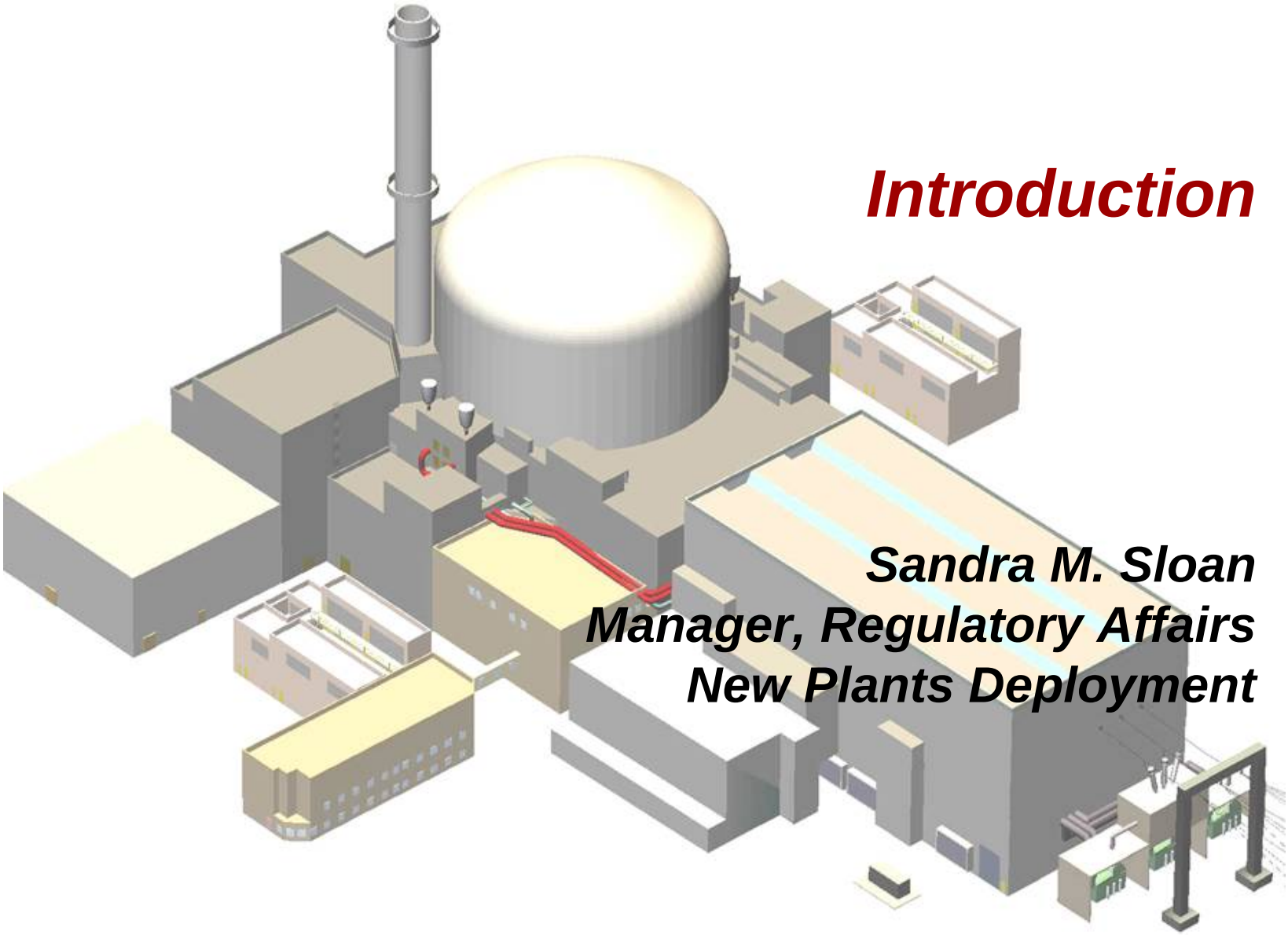
# U.S. EPR Pre-Application Review Meeting: U.S. EPR Digital Protection System Topical Report

AREVA NP Inc. and the NRC
March 1, 2007

# Introduction




***Sandra M. Sloan***
***Manager, Regulatory Affairs***
***New Plants Deployment***

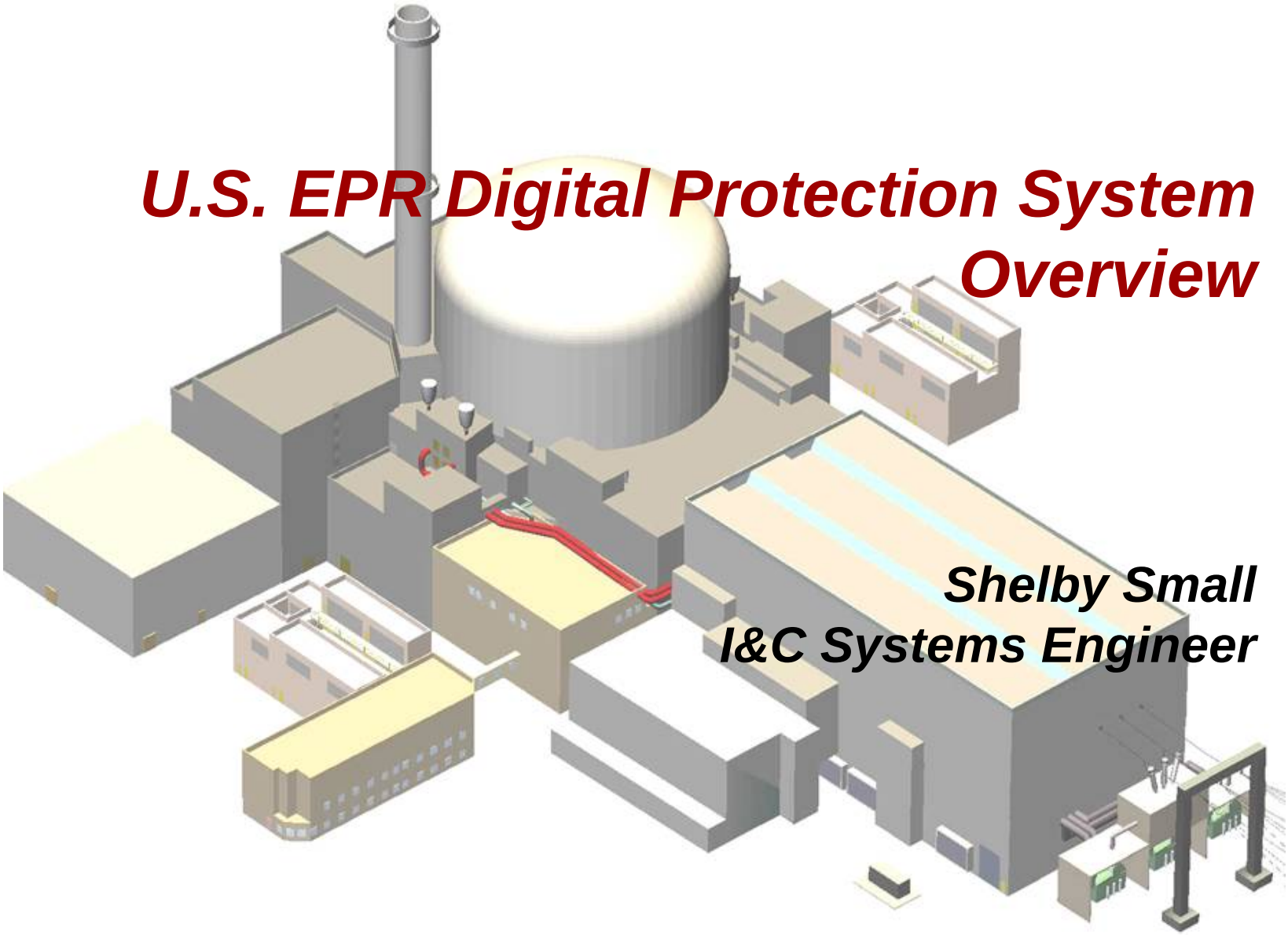
# Agenda

- Introduction and Meeting Objectives (S. Sloan)
- Digital Protection System Overview (S. Small)
- Digital Protection System Topical Report (S. Small)
  - Contents
  - Application of TELEPERM XS (TXS) to the Digital Protection System design and selected technical topics
- Summary and Next Steps (S. Sloan)

# Meeting Objectives

- Provide an overview of the U.S EPR Digital Protection System Topical Report
- Follow-up from the August 31, 2006 meeting on I&C Digital Instrumentation and Control System Topics
- Provide information on application of generic TXS technology to the U.S. EPR design
- Provide an opportunity for early NRC feedback on the U.S. EPR Digital Protection System Topical Report

