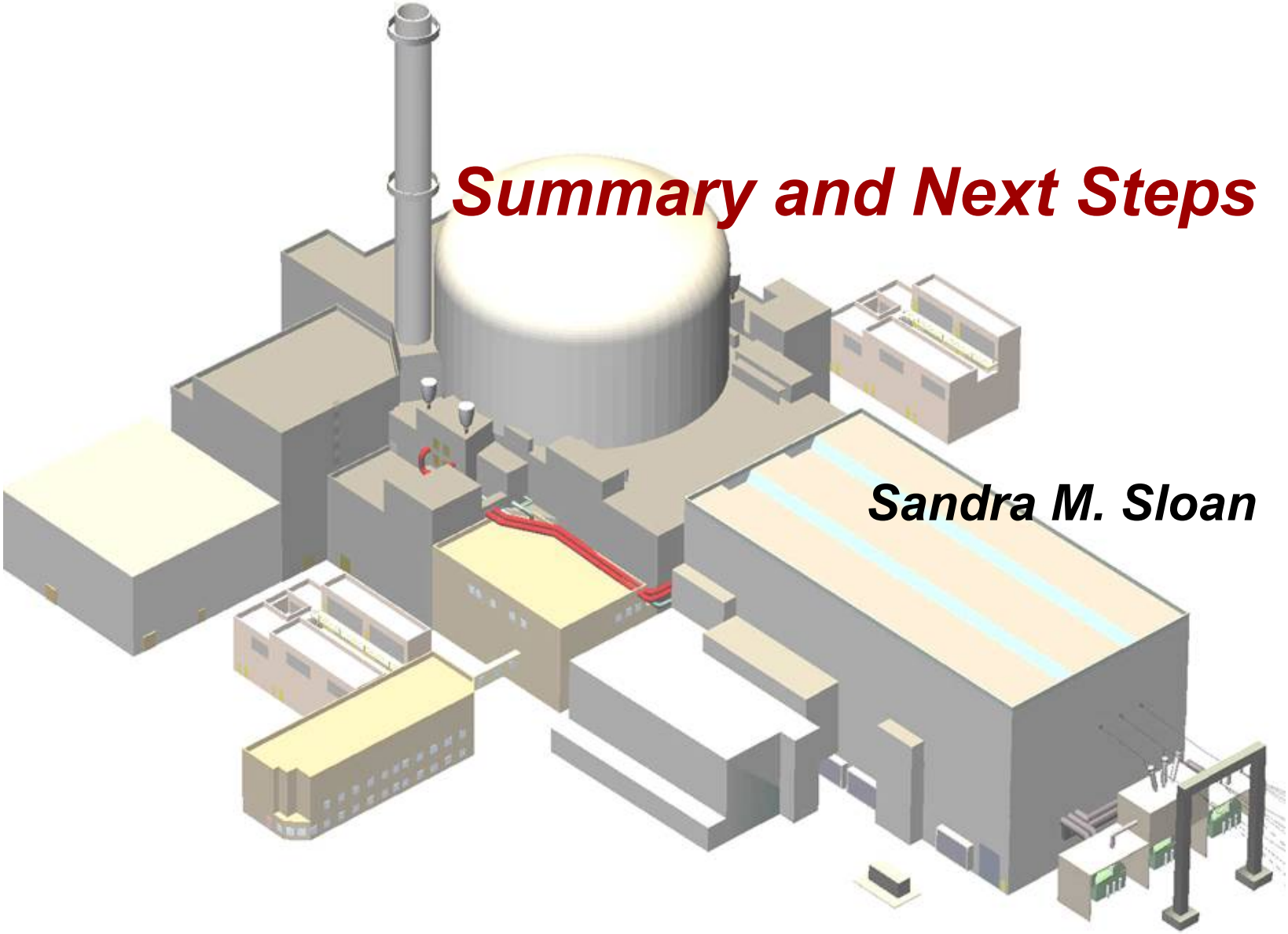
Safety system quality minimizes probability of CCF

U.S. EPR Diversity and Defense-In-Depth Methodology

U.S. EPR Diversity and Defense-In-Depth Methodology: Approach Addresses BTP-7-19

1. **Determine susceptibility of PS to CCF**
2. **Evaluate plant response assuming the CCF(s) identified in step 1 using best-estimate methods for Chapter 15 events**
   - **Credit systems (safety and non-safety) not affected by CCF**
   - **Use acceptance criteria per BTP-7-19 for AOO's and DBA's**
3. **If acceptance criteria not met:**
   1. **Determine required functionality to be added**
   2. **Perform functional allocation using the automation criteria in the U.S. EPR HFE program**
      - **MANUAL ON SICS, or**
      - **AUTOMATIC IN DAS**
4. **Assess that manual controls and indications for critical safety functions in MCR are diverse from systems affected by CCF**

Summary and Next Steps



Sandra M. Sloan

Summary

- The U.S. EPR I&C Architecture has been designed with a high degree of diversity and defense-in-depth
- The I&C Diversity and Defense-in-Depth Methodology conforms with regulatory guidance
- This type of interaction helps us understand NRC expectations and thus produce a high-quality DC submittal

Next Steps

- AREVA NP will submit the I&C Diversity and Defense-in-Depth Methodology Topical Report in June 2007
- Next meetings:
  - Meeting on PRA Methods Report, May 9th
  - Meeting on Environmental Qualification Program Report, May 16th
  - Support further discussions with NRC to facilitate review of the Diversity and Defense-in-Depth Topical Report

Abbreviations and Acronyms

>	AOO:	Anticipated Operational Occurrence
>	ATWS:	Anticipated Transient Without Scram
>	BDBE:	Beyond Design Basis Event
>	CCF:	Common Cause Failure
>	DAS:	Diverse Actuation System
>	D3:	Diversity and Defense-in-Depth
>	DBA:	Design Basis Accident
>	DBE:	Design Basis Event
>	ESF:	Engineered Safeguard Features
>	HFE:	Human Factors Engineering
>	MCR:	Main Control Room
>	PACS:	Priority Actuation & Control System
>	PAM:	Post-Accident Monitoring
>	PAS:	Process Automation System
>	PLD:	Programmable Logic Device
>	PICS:	Process Information & Control System
>	PS:	Protection System
>	RCSL:	Reactor Control, Surveillance, & Limitation System
>	RSS:	Remote Shutdown Station
>	RT:	Reactor Trip
>	SA I&C:	Severe Accident I&C
>	SAS:	Safety Automation System
>	SICS:	Safety Information & Control System
>	TG I&C:	Turbine Generator I&C
>	TSC:	Technical Support Center
>	TXS:	Teleperm XS