U.S. EPR I&C Closure Plan Progress Update

February 15, 2011

EPR™ by AREVA

AREVA

Objectives

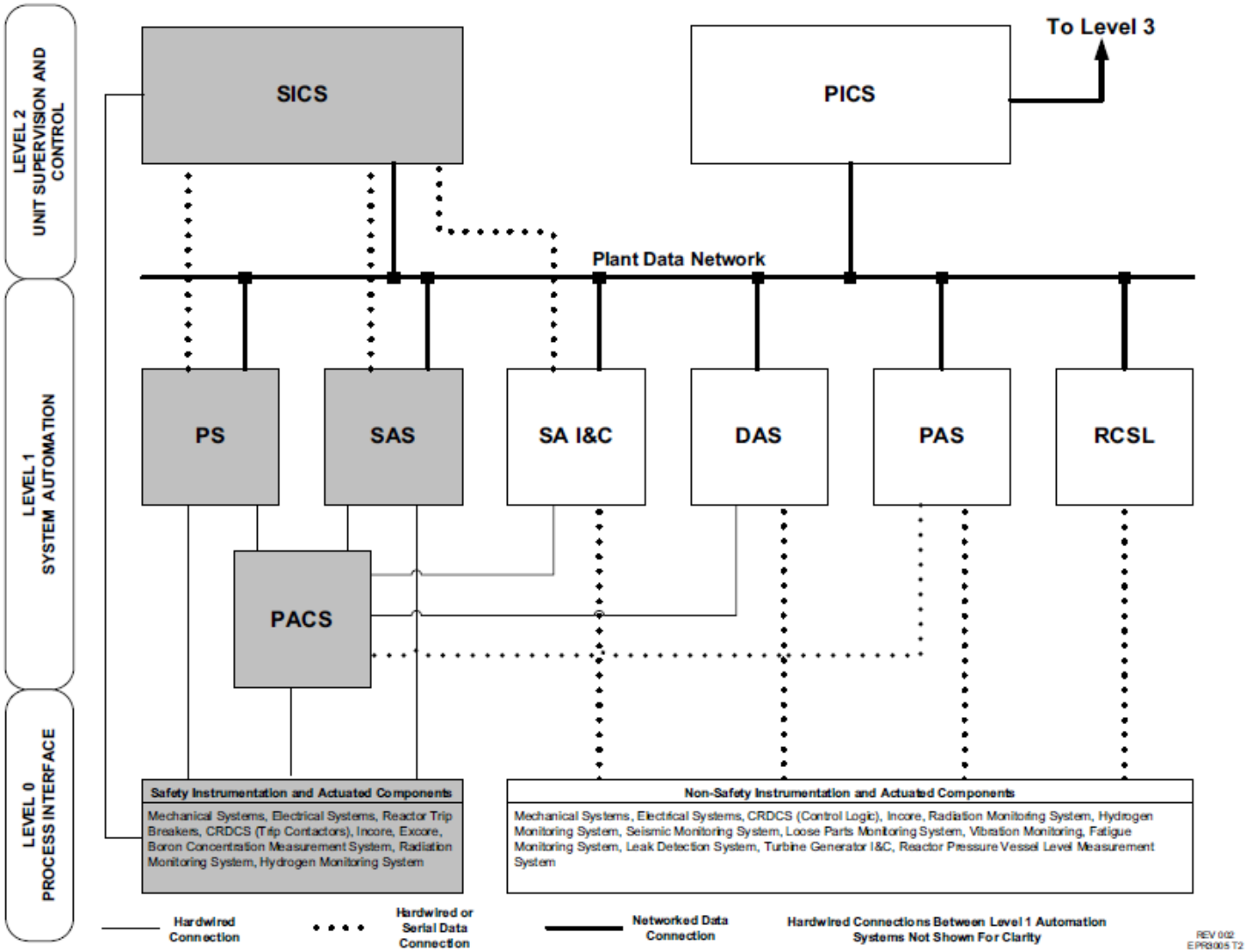
- Provide an update on development of technical solutions being implemented to address NRC concerns
- Discuss resolution of outstanding technical issues
- Provide an update and discuss the SPND alternative request
- Discuss schedule for submittal of revised documentation

Topics

- **Proposed I&C Architecture**
  - Baseline design
  - Proposed design
  - Next steps
- **PS and SAS Service Units**
  - Review proposed design
- **SAS Interdivisional Communication**
  - Status update
- **Alternative Request**
  - Issue summary
  - What to expect
- **Schedule**
  - Expected submittal timeline

