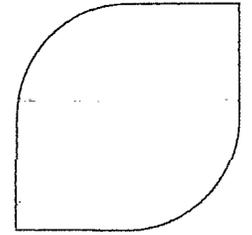


U.S. EPR Protection System: SPND-Based Reactor Trip Functions

Shelby Small – I&C Systems Engineer
Aug. 30, 2010

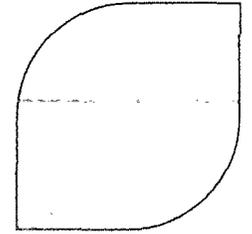


Purpose

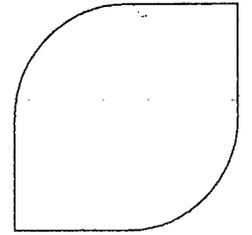


- **Following June 25, 2010 public meeting, AREVA NP:**
 - ◆ **Evaluated NRC feedback relative to SPND-based functions**
 - ◆ **Re-evaluated the relevant regulatory requirements**
 - ◆ **Re-evaluated the design of the SPND-based functions**
- **This presentation represents the conclusions of our evaluation, which include:**
 - ◆ **The current design of the SPND-based functions satisfies all regulations for independence.**
 - ◆ **NRC feedback included some points that are not well understood or may inaccurately represent the U.S. EPR design.**
 - ◆ **More detail is needed regarding exactly which aspects of the system are viewed as non-compliant with exactly which regulations.**
- **Purpose of the presentation:**
 - ◆ **Clearly convey AREVA NP understanding of independence regulations and how the SPND-based functions are in compliance.**
 - ◆ **Gain a more detailed understanding of NRC concerns to better understand how to address them.**

Presentation Outline

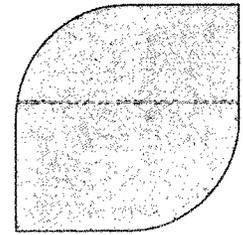


- **I&C Implementation of SPND-based RT functions**
- **Independence Regulations**
- **Independence for SPND-Based Reactor Trip Functions**
- **NRC Concerns Conveyed on June 25, 2010**



Overview of I&C Implementation of SPND- based RT functions

Relationship between Reactor Core Design and I&C Implementation of SPND Functions



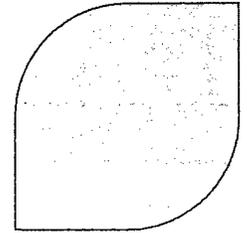
- Advantages of using of in-core SPND measurements:
 - ◆ Direct measurement of linear power density (LPD).
 - ◆ Accurate evaluation of DNBR.
 - ◆ Protection of SAFDLs based on measurements which directly represent the phenomena that could challenge the SAFDLs.

- In the U.S. EPR reactor core design, in-core flux measurement is fundamental to protection of SAFDLs.

- Adequate protection of the SAFDLs depends on use of all 72 measurements together, in aggregate.

The availability of 72 SPND measurements in each PS division is a fundamental feature of core protection reflected in the U.S. EPR safety analysis.

Holistic Treatment of Requirements

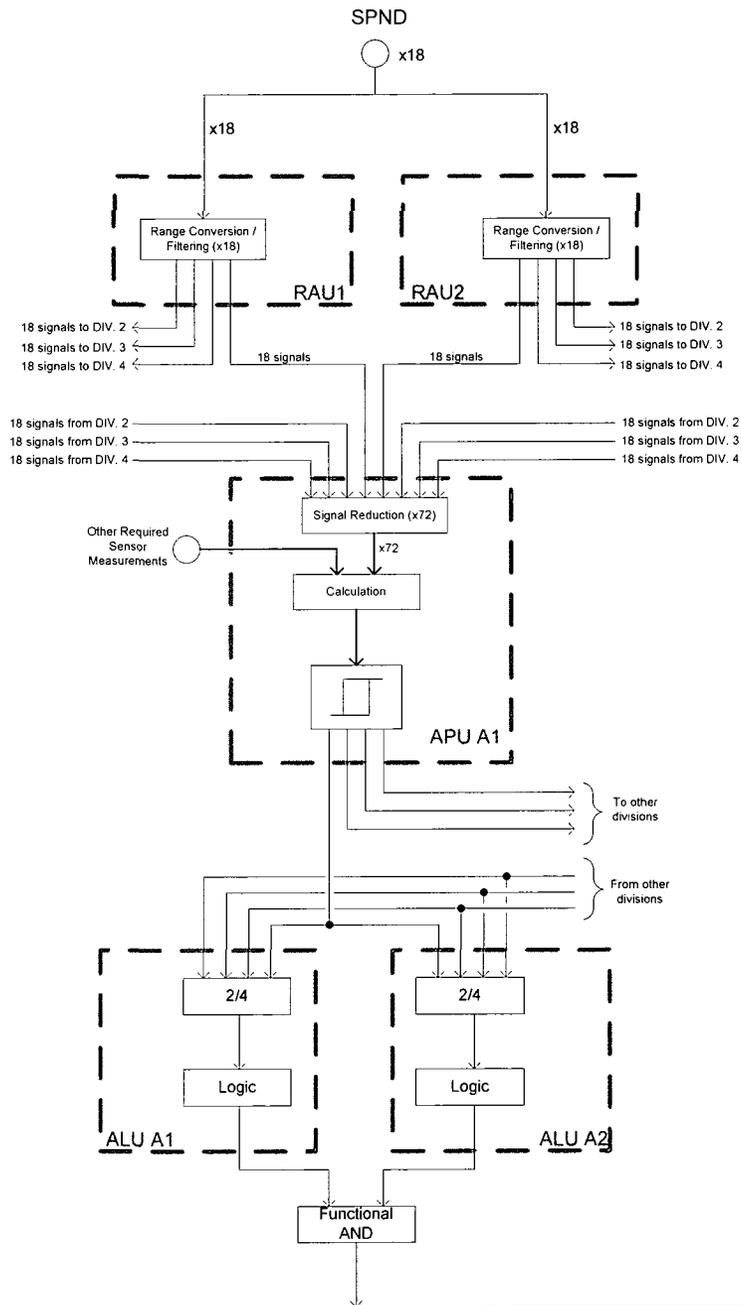
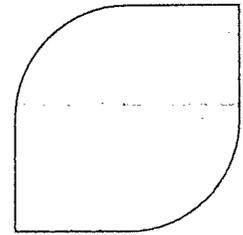