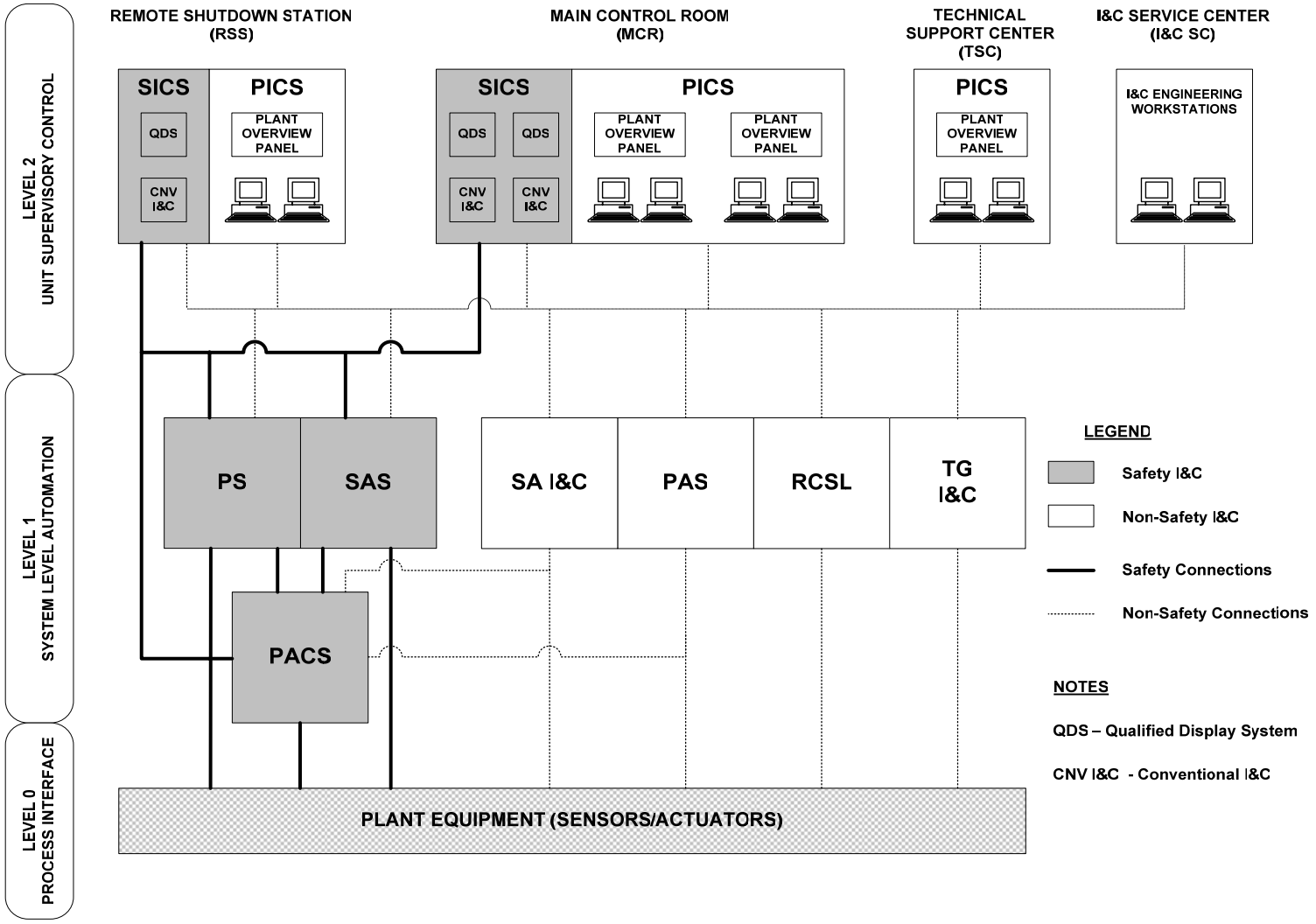
# U.S. EPR Digital Protection System Overview




***Shelby Small***
***I&C Systems Engineer***

# Digital Protection System Overview

## Overall I&C Architecture



# Digital Protection System Overview

## Background

- **U.S. EPR Digital Protection System is an integrated Reactor Protection and Engineered Safeguard Features Actuation System (ESFAS)**
  - **Reactor Trip (RT)**
  - **ESFAS**
  - **Permissive signals**
- **Implemented in the TELEPERM XS platform**
- **TXS platform is described in topical report EMF-2110, Revision 1, TELEPERM XS: A Digital Reactor Protection System, September 1, 1999**
- **NRC issued a safety evaluation report (SER) for the topical report via letter dated May 5, 2000 (TAC No. MA1983, ML003732662)**

# Digital Protection System Overview

## TXS Safety Principles

- **TXS computer processors use a deterministic operating system**
  - **Increases the predictability of the software**
- **The most important features of the TXS software design include a strictly cyclic processing of application software**
  - **Asynchronous operating system (meaning no real-time clock that redundant processors synchronize to) reduces failure potential and enhances reliability**
- **Only static memory allocation**
  - **Each variable in the application program has a permanent dedicated place in memory, so that memory conflicts caused by dynamic memory allocation are not possible**
- **No process-driven interrupts**
- **Other important features include:**
  - **Bus systems with a constant load**
  - **No long-term data storage**
  - **No self-contained external data storage media**

# Digital Protection System Overview

## Design Features

- **Functionality**
  - Performs RT, Engineered Safety Features (ESF) functions, safety permissives
  - Each division independently generates a trip decision per parameter
  - Each division votes 2/4 on trip decisions from all four divisions
- **Redundancy**
  - Four redundant divisions
  - Redundant voting within each sub-system
- **Functional diversity for RTs**
  - Two functionally diverse sub-systems per division
- **Independence**
  - Between redundant divisions
  - Between functionally diverse sub-systems
- **Reliability and availability**
  - Protection against spurious reactor trips
  - Protection against unavailability of ESF functions

***Redundant, Diverse, and Reliable***

# Digital Protection System Overview

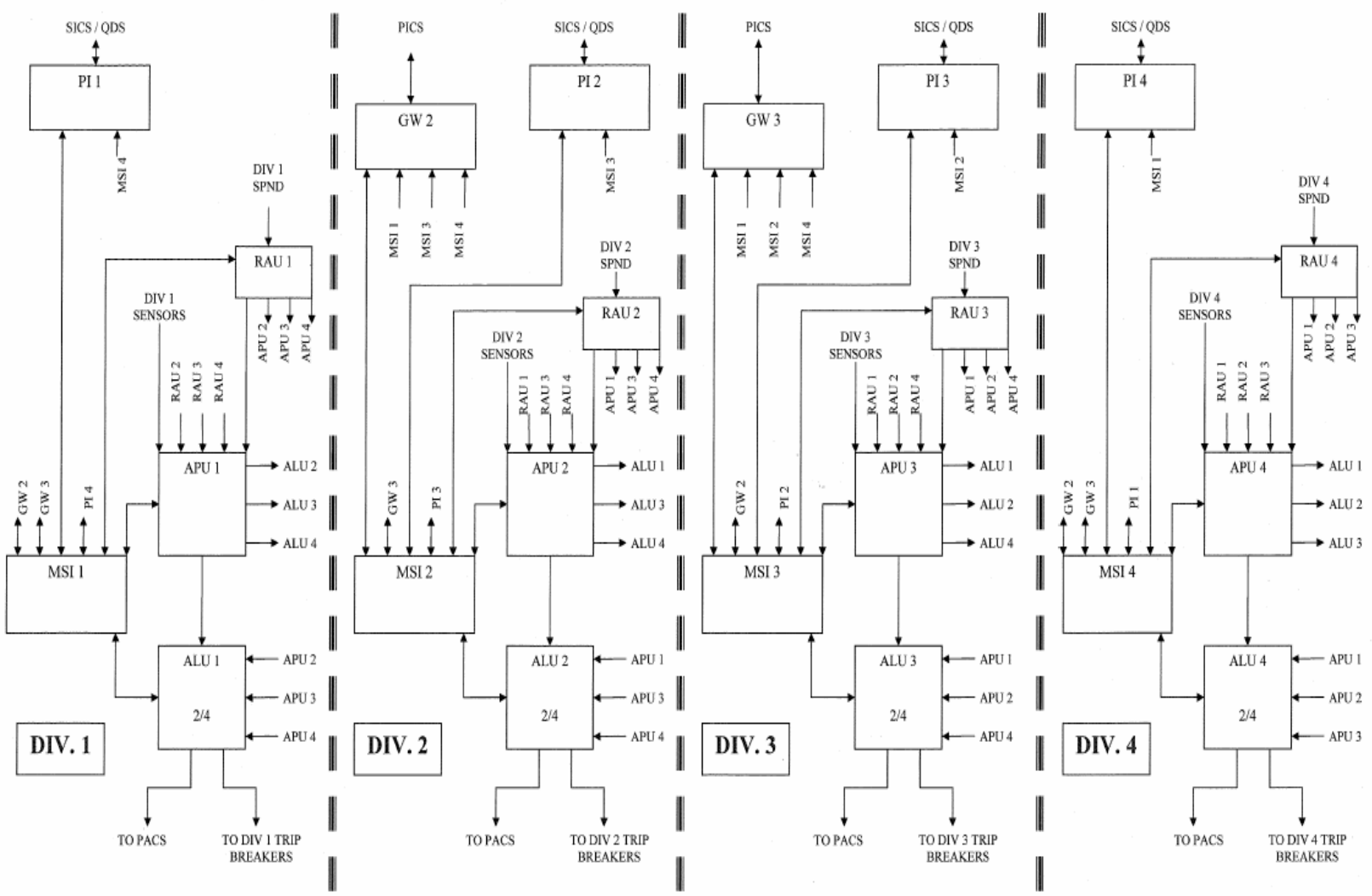
## Functional Diversity

- **For each event requiring reactor trip, if the primary initiation signal is processed in sub-system A (or B), a diverse initiating signal, if necessary, is provided in sub-system B (or A)**
  - **A sensor used for a primary initiation signal in one sub-system cannot be used by the secondary initiation signal in the other sub-system**
  - **Sub-system A must comprise separate function computers from sub-system B**
  - **The function computers of different sub-systems are not be located in the same cabinets**
  - **Communications between function computers within a division must be limited to units of the same sub-system**
  - **Communications between divisions must be limited to units of the same sub-system**