Proposed I&C Architecture

Baseline I&C Architecture



NRC Concerns on Baseline I&C Architecture

- Complexity of Design
- Data Communication Between Safety Divisions
  - SICS
  - SAS
  - PS
- Data Communications from Non-Safety Service Unit (SU) to safety divisions
- Data Communications from Non-Safety Process Information and Control System (PICS) to safety divisions

Proposed I&C Architecture: Summary of Design Changes

- **Design Change #1 - Eliminated Bi-Directional Communication between PICS and PS/SAS**
  - **Basis**
    - Simplify analysis to demonstrate independence between safety and non-safety systems
  - **Description**
    - All signals from PICS to PS and from PICS to SAS are removed

Proposed I&C Architecture: Summary of Design Changes

- **Design Change #2 - Changed SICS design to a primarily hardwired system**
  - **Basis**
    - Limit need for interdivisional communication in SAS while maintaining satisfactory human factors interface
    - Limit overall complexity of safety systems
  - **Description**
    - Controls are moved from QDS to hardwired
      - Manual component controls routed directly from SICS to PACS
      - Manual grouped controls with multiple divisions will use buttons with multiple contacts to each division in SAS
    - Indications are moved from QDS to hardwired
      - PAM Type A-C and Severe Accident Indications routed directly to SICS bypassing PS and SAS
    - Limited indications will be duplicated on remaining QDS
      - Retain limited number of QDS for monitoring only
      - Displays only those parameters needed for trending and graphical display for situational awareness (expected to be similar in scope to an SPDS)

Proposed I&C Architecture: Summary of Design Changes

- **Design Change #3 - Added Signal Conditioning and Distribution System (SCDS)**
  - **Basis**
    - Simplify and clarify routing of signals acquired from the field or black boxes and are needed in multiple systems within the I&C architecture with a hardwired SICS concept
    - Simplifies D3 evaluation that PAM Type A-C variables are not subject to software CCF
  - **Description**
    - Moved signal conditioning cabinets within PS and SAS into SCDS

Proposed I&C Architecture: Summary of Design Changes

- **Design Change #4 - Removed Severe Accident I&C (SA I&C) as a stand-alone system**
  - **Basis**
    - Dedicated digital system no longer needed with hardwired SICS and SCDS
  - **Description**
    - Manual component controls for severe accident are implemented from SICS -> PACS
    - Indications for severe accident are implemented from SCDS -> SICS

Proposed I&C Architecture: Summary of Design Changes

- **Design Change #5 - Moved DAS Manual Controls from PICS to SICS**
  - **Basis**
    - Eliminate DAS reliance on plant data network
    - Reduce overall complexity
  - **Description**
    - Moved controls from PICS to SICS
    - Removed connection between DAS and PICS
    - DAS alarms and status still provided on PICS via hardwired connection to PAS

Proposed I&C Architecture: Summary of Design Changes

- **Design Change #6 - Changed DAS technology from Digital to Non-Microprocessor Technology**
  - **Basis**
    - Digital technology no longer needed with hardwired SICS interface
    - Simplifies justification of diversity between DAS and PS (e.g., NUREG/CR-7007)
  - **Description**
    - Changed technology from digital to non-microprocessor technology