- **There are multiple types of requirements that must be addressed:**
 - ◆ **Regulatory requirements**
 - ◆ **Stakeholder requirements**
 - ◆ **Functional requirements**
 - ◆ **Performance requirements**
 - ◆ **Etc.**

- **Key design requirements/constraints to consider in conjunction with regulatory requirements for independence:**
 - ◆ **72 SPND measurements used in each PS division.**
 - ◆ **Sensed parameter is spatially dependent, not homogenous throughout the core.**
 - ◆ **Physical core design does not allow for multiple SPND at each location.**
 - ◆ **SPND signal is nano-amps. Signal cannot be split until amplified (i.e., has already been “divisionalized” for electrical purposes).**

I&C implementation of these functions reflects consideration of all requirements; not just independence requirements.

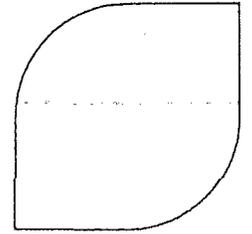
Overview of I&C Implementation



➤ One division represented

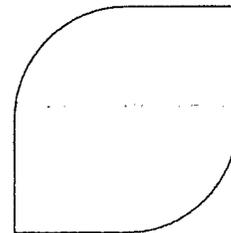
- ◆ 18 SPND acquired redundantly by two RAU. Redundancy is within a division.
- ◆ Each RAU sends 18 SPND to APU in each of four divisions. Redundancy achieved through network topologies.
- ◆ APU selects more conservative of two signals for each SPND measurement. DNBR and HLPD calculations performed. Setpoint comparisons performed. Redundancy is between divisions.
- ◆ Results of setpoint comparisons sent from APU in each division to ALU in all four divisions. Redundancy is between divisions.
- ◆ 2/4 voting performed in ALUs in all four divisions. Redundancy is between divisions.

Overview of I&C Implementation (Cont.)



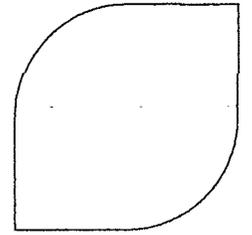
➤ Important fault-tolerant features designed into SPND-based functions:

- RAU →
 - ◆ Range monitoring of SPND input signals
- APU {
 - ◆ Selection of more conservative of two signals for each SPND.
 - ◆ 2nd min selection between 12 calculated DNB values (1 DNB value per string).
 - ◆ 2nd max selection between 72 calculated HLPD values (1 HLPD value per SPND).
- ALU {
 - ◆ Calculation of imbalance between symmetric pairs of SPND.
 - ◆ Use of more conservative RT setpoints for 1, 2, 3, 4 or 5 invalid SPND signals.
 - ◆ Tech. spec. administrative control to reduce power for 6 invalid SPND signals (conservative setpoint for 5 invalid SPND still active).
 - ◆ Automatic RT for 7 or more invalid SPND signals.
- ALU {
 - ◆ Detection of rod drops to invoke more conservative setpoints.
 - ◆ 2/4 voting on setpoint comparison results.



Independence Regulations

Independence Regulations



➤ **GDC 21- Protection system reliability and testability**

- ◆ Redundancy and independence designed into the protection system shall be sufficient to assure that (1) no single failure results in loss of the protection function and (2) removal from service of any component or channel does not result in loss of the required minimum redundancy unless the acceptable reliability of operation of the protection system can be otherwise demonstrated.

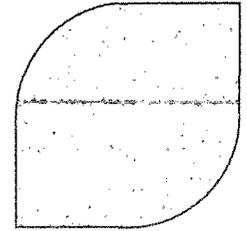
➤ **GDC 22 – Protection system independence**

- ◆ The protection system shall be designed to assure that the effects of natural phenomena, and of normal operating, maintenance, testing, and postulated accident conditions on redundant channels do not result in loss of the protection function, or shall be demonstrated to be acceptable on some other defined basis.

➤ **GDC 23 – Protection system failure modes**

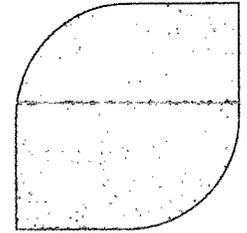
- ◆ The protection system shall be designed to fail into a safe state or into a state demonstrated to be acceptable on some other defined basis if conditions such as disconnection of the system, loss of energy (e.g., electric power, instrument air), or postulated adverse environments (e.g., extreme heat or cold, fire, pressure, steam, water, and radiation) are experienced.

Independence Regulations



- **10 CFR 50.55a(h)**
- **IEEE 603-1998, Clause 5.6.1 “Independence between redundant portions of a safety system”**
 - ◆ Redundant portions of a safety system provided for a safety function shall be independent of, and physically separated from, each other to the degree necessary to retain the capability of accomplishing the safety function during and following any design basis event requiring that safety function.
- **IEEE 603-1998, Clause 6.4 “Derivation of system inputs”**
 - ◆ To the extent feasible and practical, sense and command feature inputs shall be derived from signals that are direct measures of the desired variables as specified in the design basis

Compliance with GDC 21 – SPND RT Functions



GDC 21

Redundancy and independence designed into the protection system shall be sufficient to assure that (1) no single failure results in loss of the protection function and (2) removal from service of any component or channel does not result in loss of the required minimum redundancy unless the acceptable reliability of operation of the protection system can be otherwise demonstrated.