***The goal is functional independence between sub-systems***

# Digital Protection System Overview

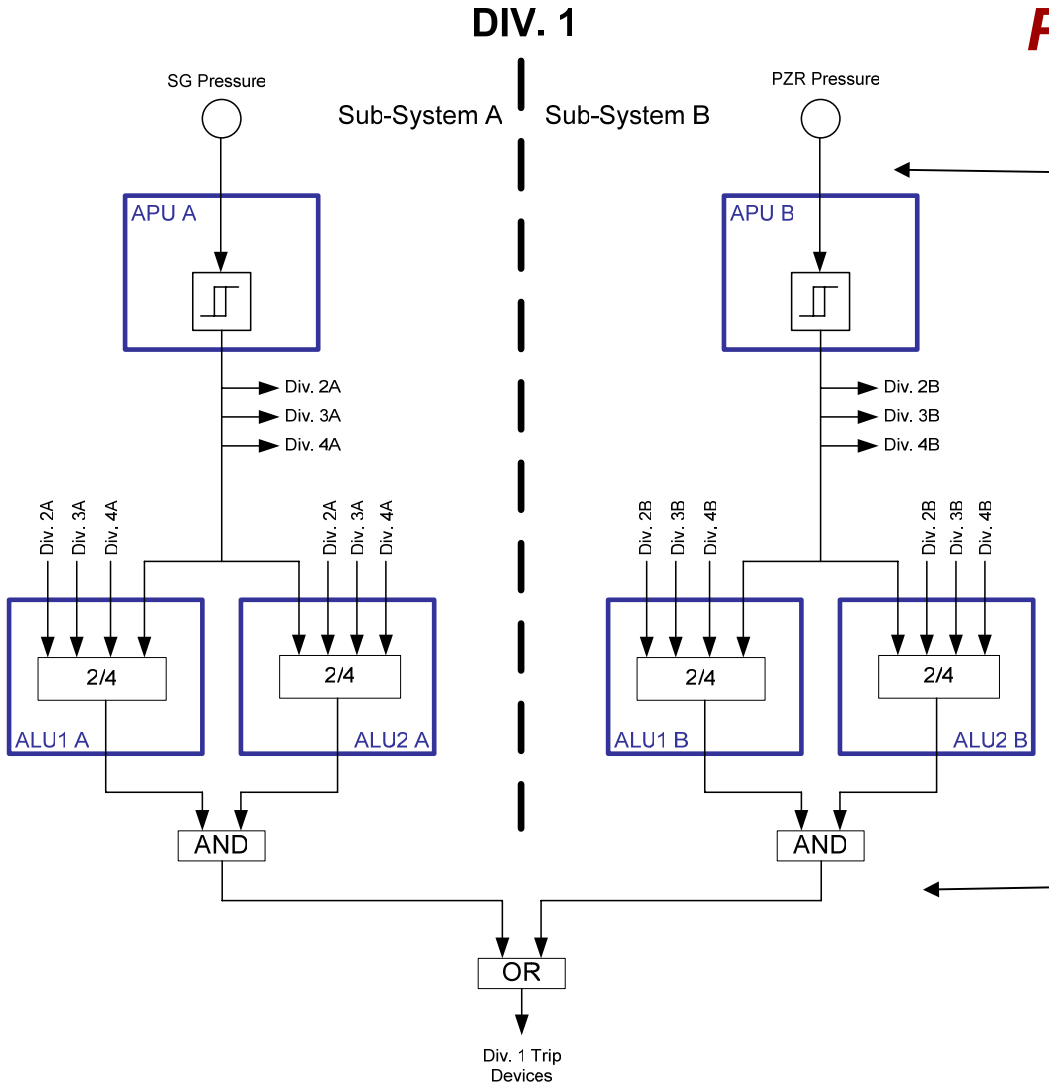
## Block Diagram




**4 Divisions – Increased Safety and Reliability**

# Digital Protection System Overview

## Reactor Trip Logic




***Functional Diversity***

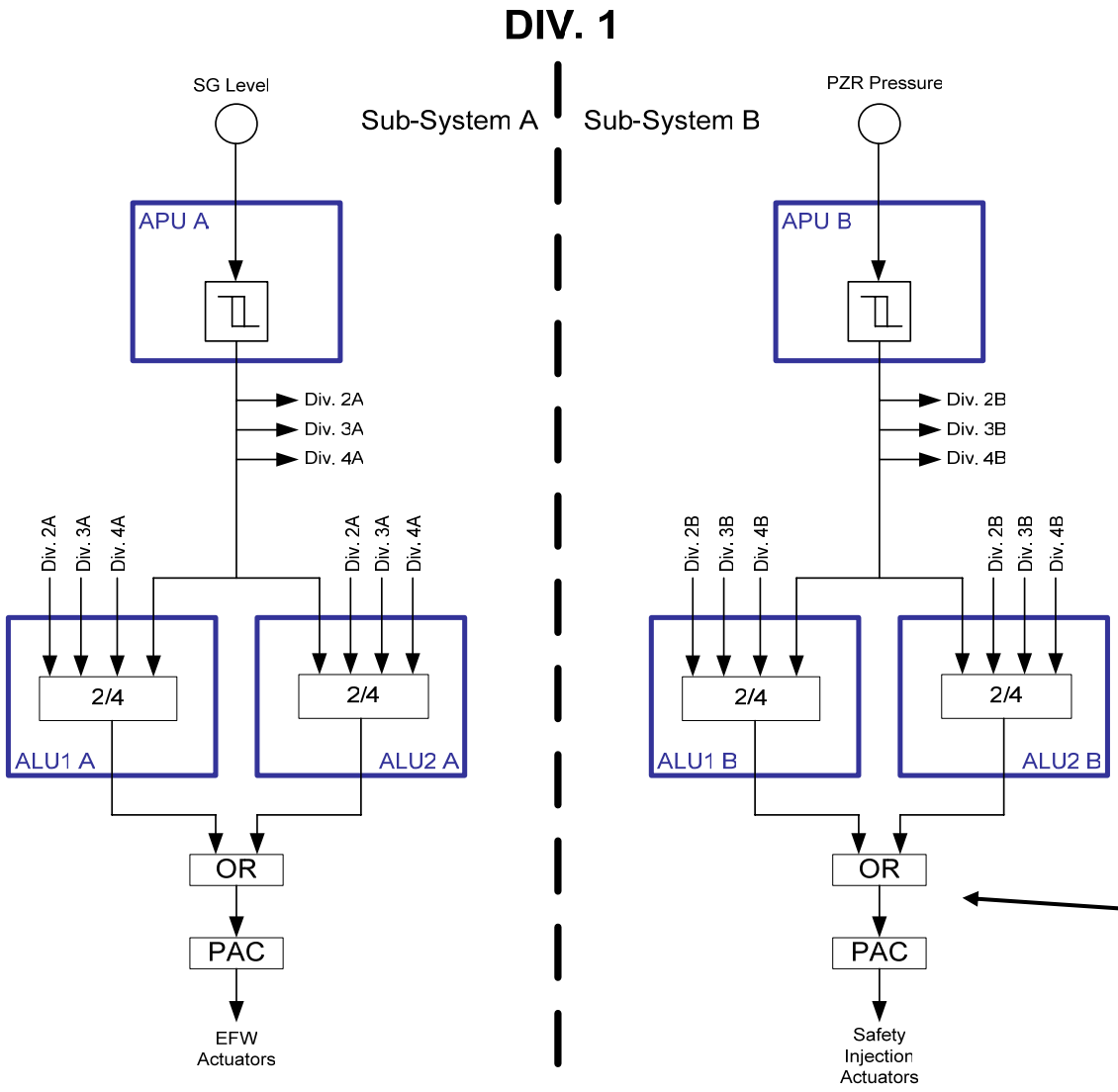
***Redundant Voting per Sub-System***

***Protection Against Spurious Trip***

***Safe & Reliable - 2 Sub-Systems and Redundant Voting***

# Digital Protection System Overview

## ESF Logic




***Redundant Voting Per Sub-System***

***Protection Against ESF Unavailability***

***Safe & Reliable - 2 Sub-Systems and Redundant Voting***

# U.S. EPR Digital Protection System
## Topical Report Contents

# Topical Report Contents

1. **Introduction**
   - Background
   - Purpose and scope
2. **System Definition**
   - Role of the system
   - System organization
   - System implementation
3. **Overall System Architecture**
   - Architecture diagram explanation
   - System architecture features
4. **Units of the Digital Protection System**
   - Description of each unit type Remote Acquisition Unit (RAU), Acquisition & Processing Unit (APU), Actuation Logic Unit (ALU), etc.
   - Includes Panel Interface (PI), Qualified Display System (QDS) and Priority Actuation & Control System (PACS) modules

# Topical Report Contents (cont'd)

5. **Detailed System Architecture**
   - Presented as a series of network diagrams
   - General concepts related to network topologies
6. **Reactor Trip Functionality**
   - Typical automatic RT sequence
   - SPND-based automatic RT sequence
   - Reactor trip voting logic and outputs
   - Manual RT
   - RT actuators
7. **Engineered Safety Features Actuation Functionality**
   - Typical automatic ESF actuation sequence
   - ESF actuation voting logic
   - ESF actuation outputs
   - Divisional assignments - ESF actuation outputs
   - Manual ESF actuations

# Topical Report Contents (cont'd)

8. **Permissive Signals**
   - Definition of permissive
   - Design rules
9. **Functional Diversity**
   - Definition of functional diversity
   - Design rules
10. **Use of PAC in ESFAS**
    - General operation of PAC module
    - General description of PAC concept in the U.S. EPR
11. **Inter-Channel Communication**
    - Communication interfaces
    - Communication independence
12. **Safety to Non-Safety Interfaces**
    - General requirements for interfaces
    - Service Unit Interface
    - PICS Interface
    - Control System Interface

# Topical Report Contents (cont'd)

13. Compliance with IEEE 603-1991
    - IEEE 603-1998 is used as framework to demonstrate compliance
        - Adds specific references to IEEE 7-4.3.2 in the relevant clauses
        - Updates references to other IEEE standards that have been endorsed by NRC Regulatory Guides
        - Applies to "computer-based safety systems and to advanced nuclear power generating station designs"
    - Clause 4 will be addressed in DCD
    - Clauses 5-8 addressed in this topical report
14. TXS Operating Experience
    - Observed vs. calculated failure rates
    - Examples of TXS protection systems currently in operation
15. Summary and Conclusions
16. References