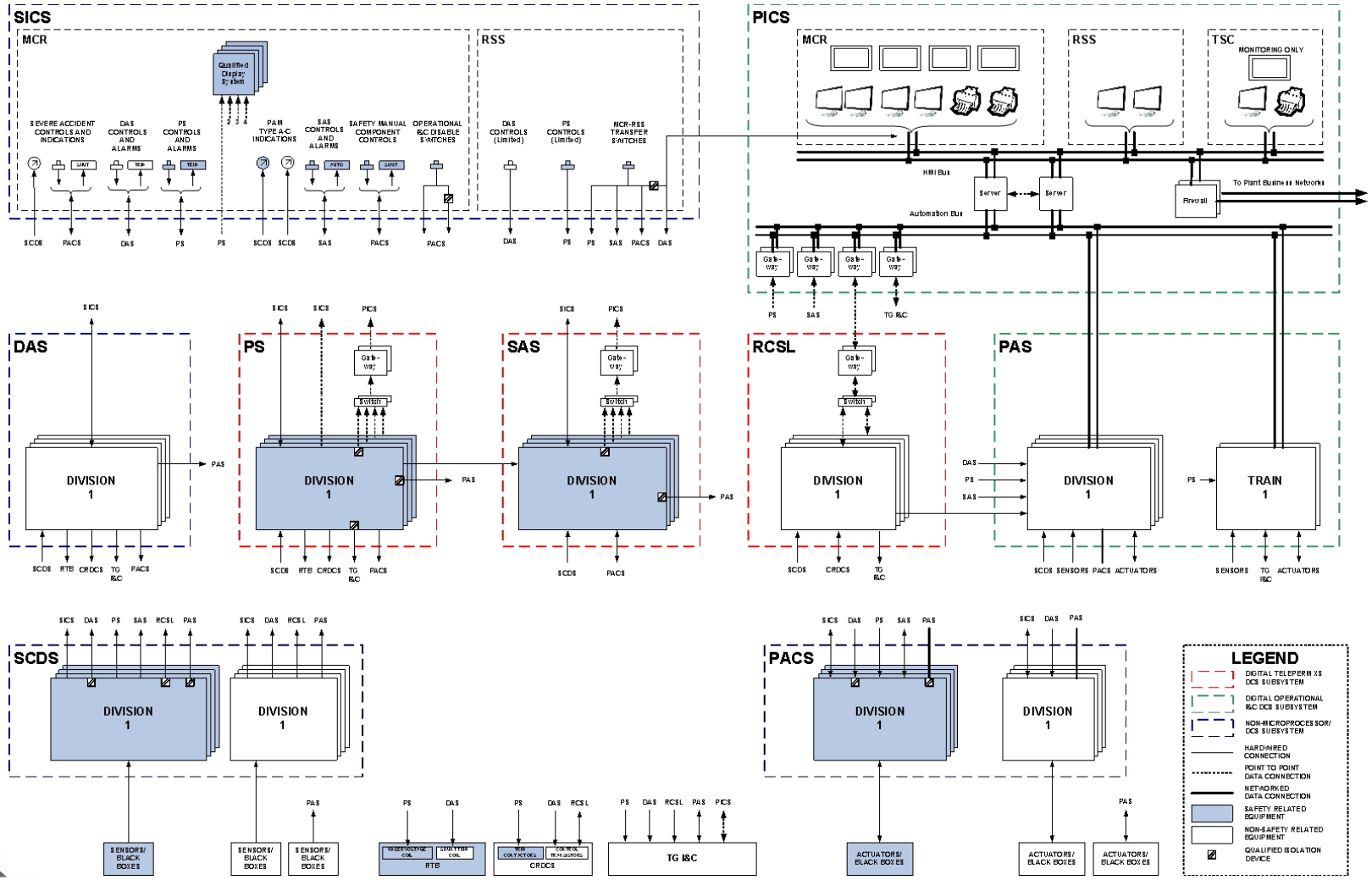
Proposed I&C Architecture: Summary of Design Changes

- **Design Change #7 - Removed RAUs and associated Networks for Sharing 72 SPND Signals from PS**
  - **Basis**
    - To simplify demonstration of independence between divisions
  - **Description**
    - Removed RAUs
    - Removed RAU to APU ring networks
    - Each PS division will acquire all 72 SPNDs hardwired from SCDS

FOR INFORMATION ONLY

The system configuration shown in this diagram is subject to final design review and approval in the AREVA design control process

Proposed I&C Architecture: Updated Drawing



Proposed I&C Architecture: Addresses NRC Concerns

- **NRC Concern**
  - **Complexity of Design**
- **Design Changes to Address NRC Concern**
  - **Design Change #2 - Changed SICS design to a primarily hardwired system**
  - **Design Change #3 - Added SCDS**
  - **Design Change #4 - Removed SA I&C as a stand-alone system; integrated controls into HW SICS concept to SCDS and PACS**
  - **Design Change #5 - Moved DAS controls from PICS to SICS**
  - **Design Change #6 - Changed DAS technology from digital to non-microprocessor based**

Proposed I&C Architecture: Addresses NRC Concerns

- **NRC Concern**
  - **Data communication between safety divisions (SICS, SAS, PS)**
- **Design Changes to Address Concern**
  - **SICS**
    - Design Change #2 - Changed SICS design to a primarily hardwired system
    - NOTE – Each QDS receives input from all 4 PS divisions. Sharing is done at QDS level which is monitoring only.
  - **SAS**
    - Design Change #2 - Changed SICS design to a primarily hardwired system
    - NOTE - Maintained capability to share data between divisions for some automatic controls => will discuss in following sections
  - **PS**
    - Design Change #7 - Removed RAUs and RAU networks for SPND sharing
    - NOTE - Single undetected failure of an SPND => will discuss in the following sections

