

**U.S.NRC**

United States Nuclear Regulatory Commission

*Protecting People and the Environment*

# U.S. EPR Data Communications Issues

Deanna Zhang

Electronics Engineer, NRO/DE/ICE1

June 25, 2010

# Objective

The purpose of this presentation is to present the staff's findings on the U.S. EPR I&C system architecture and data communications design with respect to meeting the NRC's regulations on functional and communications independence.

# Agenda

- Safety Significance of Issue
- Regulatory Basis for Independence
- Current NRC Guidance for Bi-directional Communication
- Examples of U.S. EPR I&C Systems Independence and Data Communications Issues
- Path forward
- Summary

## Safety Significance of Issue

- Independence is critical to assure that a safety division can accomplish its safety functions without influence from other divisions or non-safety equipment
- Without independence, failures of one division or non-safety equipment can affect all safety divisions, and result in loss of the ability to complete the intended safety functions.

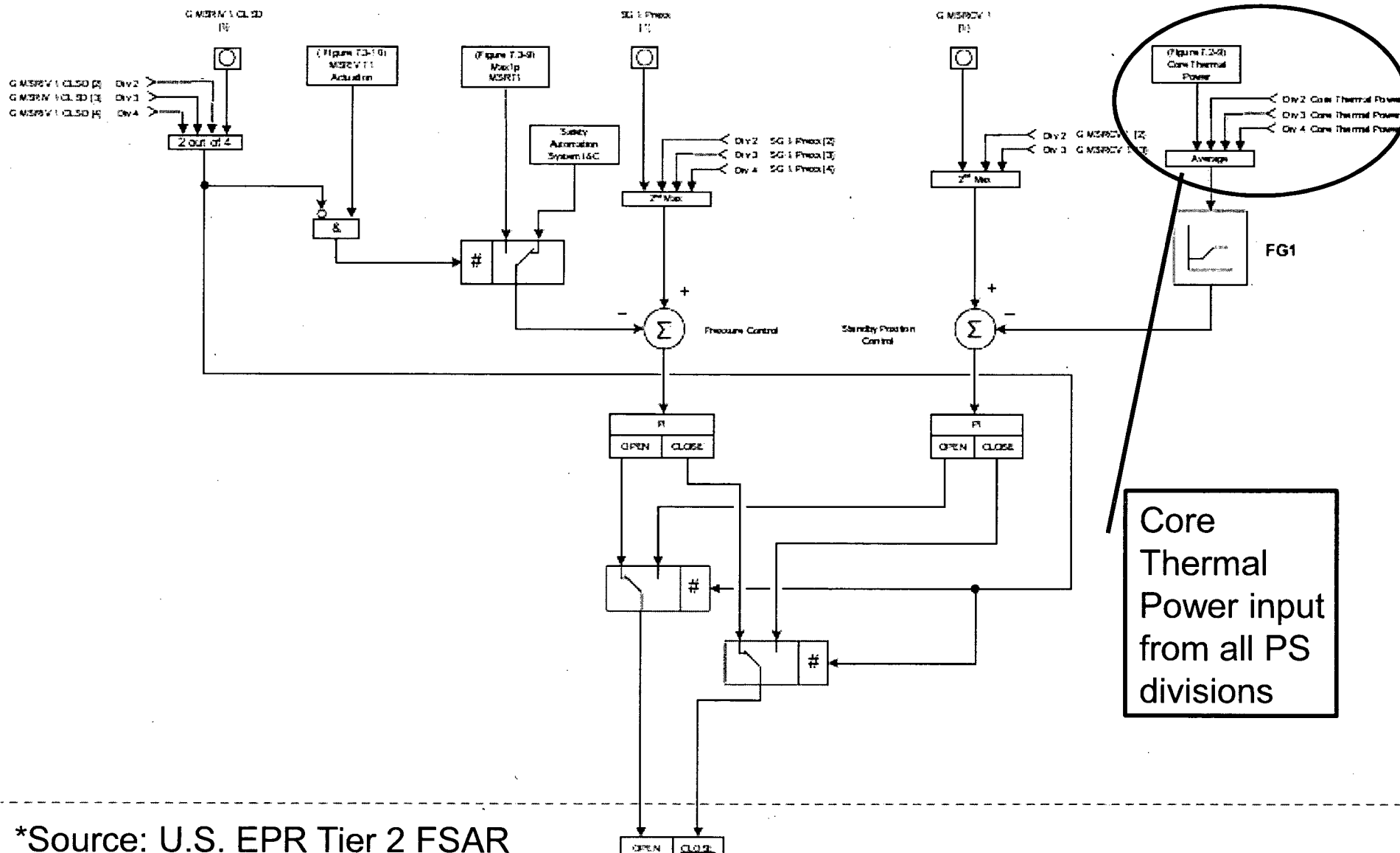
# Regulatory Basis for Independence

- IEEE Std. 603-1991, as incorporated by reference 10 CFR 50.55a(h), requires independence between redundant portions of safety systems, and between safety and non-safety systems.
  - 10 CFR Part 50, GDC 24, requires independence between protection and control systems, and minimizing interconnections between protection and control systems.
  - Regardless of communications flow, a division should not rely on information from outside the division to accomplish its safety function, and should be protected from adverse influence from outside the division.
- \*It is recognized that the division voting logic must receive inputs from other divisions.*