# Related Reports

| Report No. | Title | Date |
|---|---|---|
| EMF-2110, Revision 1 | TELEPERM XS: A Digital Reactor Protection System | May 2000 (ML003732662) |
| ANP-10272 | Software Program Manual for TELEPERM XS Safety Systems Topical Report | December 2006 (ML063610100) |
| ANP-10273P<br>ANP-10273NP | AV42 Priority Actuation and Control Module Topical Report | November 2006 (ML063380081, ML063380086) |
| ANP-10274NP | U.S. EPR Probabilistic Risk Assessment Methods Report | December 2006 (ML063540121) |
| ANP-10279 | U.S. EPR Human Factors Engineering Program Topical Report | January 2007 (ML070370197) |
| TBD | U.S. EPR Instrument Setpoint Methodology Topical Report | March 2007* |
| TBD | U.S. EPR Diversity and Defense-In-Depth Analysis Methodology | June 2007* |

**** scheduled submittal date***

# Topical Report Contents
## Background

- **The NRC SER approved:**
  - **TXS as a qualified generic digital I&C platform acceptable for safety related applications**
  - **The TXS system design principles:**
    - **Use of four system building blocks described in SER**
    - **Equipment qualification methods**
    - **Software development including V&V methods**
    - **Processing principles**
    - **Inter-channel communication principles**
    - **Maintenance interface**
- **The existing SER requires each applicant to demonstrate:**
  - **The "as-built" system adheres to approved TXS design principles**
  - **Generic qualification bounds plant license requirements**
  - **Plant-specific interface items are sufficiently addressed**

# Topical Report Contents
## Purpose and Scope

- **AREVA NP seeks an SER approving U.S. EPR-specific implementation of:**
  - **Protection System architecture**
  - **Specific network configurations**
  - **Typical RT concepts and sequences**
  - **Typical ESFAS concepts and sequences**
  - **Design rules for permissive signals**
  - **Inter-channel communication independence**
  - **Safety to non-safety system interfaces**
  - **Compliance with relevant clauses of IEEE-603**
- **Not seeking approval of a specific set of TXS hardware components or version of software for use in the U.S. EPR**

# *Application of TELEPERM XS to the U.S. EPR Digital Protection System Design: Selected Technical Topics*

# Topical Report
## Selected Technical Topics

- **Follow-up to NRC feedback from August 31, 2006 meeting**
  - **Manual RT actuation**
  - **Manual ESF actuation**
- **Application of TELEPERM XS to U.S. EPR Digital Protection System architecture**
  - **Inter-divisional communication**
  - **Safety to non-safety interfaces**

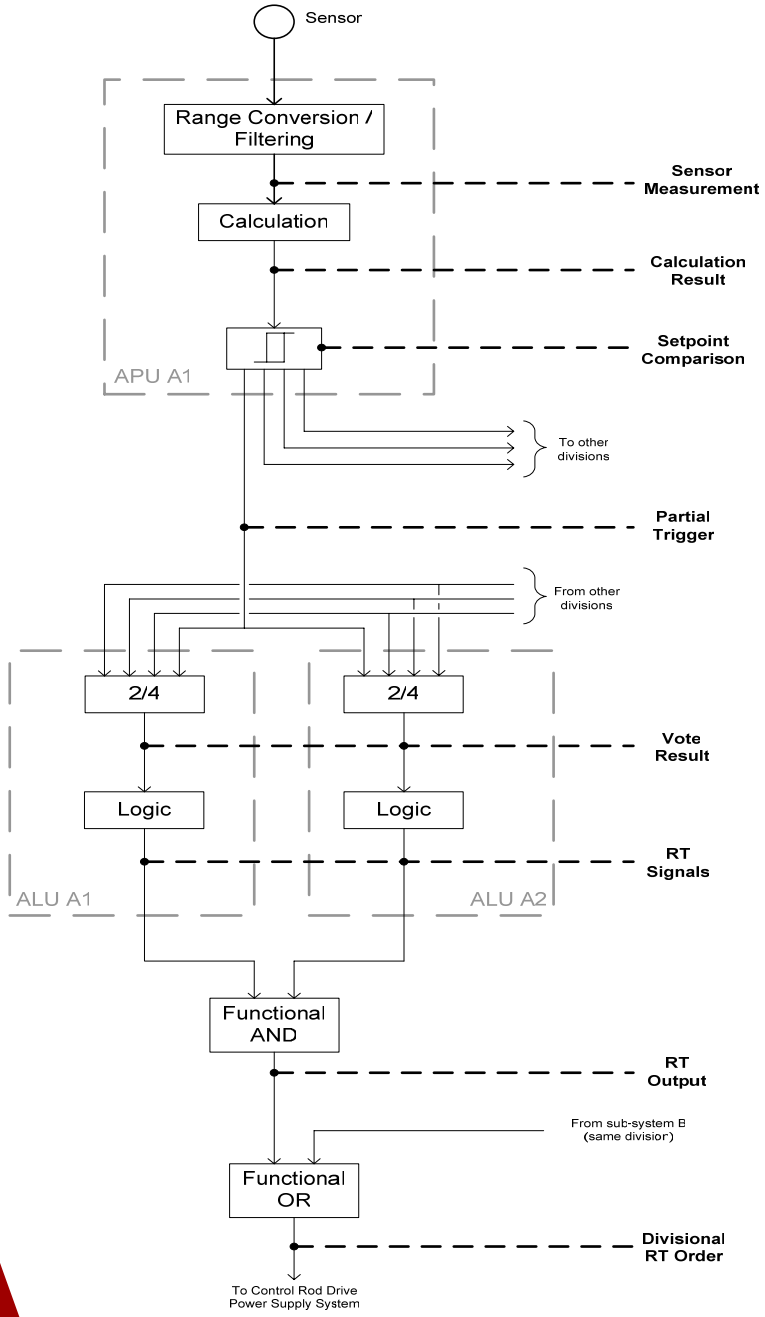
# Topical Report
## Manual Reactor Trip

- **Main Control Room (MCR)**
  - **Four dedicated buttons (one per PS division)**
  - **Hardwired around PS electronics**
  - **Also hardwired to ALU level, combined with auto trip logic**
  - **Acts on the under-voltage coils of trip breakers, trip contactors, transistors of operating coils**

- **Remote Shutdown Station (RSS)**
  - **Four dedicated buttons**
  - **Hardwired around PS electronics**