Proposed I&C Architecture: Addresses NRC Concerns

- **NRC Concern**
  - **Data communications from Non-Safety Service Unit (SU) to safety divisions**
- **Design Change to Address Concern**
  - **Will discuss in following sections**

Proposed I&C Architecture: Addresses NRC Concerns

- **NRC Concern**
  - **Data communications from Non-Safety PICS to safety divisions**
- **Design Change to Address NRC Concern**
  - **Design Change #1 - Eliminated bi-directional communication between PICS and PS/SAS**

Proposed I&C Architecture: Next Steps

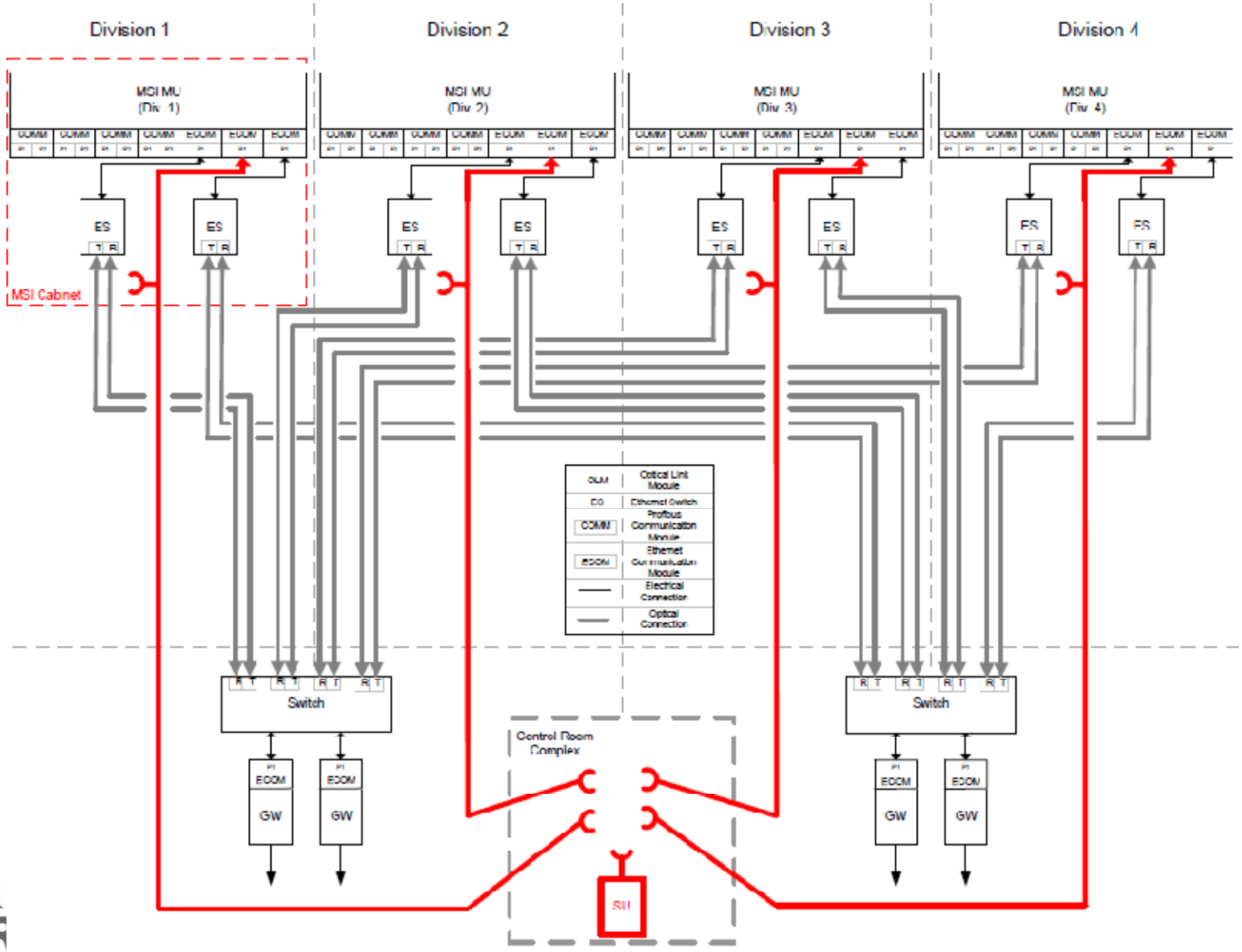
- **Finalize I&C architecture in accordance with internal AREVA design change and review processes**
- **Confirm issue resolution relative to:**
  - **PS and SAS Service Units**
  - **SAS Interdivisional Communication**
  - **PS Interdivisional Communication**