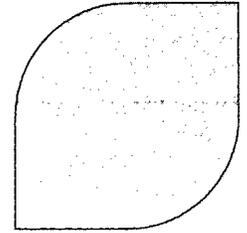
➤ **No single failure results in loss of RT functions**

- ◆ **Demonstrated through FMEA summarized in U.S. EPR FSAR Tier 2, Section 7.2.**

➤ **Removal from service of any component does not result in loss of required minimum redundancy unless acceptable reliability is demonstrated**

- ◆ **With exception of RAUs, any PS component can be removed from service with redundancy retained (FMEA including single failure + maintenance audited by NRC in 2009)**
- ◆ **RAU removed from service: acceptable reliability of RT function is otherwise demonstrated**
 - Technical specification limit of 6 hours or power reduction to <10%, consistent with IEEE 603-1998 Clause 6.7
 - Described in response to RAI 309, Q 7.09-59

Compliance with GDC 22 – SPND RT Functions



GDC 22

The protection system shall be designed to assure that the effects of natural phenomena, and of normal operating, maintenance, testing, and postulated accident conditions on redundant channels do not result in loss of the protection function, or shall be demonstrated to be acceptable on some other defined basis.

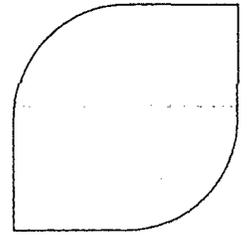
➤ **Natural phenomena do not cause loss of protection function**

- ◆ **PS located in safeguard buildings designed to protect against natural phenomena (Tier 2, Section 7.1.2.2.2)**
- ◆ **PS equipment seismically qualified (Tier 2, Section 7.1.1.4.1)**

➤ **Normal operating, maintenance, testing conditions do not result in loss of the protection function**

- ◆ **Technical specification controls are applied so that normal operating, maintenance, and testing conditions do not result in loss of the protective function (Tier 2, Chapter 16, LCO 3.3.1)**

Compliance with GDC 22 – SPND RT Functions (Cont.)



➤ Accident conditions do not result in loss of the protection function

◆ SPND located in the core:

- Qualified to accident environment (harsh environment qualification IAW Tier 2, Section 3.11)

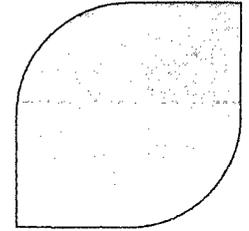
◆ SPND cabling in containment

- Qualified to accident environment (harsh environment qualification IAW Tier 2, Section 3.11)

◆ Remainder of PS:

- Location in mild environment protected from effects of accident (Tier 2, Section 7.1.1.4.1)
- Class 1E equipment qualification (Tier 2, Section 7.1.1.4.1)

Compliance with GDC 23 – SPND RT Functions



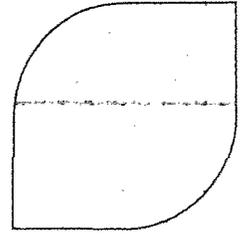
GDC 23

The protection system shall be designed to fail into a safe state or into a state demonstrated to be acceptable on some other defined basis if conditions such as disconnection of the system, loss of energy (e.g., electric power, instrument air), or postulated adverse environments (e.g., extreme heat or cold, fire, pressure, steam, water, and radiation) are experienced.

- **Automatic RT on 7 or more invalid SPND measurements is consistent with GDC 23.**
- **SPND-based RT functions fail into a safe state in case of:**
 - ◆ Complete disconnection of data communication between divisions (multiple network failures or multiple communication processor failures)
 - ◆ Complete loss of electrical power to one division (failure of normal supply + failure of backup batteries + failure of emergency diesels)
 - ◆ Adverse environment that incapacitates both RAU in a division
- **No postulated single failure causes the system to revert to the safe state.**

All protective functions in the U.S. EPR design revert to the safe state when the function can no longer be reliably performed due to accumulation of detected failures.

Compliance with IEEE 603-1998 Clause 5.6.1 – SPND RT Functions

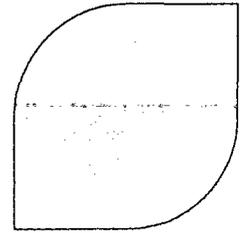


IEEE 603-1998, Clause 5.6.1 (via 10 CFR 50.55a(h))

Redundant portions of a safety system provided for a safety function shall be independent of, and physically separated from, each other to the degree necessary to retain the capability of accomplishing the safety function during and following any design basis event requiring that safety function.

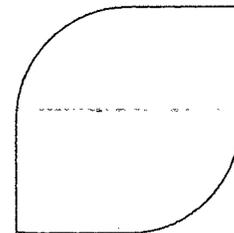
- **The following are implemented between redundant portions of PS to assure independence (Tier 2, Section 7.1.1.6.4):**
 - ◆ **Physical separation**
 - ◆ **Electrical isolation**
 - ◆ **Communication isolation**

Compliance with IEEE 603-1998 Clause 5.6.1 – SPND RT Functions (Cont.)



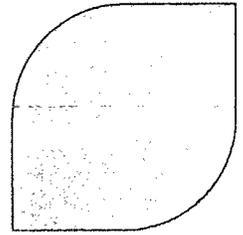
- **Application of IEEE 603 Clause 5.6.1 must be consistent with GDC 21 and GDC 22 independence requirements.**
 - ◆ **GDC 21: no single failure results in loss of protection function.**
 - ◆ **GDC 22: postulated accident conditions do not result in loss of protection function.**

- **IEEE 603-1998 Clause 5.6.1 is satisfied if the safety function can be performed in the presence of postulated accident conditions and any credible single failure.**
 - ◆ **Compliance is demonstrated by:**
 - Accounting for, or dispositioning, postulated accident conditions.
 - Postulating a credible single failure anywhere in the PS.
 - Confirming that system design features for independence (i.e., physical separation, electrical isolation, communication isolation) protect redundant portions of the system from the failure, allowing the redundant portions to perform the safety function.