**Acts on the shunt trip coils of trip breakers**

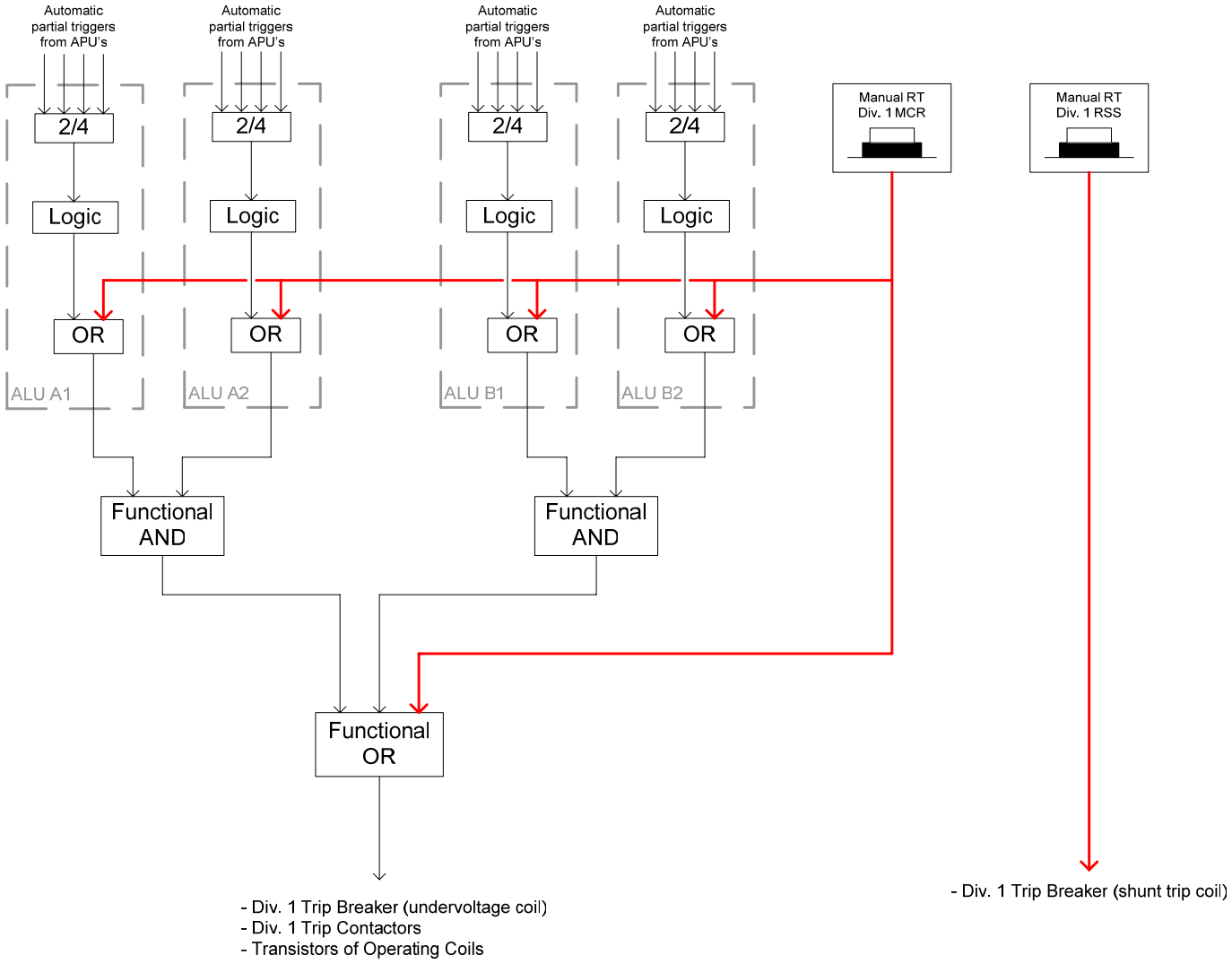
# Topical Report
## Manual Reactor Trip




## Typical Automatic RT Sequence

## (orientation for next slide)

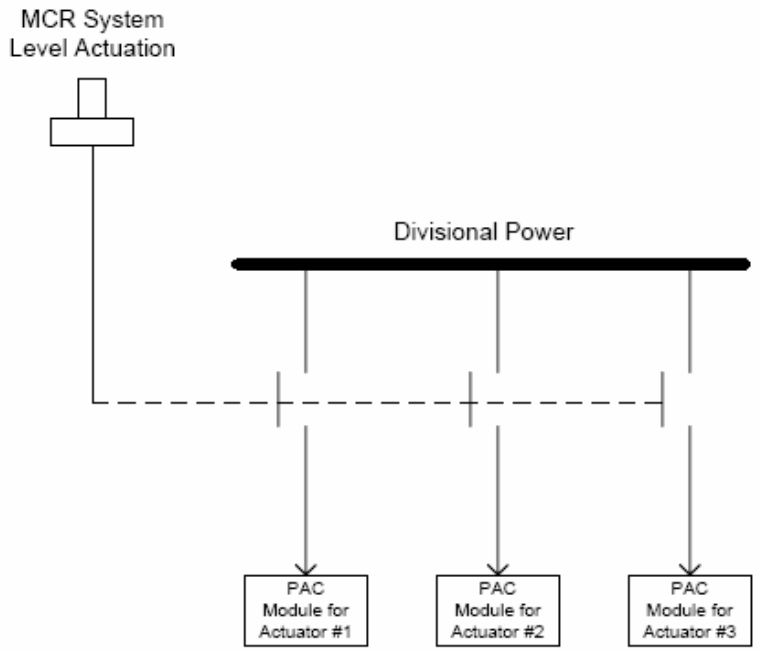
# Topical Report
## Manual Reactor Trip



# Topical Report
## Manual ESF Actuations

- **System level initiation (division by division)**
  - **Implemented completely through 1E paths**
  - **Performs all actions performed by the related automatic functions**
  - **System level actuation has priority over individual component control**
- **Implementation in the design**
  - **Three typical implementations**
  - **Determined on a case by case basis**
    - **Number and types of actuators involved**
    - **Level of sequencing required**
    - **Defense-in-depth and diversity analysis considerations**

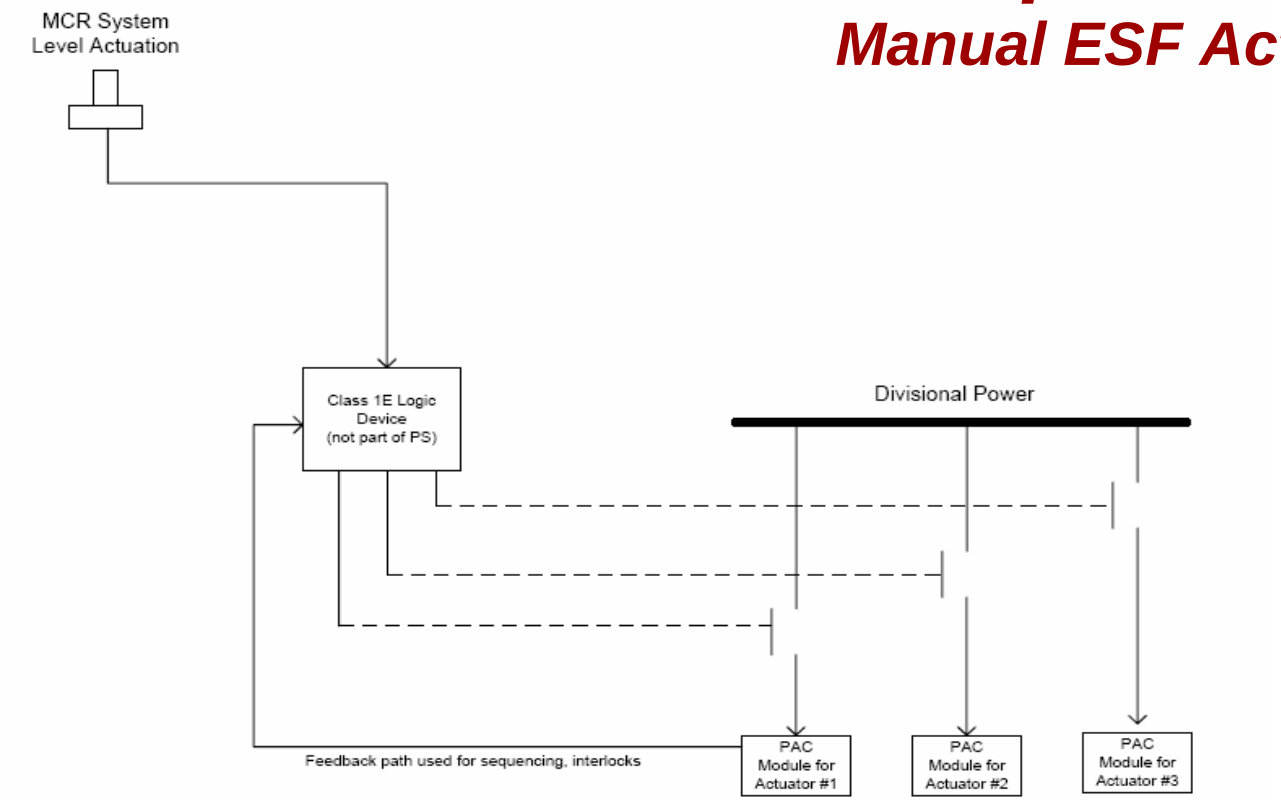
# Topical Report
## Manual ESF Actuations




**Typical #1**

- **1E actuation path, diverse from the PS**
- **Only used when no sequencing is required**
- **Can be credited in defense-in-depth and diversity analysis**

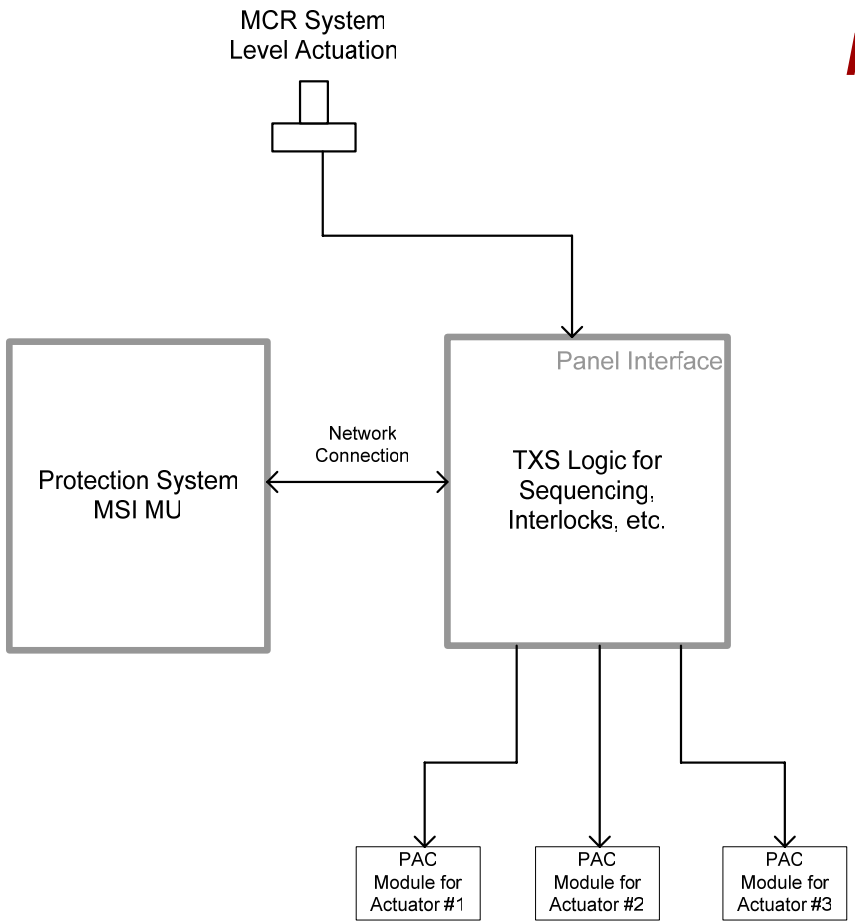
# Topical Report
## Manual ESF Actuations




## Typical #2

- 1E actuation path, diverse from the PS
- Used when sequencing required
- Can be credited in defense-in-depth and diversity analysis