PS and SAS Service Units

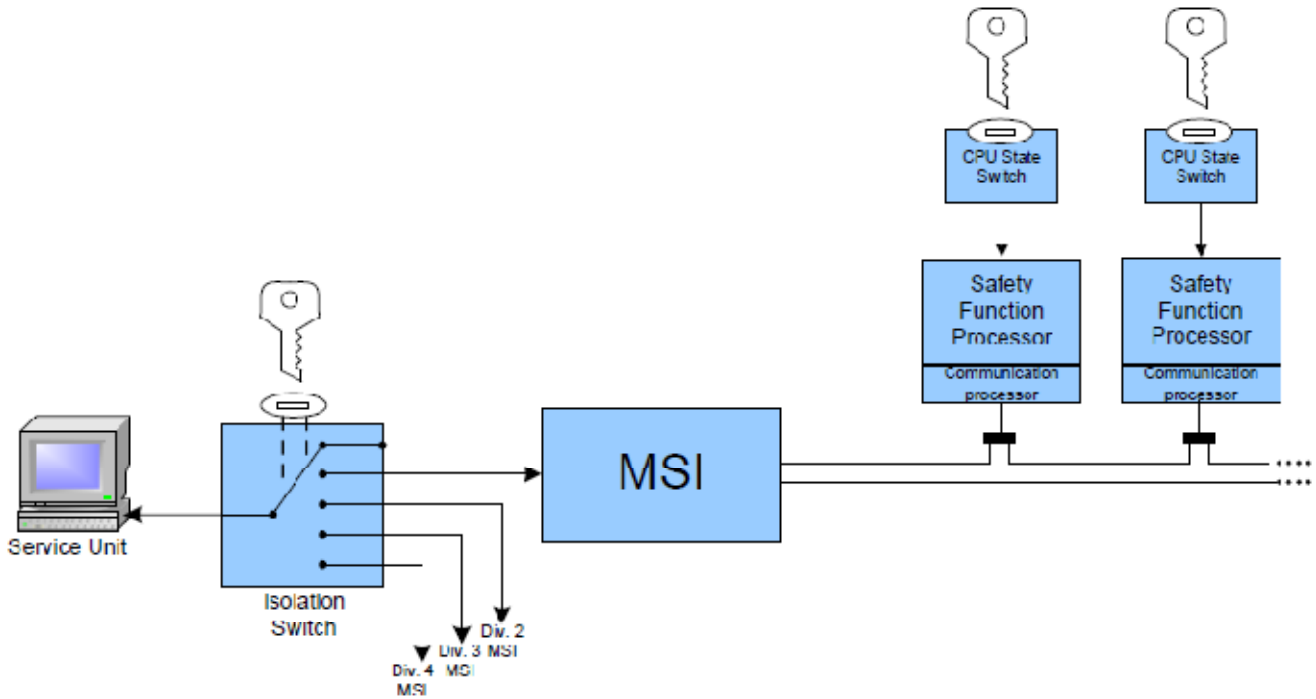
EPR™ by AREVA

AREVA

Proposed Design - Architecture



Proposed Design – Physical



- **Physical design aspects:**
  - **Isolation switch keeps SU normally disconnected and allows temporary connection to only one division at a time**
  - **Safety related MSI provides isolation barrier when SU is connected**
  - **CPU state switch per function processor ensures no changes to software from SU unless processor is in proper operational state to allow the change**

TXS Processor Operational States

- **TXS processor can be in 1 of 4 operating states**
  - **CPU mode switch must be positioned to desired state to allow change of operational state**
- **The four operational states**
  - **Cyclic processing state (OPERABLE for tech. specs.)**
    - Processor operates normally, outputs are active
    - SU cannot modify processor software or parameters
  - **Parameterization state (inoperable for tech. specs.)**
    - Processor operates normally, outputs are active
    - SU can modify pre-defined changeable parameters only (e.g., calibration constant)
  - **Functional test state (inoperable for tech. specs.)**
    - Processor outputs disabled, can be selectively enabled via SU for testing purposes
    - SU can modify pre-defined changeable parameters
  - **Diagnosis state (inoperable for tech. specs.)**
    - Processor outputs disabled, cannot be enabled
    - New version of application software can be loaded