Independence for SPND-Based Reactor Trip Functions

Independence Assessment



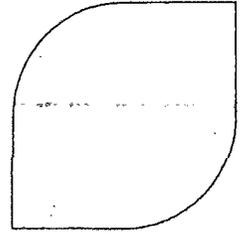
- **The following slides outline the approach to demonstrate compliance with independence requirements which includes:**
 - ◆ **Dispositioning postulated accident conditions**
 - ◆ **postulating single failures of the various components involved in performing the SPND-based RT functions.**
 - ◆ **For each failure, identifying mitigation features and independence features that assure performance of the safety function.**

- **It is expected that more detailed discussions will be needed to fully elaborate the mitigation and independence aspects for some failures.**

- **AREVA NP will support such detailed discussion today, to the extent allowed by time. A follow-on audit to inspect detailed analysis documentation would be prudent.**

The focus today is to reach agreement that this analysis approach is an acceptable means to demonstrate sufficient independence.

Disposition of Postulated Accident Environment



➤ Accident conditions do not result in loss of the protection function

◆ SPND located in the core:

- Qualified to accident environment (harsh environment qualification IAW Tier 2, Section 3.11)

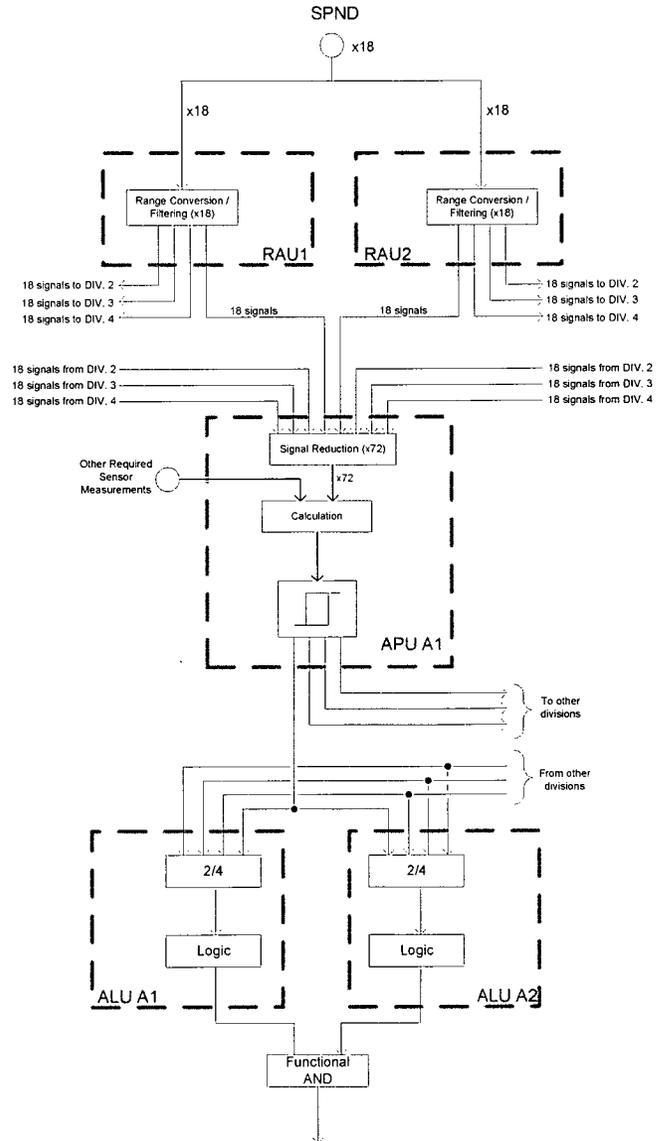
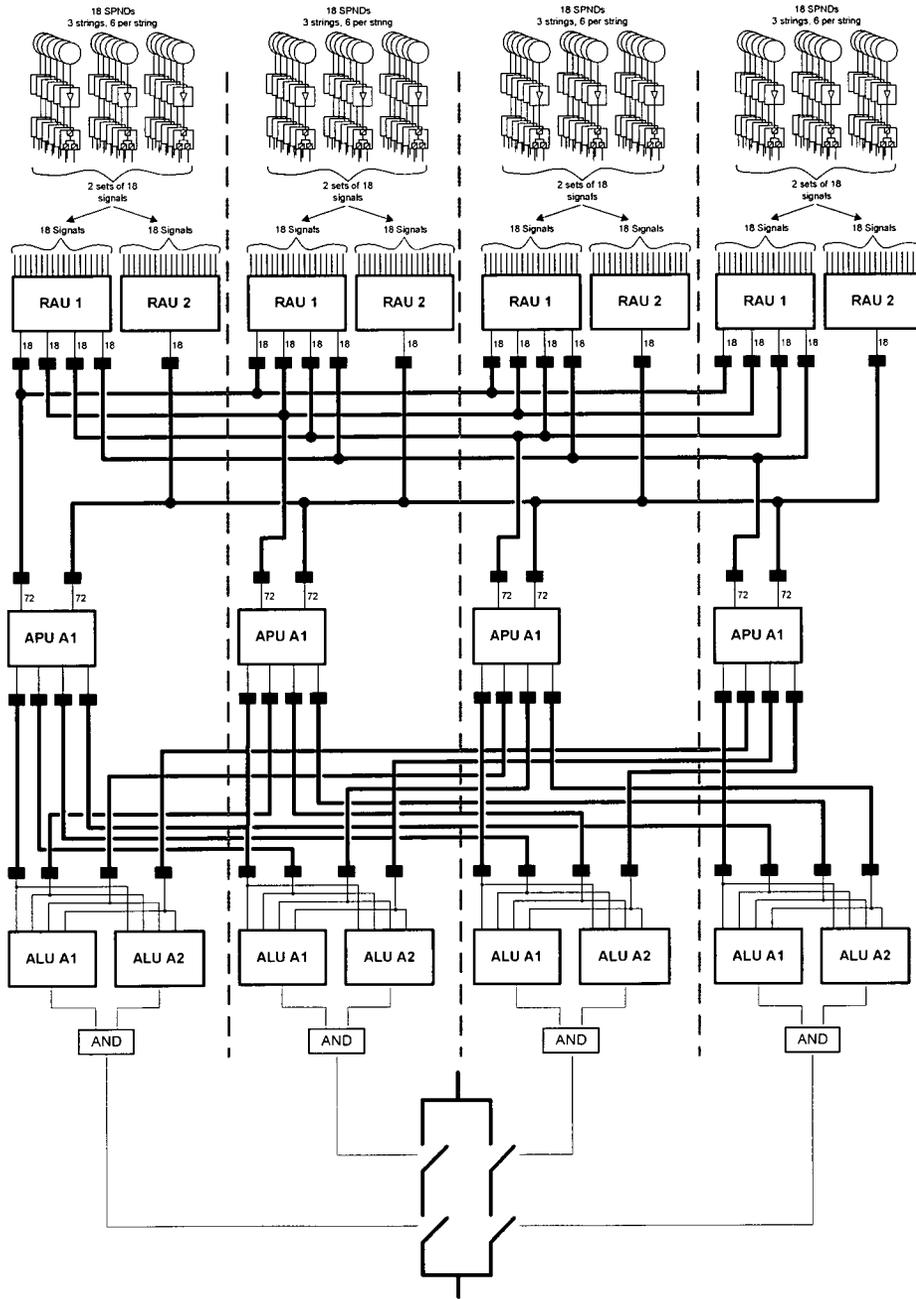
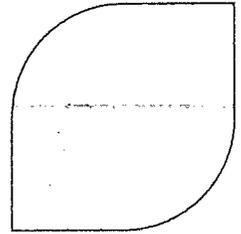
◆ SPND cabling in containment