# Topical Report
## Manual ESF Actuations




## Typical #3

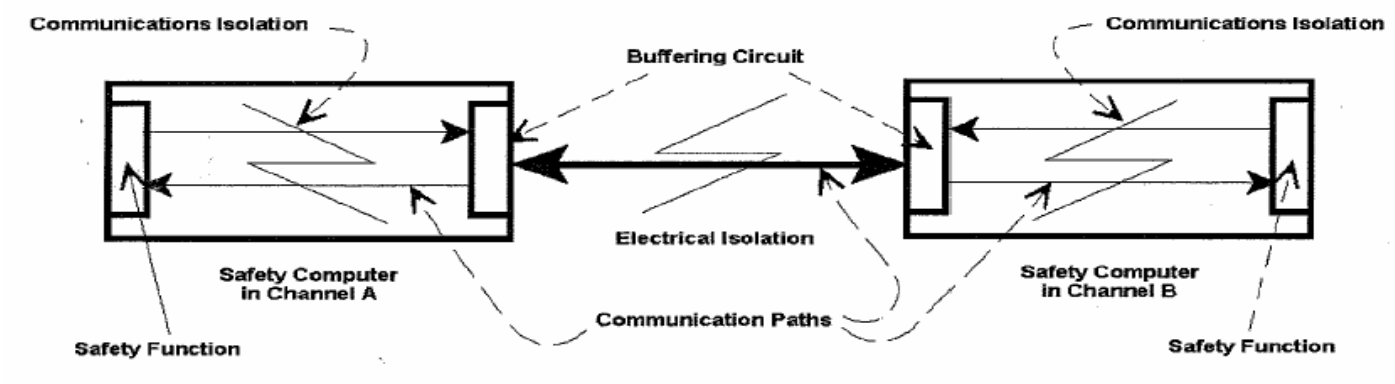
- 1E actuation path, utilizes panel interface
- Used when sequencing or timing required
- Evaluating how this approach will be credited in the defense-in-depth and diversity analysis

# Topical Report
## Inter-Divisional Communication

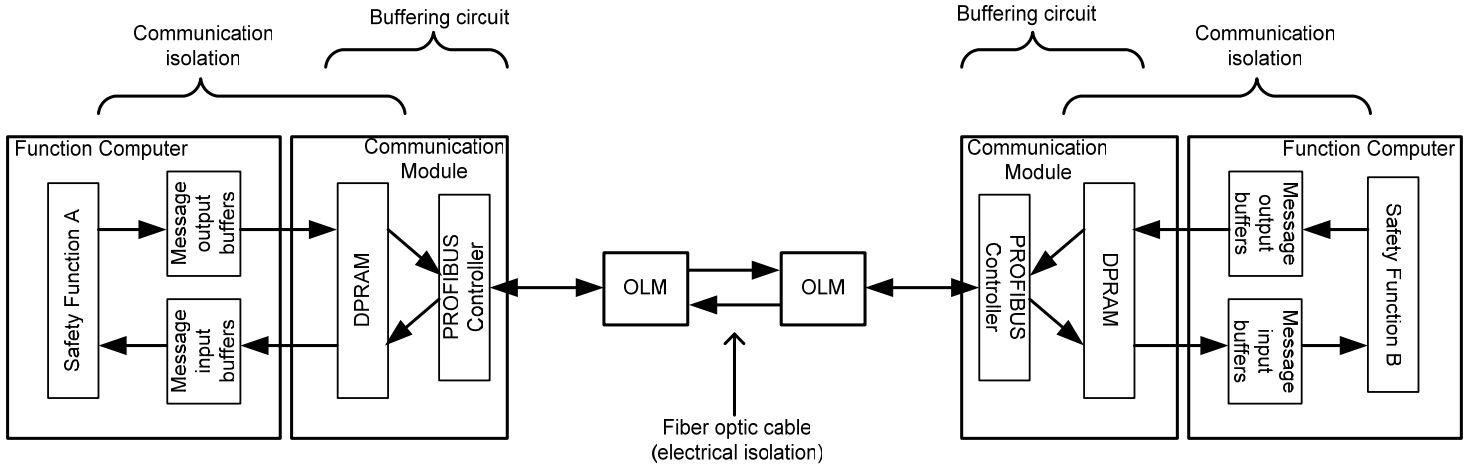
- **Two basic network configurations**
  - **Two station token ring (redundant point to point topology)**
  - **More than two station token ring (redundant ring topology)**
  - **Independence achieved in the same manner regardless of network topology**
- **Electrical isolation**
  - **Fiber optic communication paths**
- **Communications isolation**
  - **Buffering circuits**
  - **Separation of data flow**
  - **Network communication performed independently of function computer processing**