Proposed Design - Operational

- **Operational design aspects:**
  - **The SU does not have capability to control any plant equipment**
  - **The SU is only connected in order to:**
    - **Perform tech. spec. surveillance requirements and actions** (parameterization, functional test)
    - **Diagnose a system fault following indication that a fault has occurred** (Cyclic, parameterization, functional test, Diagnosis)
    - **Load new software versions needed to implement approved plant design changes** (Diagnosis)
  - **After SU is disconnected, proper operation of the division must be verified through operator observation**
  - **If SU is not disconnected and proper operation verified within six hours of initial connection, all processors in the division are inoperable regardless of operational state**
  - **When SU is connected and a processor is placed in "parameterization" state, the processor is inoperable. If the processor is placed in "parameterization" state solely for purpose of performing a required surveillance, LCO 3.3.1 note 2 applies.**

Proposed Design - Operational

- **What happens under the following scenario:**
  1.) SU connection is required for one of the three connection reasons
  2.) SU is connected to the safety division
  3.) Required maintenance is performed
  4.) SU is disconnected and proper operation of the division is verified within six hours of initial connection
  5.) A short time later an indication is received of a fault in the same safety division

- **SU can be re-connected to the same division to address a new instance of one of the three connection reasons, subject to a new six hour limit**

There is no intent to allow for SU disconnection and immediate re-connection simply to negate administrative or technical specification controls

SU Documentation

- Information regarding physical design aspects (Architecture, key switches, physical disconnects, etc.) will be added to:
  - Tier 2, Section 7.1
  - Tier 1, Sections 2.4.1 (PS) and 2.4.4 (SAS)
- Information regarding operational aspects, plus a description of the operational states of TXS processors, will be added to:
  - Tier 2, Section 7.1
  - Technical Specification Bases 3.3.1
- COL information items already exist for administrative aspects:
  - 13.5-1 (Administrative and maintenance procedures)
  - 13.6-3 (Security program)
  - 13.6-4 (Cyber security plan)
  - 13.7-1 (Physical security plan)

SAS Interdivisional Communication

SAS Interdivisional Communication

- Design change to a primarily hardwired SICS eliminates need for SAS interdivisional communication to support:
  - Manual control functions
  - Indications and displays
- SAS interdivisional communication is still needed for some automatic functions
  - System architecture figure is being revised to explicitly show point-to-point networks
- Work focus has been: clearly define each automatic SAS function and validate that, in each case, a safety function is being performed
- Volume of SAS automatic functions:
  - 50-60 automatic SAS functions
  - 30-35 automatic SAS functions using interdivisional communication

SAS Interdivisional Communication

- **AREVA understands that interdivisional communication can be approved if:**
  - **The number of functions using interdivisional communication is minimized**
  - **The SAS functions using interdivisional communication are *all* identified**
  - **A safety basis is defined for each function**
  - **The type of information communicated is identified for each function**
- **What to expect**
  - **U.S. EPR FSAR Tier 2, Section 7.4 will contain a table that lists all automatic SAS functions with columns for:**
    - Function name
    - Function safety basis
    - Interdivisional communication (Y or N)
    - If interdivisional communication, type of information (discrete or analog)
    - If interdivisional communication, signal selection type (2nd min/2nd max or vote)

Alternative Request

Alternative Request

- **Issue Summary**
  - **Historically, single failure criterion is satisfied by providing redundancy and independence between redundancies**
  - **Because SPND are spatially dependent, they are not redundant to each other; therefore, redundancy and independence cannot be used to satisfy the single failure criterion for SPND-based trip functions**
- **November 2010 AREVA proposal:**
  - **The SPND-based reactor trip functions satisfy single failure criterion by:**
    - Using graded setpoint selection when a SPND failure is *detected* by the PS
    - Single *undetected* SPND failure is not credible
  - **AREVA would submit an alternative pursuant to 10CFR50.55a(a)(3)(i) to use graded setpoint selection to satisfy the single failure criterion in lieu of independence requirements for redundant divisions in IEEE 603-1998 Clause 5.6.1**
- **NRC requested further justification that single undetected failure is not credible**