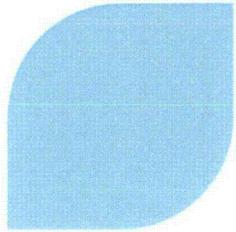
- Qualified to accident environment (harsh environment qualification IAW Tier 2, Section 3.11)

◆ Remainder of PS:

- Location in mild environment protected from effects of accident (Tier 2, Section 7.1.1.4.1)
- Class 1E equipment qualification (Tier 2, Section 7.1.1.4.1)

See Handout





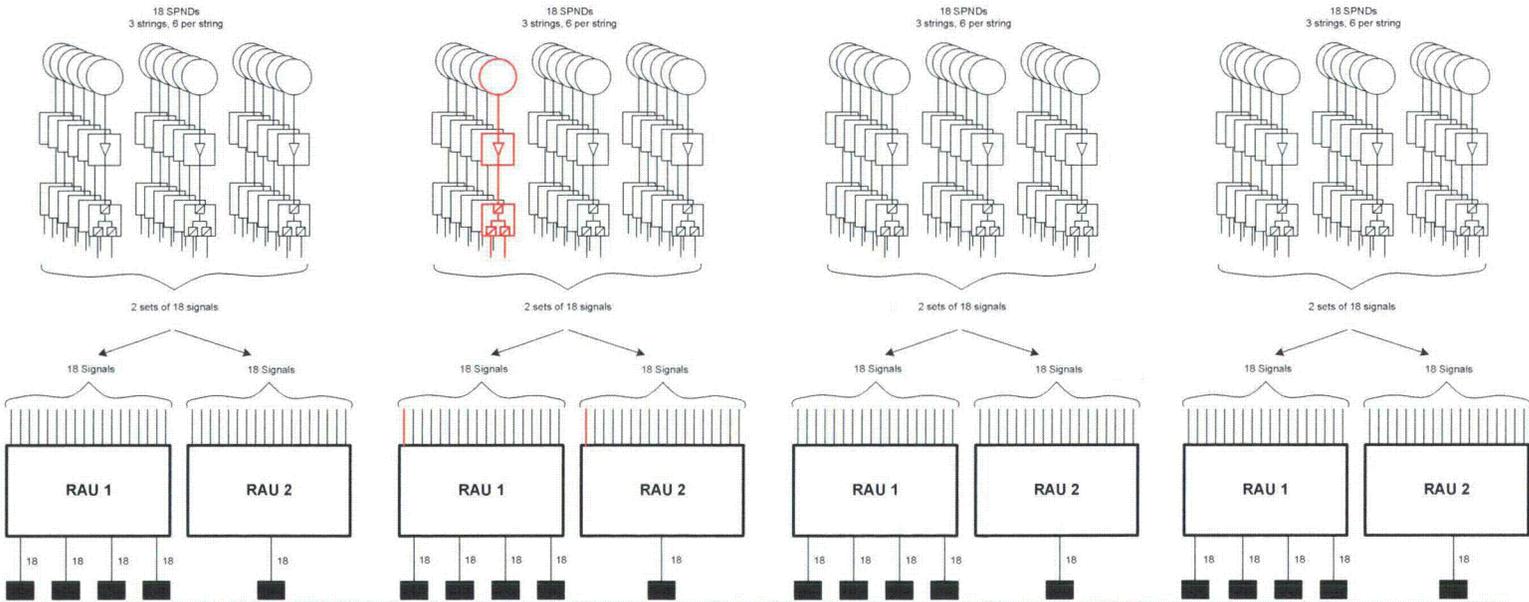
➤ **Single failure: Input channel**

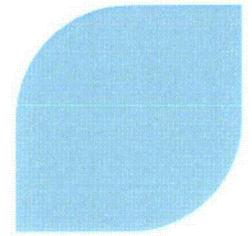
➤ **Mitigation:**

- ◆ **If detected failure: more conservative setpoint used.**
- ◆ **If undetected spurious failure: 2nd min./2nd max selection in APU**
- ◆ **If undetected blocking failure: Other SPND detect symmetrical event, imbalance functionality accommodates asymmetrical event.**