## Non-compliance to NRC Regulations

- The U.S. EPR I&C systems design does not meet the fundamental principle of functional independence as required by IEEE Std. 603-1991.
  - Several of the safety functions within the U.S. EPR design requires information from outside its own division to accomplish the safety function. Examples include:
    - Incore power measurements for DNBR and Linear Power Density Reactor Trip functions
    - Main Steam Relief Control Valve Control for ESF functions
  - Protection of SAS and PS from adverse influence from PICS is provided with operator action from SICSp

# SAS MSRCV Control



\*Source: U.S. EPR Tier 2 FSAR

## Current NRC Guidance on Bi-directional Communication

- The NRC issued Interim Staff Guidance (ISG)-04 to provide guidance on acceptable implementations of bi-directional communications to meet IEEE Std. 603-1991 in September, 2007.
- Section 1 of ISG-04 contains 20 criteria to ensure communications independence for bi-directional communication.
- Section 3 of ISG-04 contains criteria for multi-divisional control of safety-related equipment from both safety and non-safety control and display stations.



## U.S. EPR I&C Data Communications Issues

- In the original submittal and in subsequent responses to RAI 286, AREVA NP did not demonstrate how the U.S. EPR design addressed the criteria within Section 1 and 3 of ISG-04, or describe an acceptable alternate approach to meet NRC regulations on independence.
- AREVA NP has also not identified all interfaces between redundant safety division or between safety and non-safety equipment.
- Bi-directional flow exists between many safety to non-safety interfaces, and between safety divisions.