# Topical Report
## Inter-Divisional Communication

### IEEE 7-4.3.2

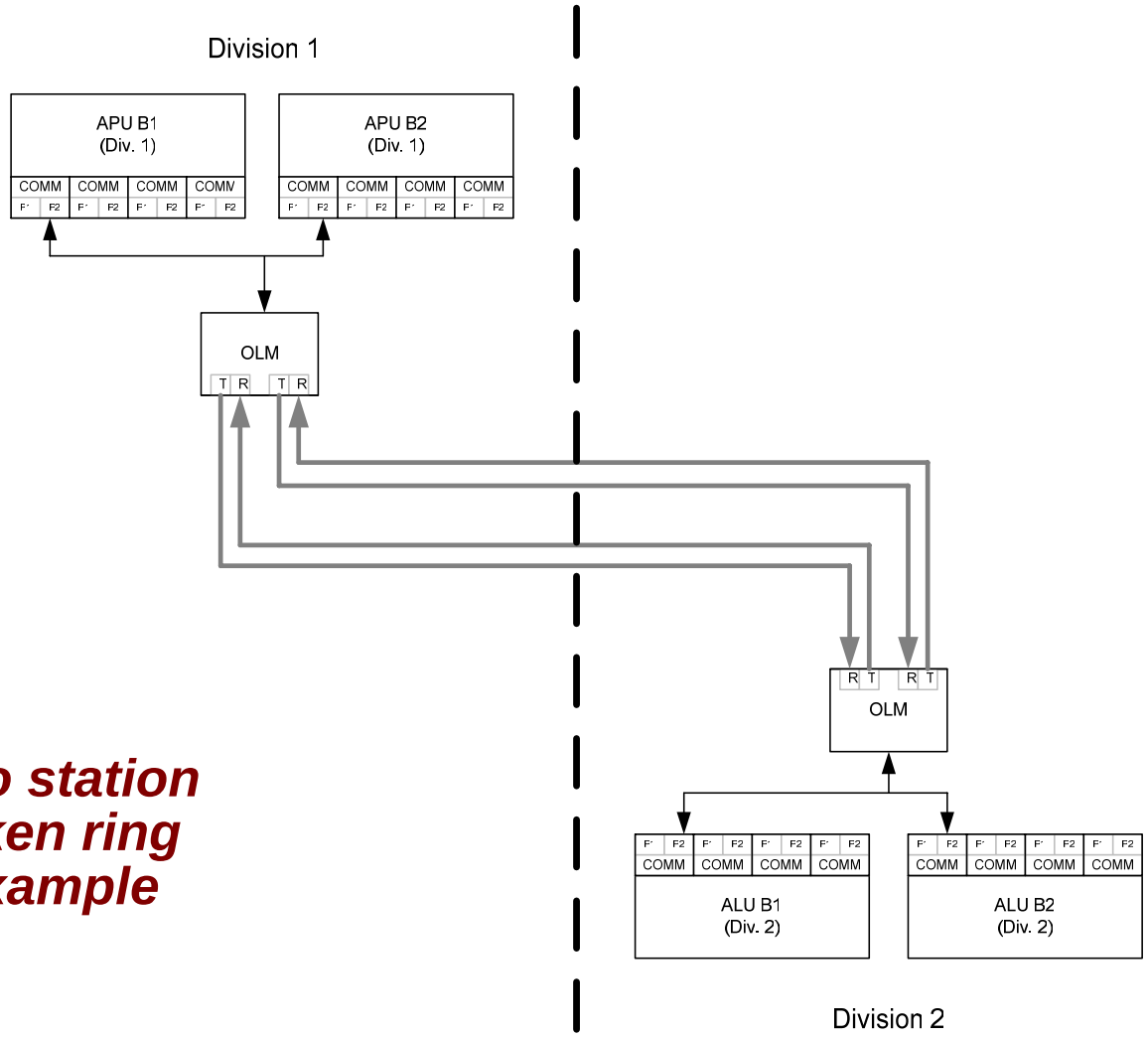



### U.S. EPR



# Topical Report

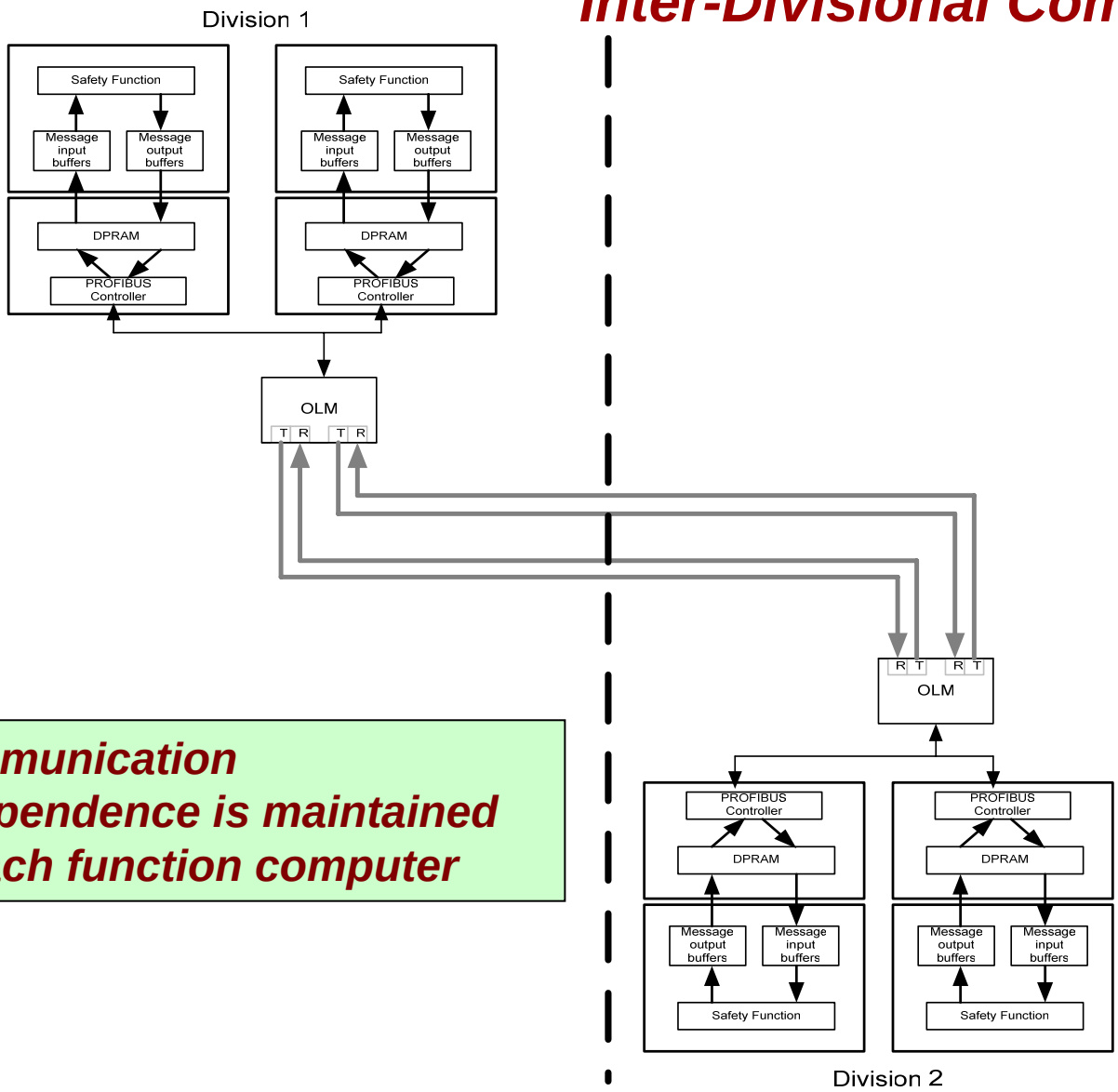
## Inter-Divisional Communication




***Two station token ring example***

# Topical Report

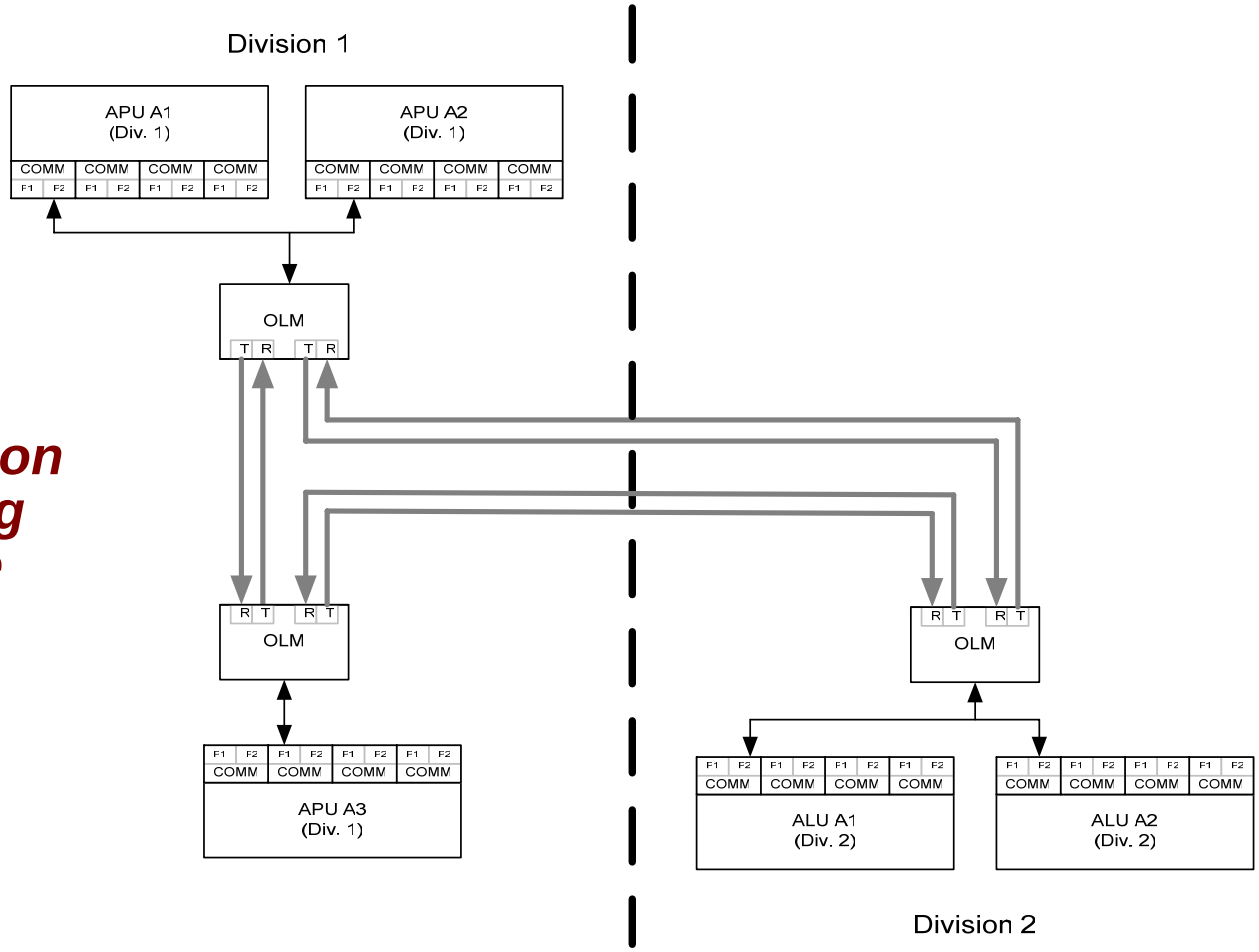
## Inter-Divisional Communication




***Communication independence is maintained at each function computer***

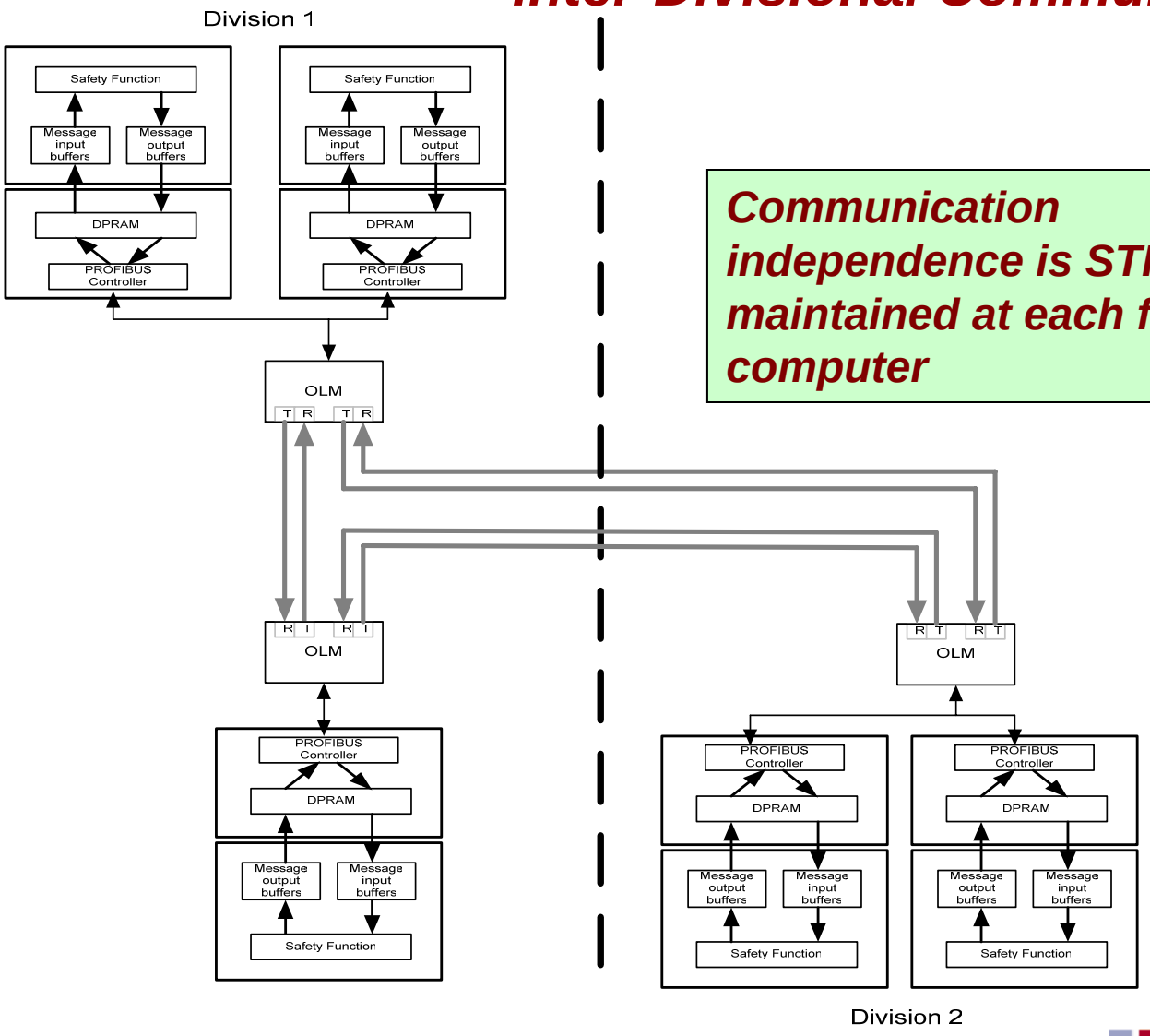
# Topical Report
## Inter-Divisional Communication