Failure Mode Definition

- There is a difference between IEEE 603 “identifiable but undetectable” failures and “undetected” failures in PS FMEA:
  - IEEE 603 “identifiable but undetectable” failures cannot be detected via periodic testing
  - PS FMEA “undetected” failure refers to the ability of the PS to automatically detect a failure. The “undetected” SPND failure is detectable via periodic testing (performed every 15 days)

- There are no “identifiable but undetectable” failures in the PS system design

Failure Analysis

Name of Sensor, Functional Unit, or Equipment	Associated RT	Associated ESFAS	Failure Mode	Failure Cause	Method of Detection	Inherent Compensating Provision	Effect on the Protection System	Comments
Incore Detector Signals (SPNDs)	Low DNBR High HLPD	None	Detected Failure =< 6 SPNDs to all division	Not defined	TXS inherent or engineered fault detection mechanism	Failed SPND marked invalid	Degraded setpoints up to first five failed SPNDs in all divisions.	Plant still in operation. Trip function is still available.
			Detected Failure > 6 SPNDs to all division	Not defined	TXS inherent or engineered fault detection mechanism	Failed SPND marked invalid	All four divisions issue reactor trip signal => reactor trip occurs.	Plant is put into safe state
			Detected Failure =< 6 SPNDs to 1 division	Not defined	TXS inherent or engineered fault detection mechanism	Failed SPND marked invalid	Degraded setpoints up to first five failed SPNDs in affected division. Other divisions unaffected.	Plant still in operation. Trip function is still available
			Detected Failure > 6 SPNDs to 1 division	Not defined	TXS inherent or engineered fault detection mechanism	Failed SPND marked invalid	Affected division issues a vote to trip. Other divisions unaffected. Since 2/4 required to trip, there is no reactor trip.	Plant still in operation. Trip function is still available
			Undetected Failure – Spurious or Blocking	None	N/A	N/A	N/A	Failure mode is not credible due to sensor design and testing and calibration of Incore Instrumentation circuits

Failure analysis presented in public meeting Nov. 9, 2010

"Undetected" SPND Failure

- **During Dec. 2010 audit, AREVA provided justification that single undetected failure, concurrent with DBE, is not credible:**
  - **The failure mode is not possible for the SPND itself, based on the physics of the detector design**
  - **Probability for the failure mode existing in the SPND signal conditioning, concurrent with an event requiring the function, is (conservatively) on the order of 10^{-6}**

- **NRC staff indicated that a deterministic approach was preferable:**
  - **Account for this failure mode in Chapter 15 accident analysis**

  -or-
  - **Modify design to make "undetected" failure "detected"**

"Undetected" SPND Failure

- **Proposed approach: Address the undetected SPND failure in the Ch. 15 analysis**
  - **Apply existing incore trip setpoint and transient methodology (ANP-10287P) to generate new HLPD and DNBR reactor trip setpoints that account for the limiting "undetected" SPND failure**
    - Propose deterministic removal of the limiting string (for DNBR) or sensor (for LPD) from consideration in the trip threshold determination and dynamic compensation confirmation calculations
  - **Re-assess Chapter 15 events that rely on the incore system**
    - No impact on symmetric events
    - Re-confirm through analysis that the dynamic compensation provides the required protection for asymmetric events with the limiting "undetected" SPND failure present
  - **No change to ANP-10287P and no change to Chapter 15 FSAR conclusions**
    - May introduce more conservative RT setpoints in Chapter 15
    - Will add discussion in Ch. 15 to describe treatment of undetected SPND failure