# Simplified U.S. EPR I&C Architecture

## Safety-Related Components

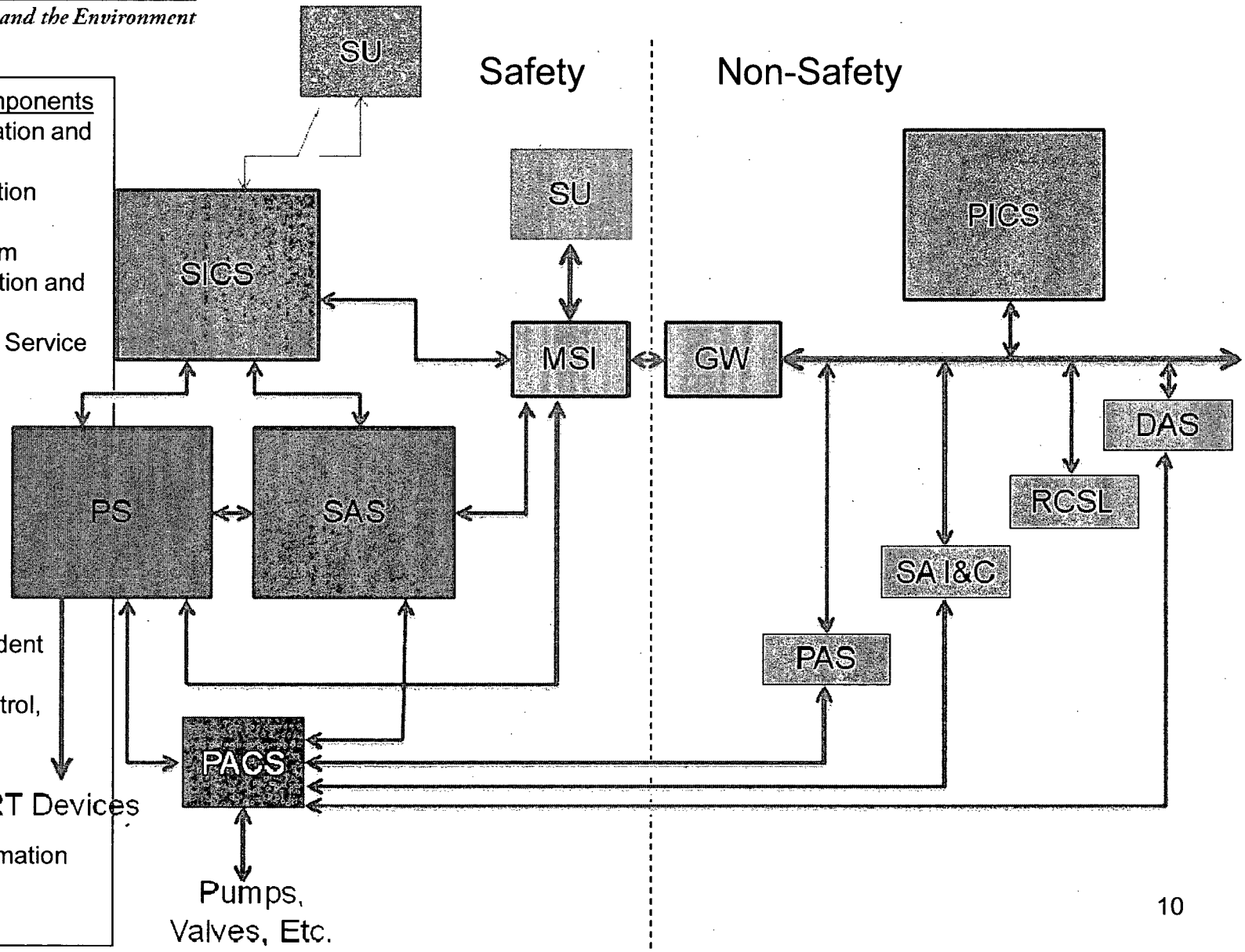
SICS-safety information and control system  
 SAS-safety automation system  
 PS-protection system  
 PACS-priority actuation and control system  
 MSI-Monitoring and Service Interface

## Non-Safety Related Components

SU-service unit  
 GW-gateway  
 PAS-process automation system  
 SA I&C-severe accident I&C  
 RCSL-reactivity control, surveillance, and limitation system  
 DAS- diverse actuation system  
 PICS-Process Information and Control System

RT Devices

Pumps, Valves, Etc.