➤ **Independence features:**

- ◆ **Electrical isolation between RAU input channels.**
- ◆ **Physical separation between RAU input channels.**





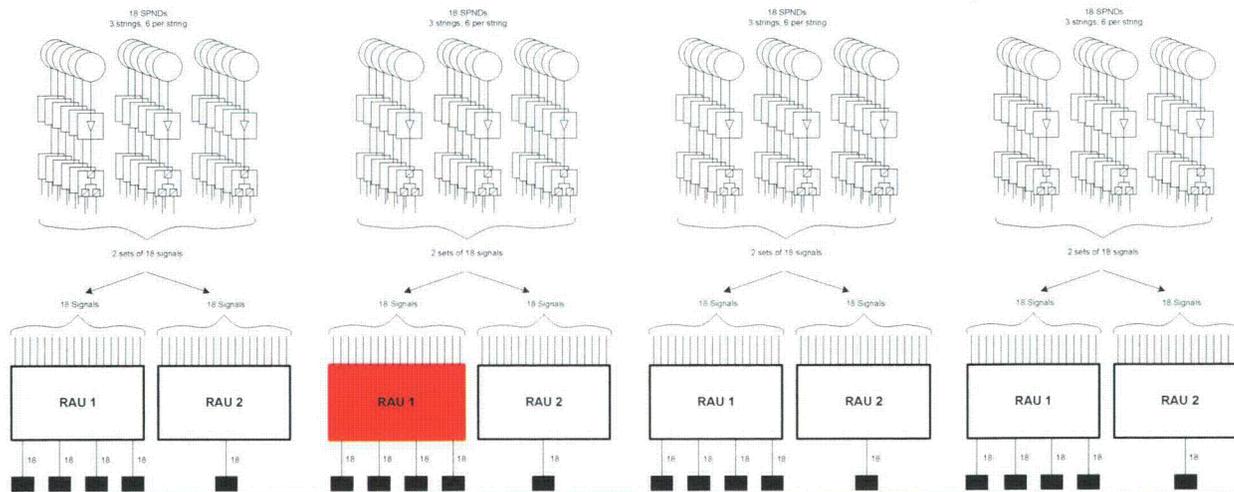
➤ **Single failure: RAU 1 or RAU 2**

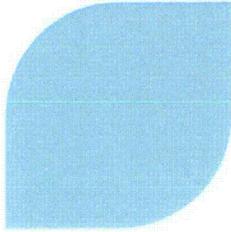
➤ **Mitigation:**

- ◆ **If detected failure: all outputs flagged faulty, redundant RAU performs function.**
- ◆ **If undetected spurious failure: Multiple spurious values sent (worst case) leads to spurious RT.**
- ◆ **If undetected blocking failure: Other RAU sends correct values, APU selects conservative values (which would be the correct values in this case).**

➤ **Independence features:**

- ◆ **Electrical isolation between RAU 1 and RAU 2.**
- ◆ **Physical separation between RAU 1 and RAU 2.**
- ◆ **No data communication between RAU 1 and RAU 2.**





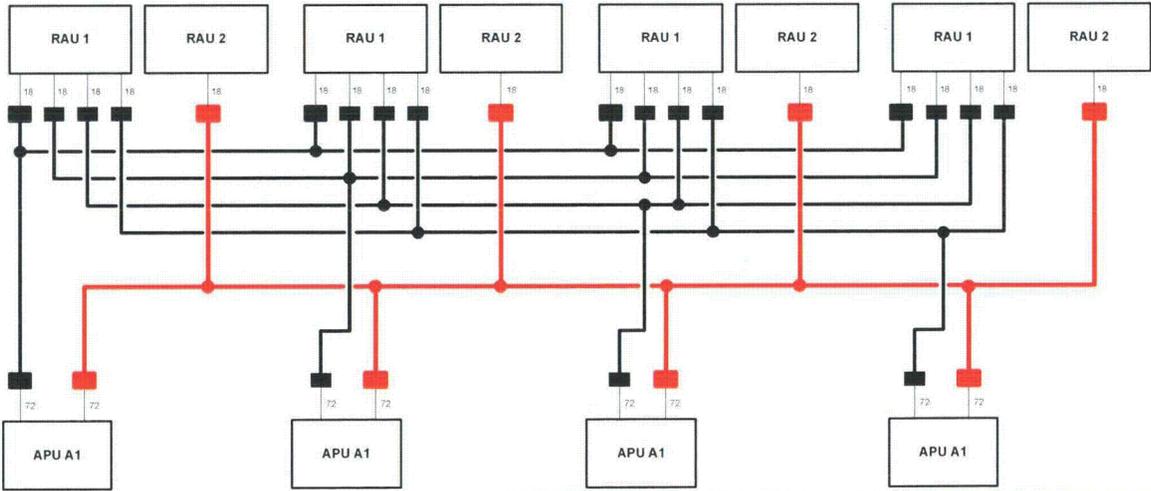
➤ **Single failure: RAU – APU network**

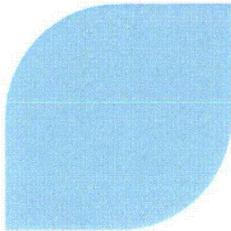
➤ **Mitigation:**

- ◆ **If detected failure: communication flagged faulty, redundant network performs function.**
- ◆ **If undetected (spurious or blocking) failure: bounded by failure of sending RAU.**