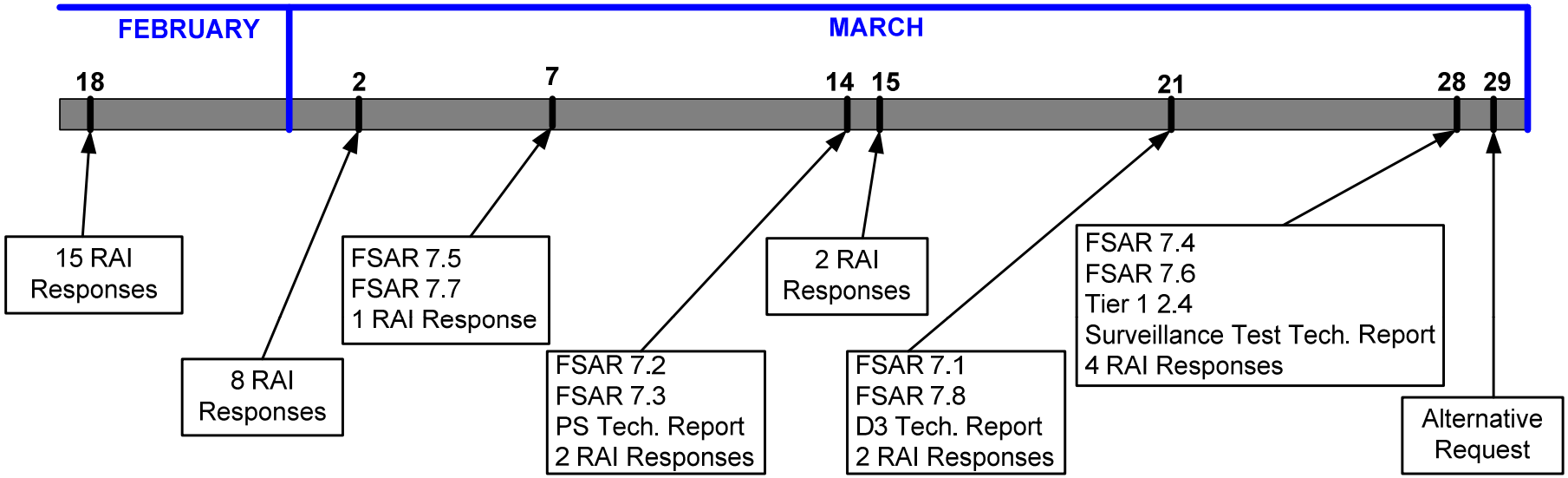
This approach provides explicit inclusion of an "undetected" SPND failure in the Chapter 15 accident analysis

Alternative Request: What to Expect

- **Alternative request letter will contain two alternative requests:**
  - **Use of IEEE Std. 603-1998 in lieu of 603-1991 to satisfy 10CFR50.55a(h)**
    - This alternative was previously submitted against ANP-10281P; that topical report was replaced with a technical report, so alternative must be re-submitted against U.S. EPR FSAR
    - Includes a table with clause-by-clause comparison of the two standards
  - **Use of alternative methods, in lieu of redundancy and independence, to satisfy IEEE Std. 603-1998 Clause 5.1, "Single Failure Criterion"**
    - Technical basis #1: graded setpoint selection to accommodate single detected failures
    - Technical basis #2: Address undetected SPND failure in Chapter 15 analysis
    - Includes description of how the undetected SPND failure will be incorporated in the Ch. 15 accident analysis
    - Includes relevant portion of FMEA addressing both detected and undetected failures

Schedule

Timeline for Draft Submittals



A schedule for submitting markups to other FSAR chapters (conforming changes) will be provided by March 14

Conclusions

- Design changes address most NRC concerns
- Resolution strategies have been proposed for these remaining issues:
  - PS and SAS service units
  - SAS interdivisional communication
  - Alternative request
- Schedule has been provided for revised documentation submittals
- Next Steps:
  - Submit RAI responses, alternative request and updated documentation
  - Continue frequent interactions with NRC staff
  - Receive NRC feedback on draft submittals to support timely submittal of final documentation

List of Acronyms

Acronym	Description
APU	Acquisition and Processing Units
CPU	Central Processing Unit
D3	Diversity and Defense-in-Depth
DAS	Diverse Actuation System
DBE	Design Basis Event
DNBR	Departure from Nucleate Boiling Ratio
FMEA	Failure Modes and Effects Analysis
HLPD	High Linear Power Density
IEEE	Institute of Electrical and Electronics Engineers
LCO	Limiting Conditions for Operation
MSI	Monitoring Service Interface
PACS	Priority and Actuator Control System
PAM	Post-Accident Monitoring
PAS	Process Automation System

Acronym	Description
PICS	Process Information and Control System
PS	Protection System
QDS	Qualified Display System
RAU	Remote Acquisition Units
RCSL	Reactor Control, Surveillance and Limitation
RT	Reactor Trip
SA I&C	Severe Accident Instrumentation and Controls
SAS	Safety Automation System
SCDS	Signal Conditioning and Distribution System
SICS	Safety Information and Control System
SPND	Self-Powered Neutron Detector
SU	Service Unit
TXS	Teleperm XS