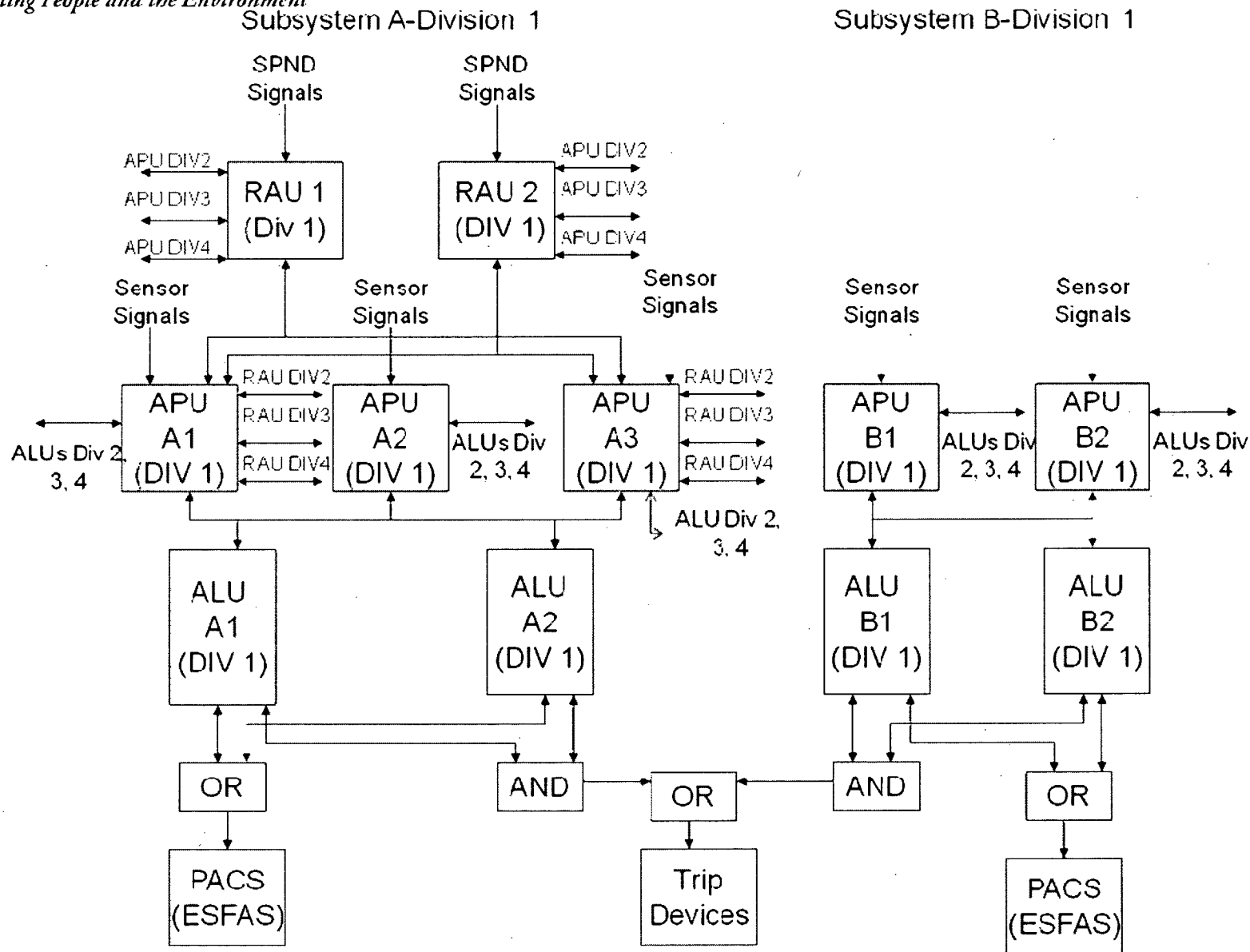




United States Nuclear Regulatory Commission

Protecting People and the Environment

# Data Communication For One Division of PS



## Non-conformance to NRC Guidance

- The applicant has not demonstrated how each criteria of ISG-04 for communications independence is satisfied or have provided sufficient justification on why an alternate approach is acceptable. Examples include:
  - Sect 1, Crit. 3: Insufficient justification for why safety divisions need to receive any communication from outside its own safety division. The communication does not enhance or support a safety function.
  - Sect 1, Crit. 8: No justification on why data exchange between redundant safety divisions or between safety and non-safety equipment is processed in a manner that does not adversely affect the safety function.
  - Sect 1, Crit. 10: Insufficient justification for continuous connection between non-safety related Service Unit and Safety Systems.
- The applicant only makes claims to conformance with certain criteria within ISG-04, and does not provide sufficient evidence to support the claim.

## Path Forward

- To achieve functional independence, the applicant must present a design such that it assures each safety division can perform its safety function independent from information received from outside the division\*.
- To ensure that the design presented for this application can be demonstrated to meet communications independence requirements, the applicant should provide a simpler design for data communications between safety divisions, and between safety and non-safety equipment with sufficient justification and evidence for the staff to reach a reasonable assurance finding

\* (with exception to voting)

# Summary

- The staff concludes that the U.S. EPR I&C systems architecture and data communications design does not meet NRC regulations for functional independence.
- The staff finds that the applicant has not demonstrated how the design addressed all criteria within ISG-#4 or proposed an acceptable alternative to meet NRC regulations for communications independence.