***Three station token ring example***



# Topical Report

## Inter-Divisional Communication




***Communication independence is STILL maintained at each function computer***

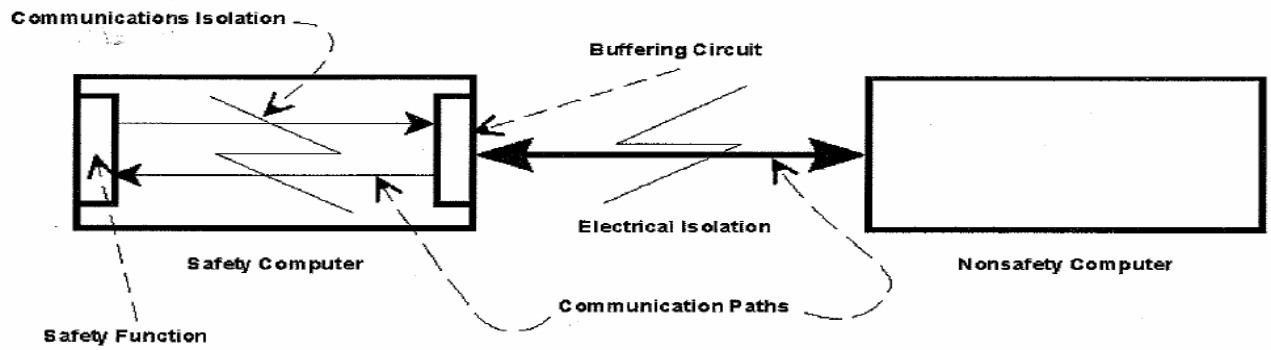
# Topical Report
## Safety/Non-Safety Interfaces

- **Three general cases**
  - **PS sends information out for display or use in non-safety systems (hardwired or network interface)**
  - **Exchange between PS and SU for diagnostics, monitoring or maintenance (network interface)**
  - **PS receives information from PICS (network interface)**
    - **ESF actuation resets**
    - **Validation/inhibition of permissive signals**
    - **Periodic testing**
- **Regulatory status**
  - **First two cases approved in the TXS SER**
  - **Third case requires approval**

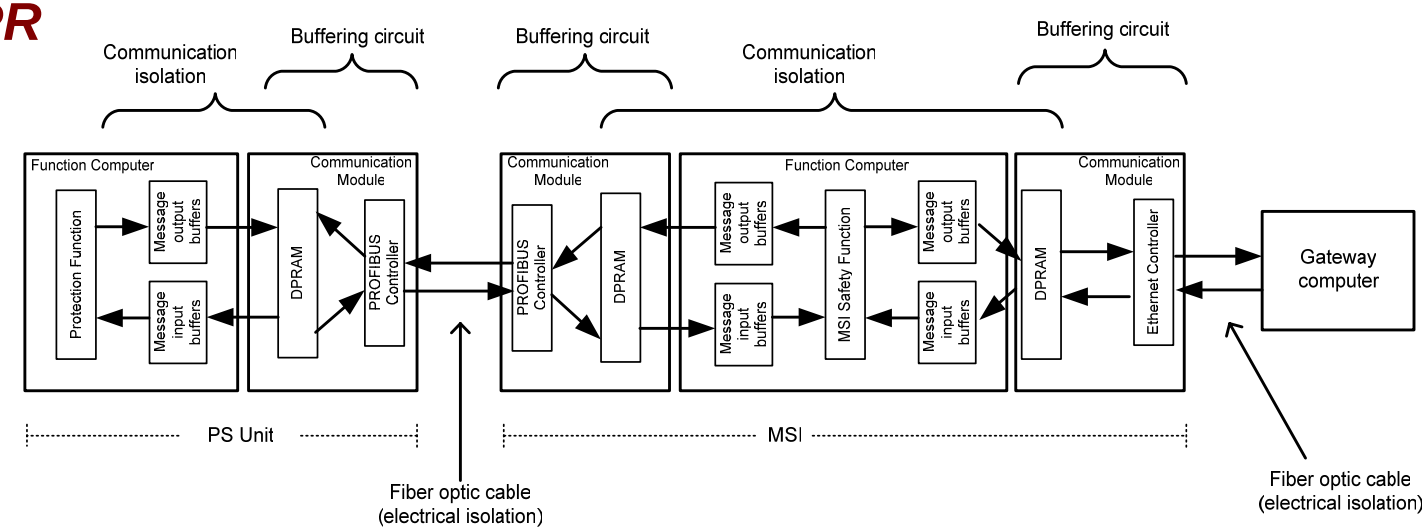
# Topical Report

## Safety/Non-Safety Communication

### IEEE 7-4.3.2




### U.S. EPR




EPR™

# Topical Report
## Safety/Non-Safety Communication

- **This interface does not prevent performance of safety functions**
  - **Protective actions not initiated through this interface**
  - **Commands from PICS required on safe shutdown path are also available on Class 1E SICS**
  - **No direct network connection between GW and function computers**
  - **Multiple layers of isolation between non-safety computer and protective function (buffering circuits, data flow separation)**
  - **MSI provides Class 1E isolation**
    - **Only checks for and uses data from expected messages**
    - **Only configured communication channels are checked**
    - **MSI does not function as part of automatic protection channels**
    - **Loss of MSI (worst case) does not lead to degradation of the automatic protection channels**

# Topical Report
## Safety/Non-Safety Control of Access

- **Physical features**
  - **Inside protected area**
  - **Separated into four areas**
  - **Key access to cabinets**
  - **Cabinet door alarms**
- **Engineered features**
  - **Engineering/service tools**
    - **Password protected**
    - **Access allowed to one safety division at a time**
    - **Access via password and key switch required to change software**
  - **Communications**
    - **Static channels (i.e., no TCP/IP or message routing services installed on the MSI)**
    - **Ignores unexpected messages**
    - **No connection outside of the plant control**
- **Administrative controls**
  - **Personnel access and work authorization**

# Summary

- The U.S. EPR Digital Protection System is redundant, reliable, and implements functional diversity
  - Four divisions
  - Two subsystems and redundant voting
- U.S. EPR Digital Protection System Topical Report describes the application of the TXS technology to the U.S. EPR design
- AREVA NP seeks an SER approving U.S. EPR-specific implementation of:
  - Protection System architecture
  - Specific network configurations
  - Typical Reactor Trip concepts and sequences
  - Typical ESFAS concepts and sequences
  - Design rules for permissive signals
  - Inter-channel communication independence
  - Safety to non-safety system interfaces
  - Compliance with relevant clauses of IEEE-603

# Summary and Next Steps

**Sandra M. Sloan**

# Summary

- **The U.S. EPR Digital Protection System:**
  - **Based on NRC approved technology (TXS)**
  - **Contains redundant divisions, functional diversity, independence, reliability, and availability**
  - **Complies with regulatory requirements and guidance**
  - **Considers latest developments**
    - **IEEE 603 and IEEE 7-4.3.2**
- **This type of interaction helps us understand NRC expectations and thus produce a high-quality DC submittal**

***Digital Protection System is safe, reliable, redundant, and complies with regulatory requirements***

# Next Steps

- **AREVA NP will submit the U.S. EPR Digital Protection System Topical Report in March 2007**
- **Next meetings:**
  - **May 2007:**
    - **I&C Diversity and Defense-in-Depth Topical Report pre-submittal**
    - **PRA Methods Report post-submittal**
    - **Equipment Qualification Program Report post-submittal**
  - **AREVA NP looks forward to timely NRC feedback and interactions to support efficient review of this topical report and inform development of the DCD**

# Abbreviations and Acronyms

| | |
|---|---|
| **ALU** | Actuation Logic Unit |
| **APU** | Acquisition & Processing Unit |
| **DCD** | Design Certification Document |
| **DPRAM** | Dual Port Random Access Memory |
| **ESF** | Engineered Safety Feature |
| **ESFAS** | Engineered Safety Feature Actuation System |
| **GW** | Gateway |
| **I&C** | Instrumentation and Controls |
| **IEEE** | Institute of Electrical and Electronics Engineers |
| **MCR** | Main Control Room |
| **MSI** | Monitoring & Service Interface |
| **MU** | Main Unit |
| **OLM** | Optical Link Module |
| **PACS** | Priority Actuation & Control System |
| **PI** | Panel Interface |

# Abbreviations and Acronyms (cont'd)

| | |
|---|---|
| **PICS** | Process Information & Control System |
| **PROFIBUS** | Process Field Bus |
| **PS** | Protection System |
| **PZR** | Pressurizer |
| **QDS** | Qualified Display System |
| **RAU** | Remote Acquisition Unit |
| **RCSL** | Reactor Control, Surveillance, and Limitation |
| **RSS** | Remote Shutdown Station |
| **RT** | Reactor Trip |
| **SAS** | Safety Automation System |
| **SER** | Safety Evaluation Report |
| **SG** | Steam Generator |
| **SICS** | Safety Information & Control System |
| **SPND** | Self Powered Neutron Detectors |
| **SU** | Service Unit |
| **TCP/IP** | Transmission Control Protocol/Internet Protocol |
| **TXS** | TELEPERM XS |

# Protection System - Function Block Definitions

- **RAU: Acquires in-core instrumentation, distributes to APU's**
- **APU: Acquires process sensors, performs threshold detection and processing functions, distributes to ALU's**
- **ALU: Performs voting of trip decisions from APU's, issues actuation orders to trip devices and PAC modules**
- **MSI: Provides 1E/non-1E isolation, performs data transfer and monitoring functions**
- **PI: Provides 1E interface to safety displays**
- **GW: Provides interface to balance of plant**