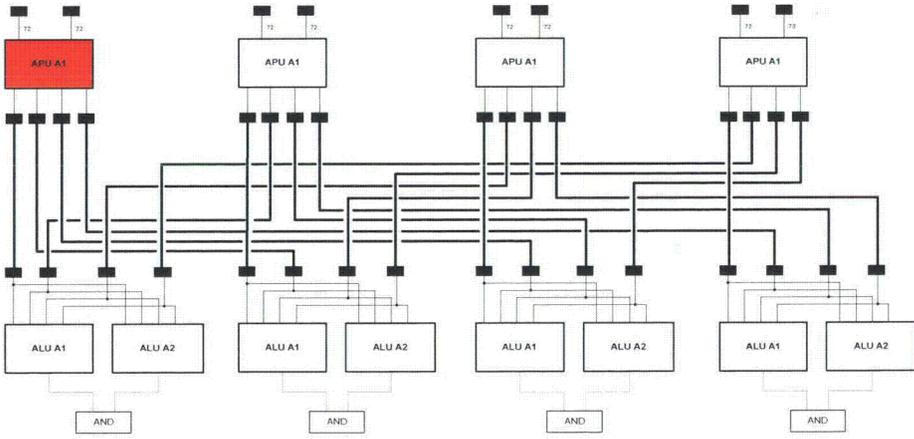
➤ **Independence features:**

- ◆ **Electrically isolated network (fiber optic).**
- ◆ **Physical separation between network cabling (IAW IEEE 384).**
- ◆ **Communication isolation between APU and RAUs.**
 - Previously approved TXS principles for interference free communication.
 - Accommodation of communication failures in RAI 286 Supp. 5 Question 7.09-46.





- **Single failure: APU**
- **Mitigation (same for all PS functions, SPND-based or not):**
 - ◆ **If detected failure: all outputs flagged faulty, downstream vote modified to 2/3.**
 - ◆ **If undetected spurious failure: Downstream vote becomes 1/3.**
 - ◆ **If undetected blocking failure: Downstream vote becomes 2/3.**
- **Independence features:**
 - ◆ **Electrical isolation between APUs.**
 - ◆ **Physical separation between APU divisions.**
 - ◆ **No data communication between APU divisions.**
 - ◆ **Communication isolation APUs and ALUs:**
 - Previously approved TXS principles for interference free communication.
 - Accommodation of communication failures in RAI 286 Supp. 5 Question 7.09-46.



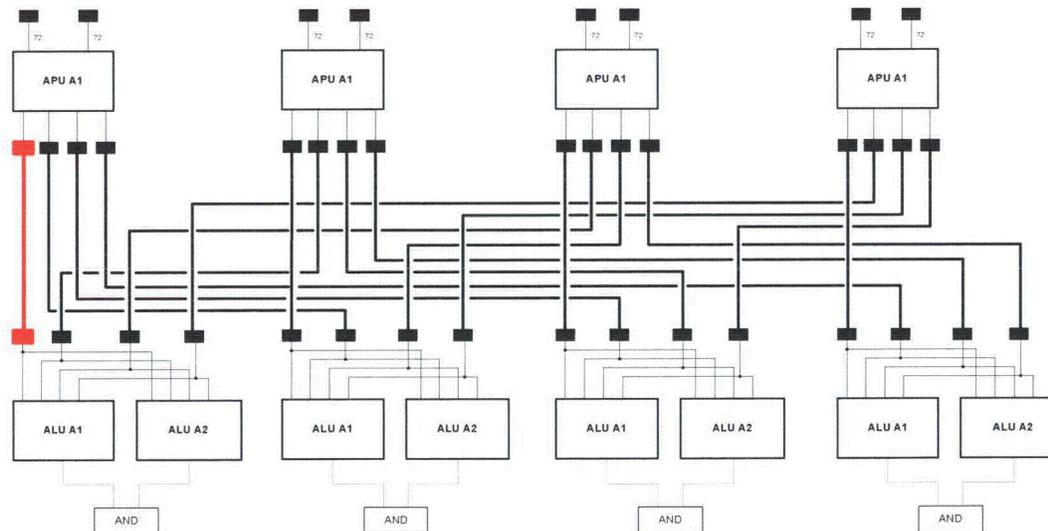
➤ **Single failure: APU – ALU network**

➤ **Mitigation (same for all PS functions, SPND-based or not):**

- ◆ If detected failure: all communication flagged faulty, downstream vote modified to 2/3.
- ◆ If undetected (spurious or blocking) failure: Bounded by sending APU failure.

➤ **Independence features:**

- ◆ Electrical isolation between APU and ALUs (fiber optic).
- ◆ Physical separation between network cabling (IAW IEEE 384).
- ◆ Communication isolation:
 - Previously approved TXS principles for interference free communication.
 - Accommodation of communication failures in RAI 286 Supp. 5 Question 7.09-46.



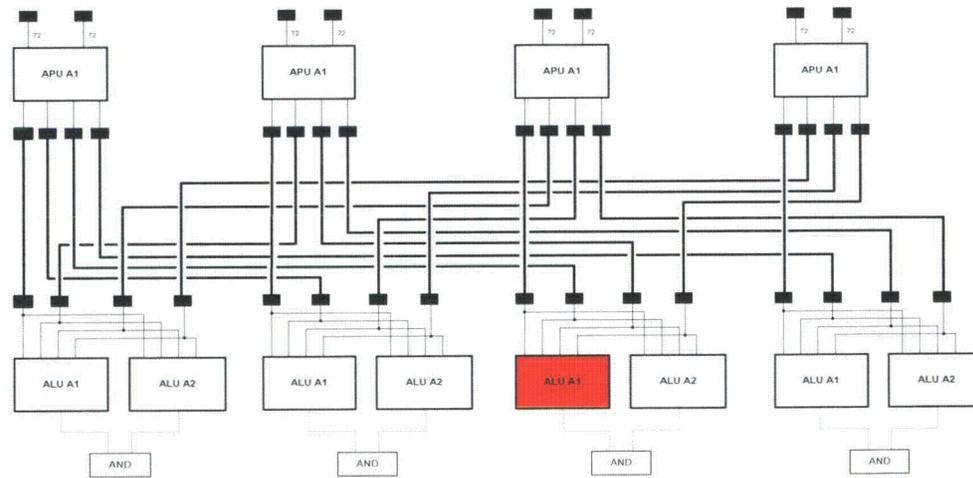
➤ **Single failure: ALU**

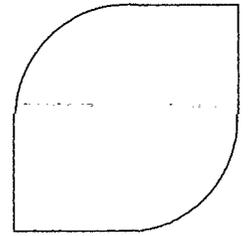
➤ **Mitigation (same for all RT functions, SPND-based or not):**

- ◆ **If detected failure: Fails into state requesting RT. Redundant ALU performs the function.**
- ◆ **If undetected spurious failure: Fails into state requesting RT. Redundant ALU performs the function.**
- ◆ **If undetected blocking failure: Division cannot issue RT. Three redundant divisions perform the function.**

➤ **Independence features:**

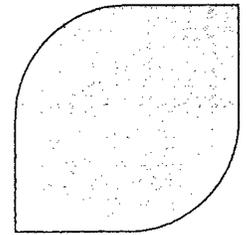
- ◆ **Electrical isolation between ALU divisions.**
- ◆ **Physical separation between ALU divisions.**
- ◆ **No data communication between ALU divisions.**





NRC Concerns Conveyed on June 25, 2010

NRC Concerns Conveyed on June 25, 2010

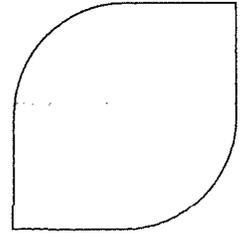


- **Following June 25, 2010 public meeting, AREVA:**
 - ◆ **Evaluated NRC feedback relative to SPND-based functions**
 - ◆ **Re-evaluated the relevant regulatory requirements**
 - ◆ **Re-evaluated the design of the SPND-based functions**
- **These evaluations resulted in the following conclusions:**
 - ◆ **The current design of the SPND-based functions satisfies all regulatory requirements**

- ◆ **NRC feedback included some points that are not well understood or may inaccurately represent the U.S. EPR design**
- ◆ **More detail is needed regarding exactly which aspects of the system are viewed as non-compliant with exactly which regulatory requirements**

By clarifying NRC staff concerns, a better understanding of how to reach closure on this issue can be attained.

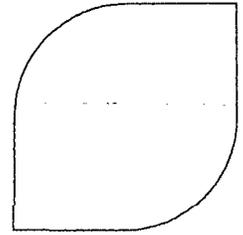
June 25 NRC Feedback



- **“Without independence, failures of one division can affect all safety divisions, and result in loss of the ability to complete the intended safety functions.” (Slide 4)**

- **Consistent with this statement, AREVA NP demonstrates adequate independence by:**
 - ◆ **accounting for accident conditions**
 - ◆ **postulating single failures**
 - ◆ **showing that the redundant portions of the system are protected from the failures (i.e., are independent) and can still perform the safety function.**

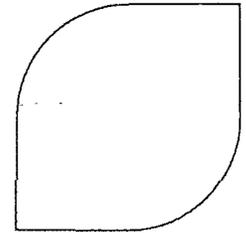
June 25 NRC Feedback – Point 2



- The DNBR and HLPD reactor trip functions “*require information from outside its own division to accomplish the safety function.*” (Slide 6)

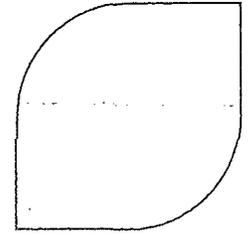
- In the U.S. EPR design, each division requires information from outside the division to perform the DNB and HLPD calculations, but does not require information from outside the division to accomplish its safety function.

June 25 NRC Feedback – Point 2 (cont.)



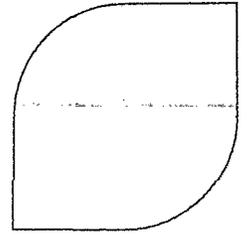
- **The safety function is accomplished without information from outside the division.**
 - ◆ **Each division uses information from outside the division to perform the DNB and HLPD calculations.**
 - ◆ **No single failure outside the division prevents these calculations from being performed.**
 - If incorrect information is received from outside the division due to a single failure, the division also receives correct information from a redundant source.
 - If a loss of information results from single failure outside the division, the division still receives correct information from a redundant source.
 - ◆ **If no information is received from outside the division (multiple failures are required to realize this scenario), the calculations cannot be performed. However, the division reverts to a safe state and the safety function is accomplished.**
 - ◆ **Therefore, each division does not require information from outside the division to accomplish its safety function, which is to trip the reactor.**

Summary



- **I&C implementation of SPND-based RT functions reflects functional requirements that are fundamental to the core design and the plant safety analysis.**
- **I&C implementation of SPND-based RT functions satisfies all regulatory requirements for independence between redundant portions of safety systems.**
- **Compliance with independence requirements is achieved by demonstrating that the safety function can be performed in the presence of postulated accident conditions and any credible single failure.**
- **Critical need: NRC staff to identify any gaps in the AREVA approach to demonstrating compliance to independence regulations.**

Path to Closure



- **AREVA NP will consolidate all I&C information previously submitted on this topic.**
- **NRC audit to inspect consolidated information and detailed analysis documentation, and to determine what information is needed on the docket.**
- **Revision to U.S. EPR Protection System Technical Report to include the necessary information.**