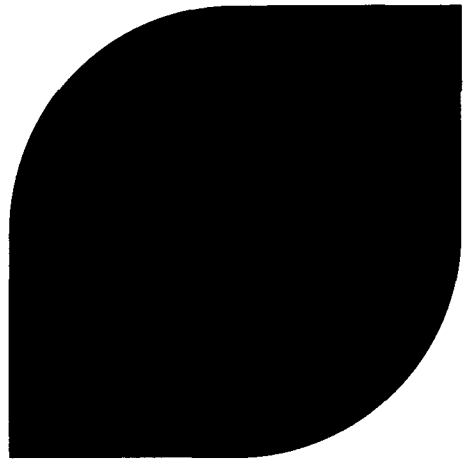

AREVA

August 27,
2010



U.S. EPR Safety Automation System (SAS) Design and Regulatory Compliance Basis

George Pannell
Manager, Product Licensing
Corporate Regulatory Affairs
AREVA, NP
August 31, 2010

EPR™
by AREVA

AREVA

August 27,
2010

Introduction

▶ Meeting Objectives

- ◇ **Explain the U.S. EPR Safety Automation System (SAS) Design Features and Process System Interfaces**
- ◇ **Demonstrate how the U.S. EPR SAS complies with applicable regulations and standards (IEEE 603-1998) including interdivisional communications:**
  - Electrical isolation
  - Physical separation
  - Communications isolation and independence
  - Mitigation of Chapter 15 events with a single failure
- ◇ **Explain Human Factors Considerations in the system design for Improved Operator Interface**

August 27,
2010

Introduction

▶ Topics

- ◇ **Description of SAS functional design and process system interfaces**
- ◇ **SAS interdivisional information sharing design features and the relationship to human factors considerations for improved operator interface**
- ◇ **U.S. EPR, SAS compliance with applicable regulations and standards (IEEE 603-1998) including interdivisional communications:**
  - Electrical isolation
  - Physical separation
  - Communications isolation and independence
  - Mitigation of Chapter 15 events with a single failure

Introduction

▶ Path Forward

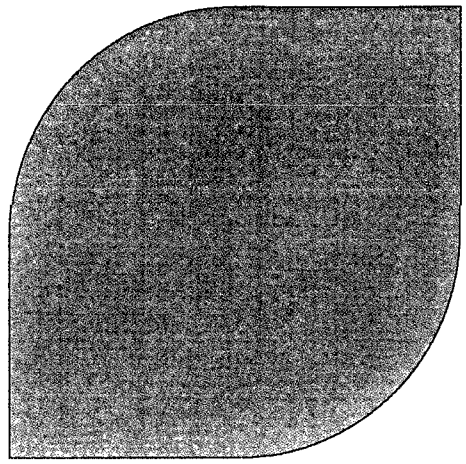
- ◇ **Provide additional technical information needed to support a reasonable assurance determination of the adequacy of the SAS design including interdivisional communication regarding:**
  - Electrical isolation
  - Physical separation
  - Communications isolation and independence
  - Mitigation of Chapter 15 events with a single failure
- ◇ **Support additional interactions as needed to resolve technical issues**

August 27,
2010

Introduction

▶ U.S. EPR Project Goal

- ◇ Obtain NRC Approval of the U.S. EPR, SAS System Design with Interdivisional Communications as Presented on 8/31/2010

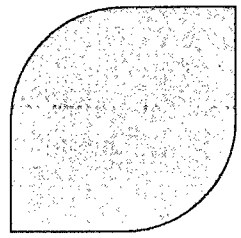


U.S. EPR I&C: Data Communication Between SAS Divisions

Thad Wingo
I&C/HFE Engineer (PLLH-A)
August 30-31, 2010

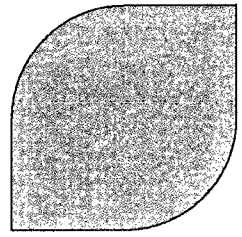
AREVA

Data Communication Between SAS Divisions

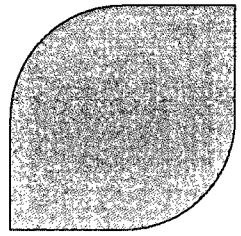


- **At June 25, 2010 public meeting, AREVA NP proposed the following:**
  - ◇ Limit the amount of information shared between SAS divisions.
  - ◇ Perform an evaluation to establish criteria governing what types of information should be shared between SAS divisions. These criteria will be defined in the FSAR.
  - ◇ For each type of information that should be shared, identify critical design features to verify each division is not dependent on the other divisions for performance of safety functions. These critical design features will be defined in Tier 2 with corresponding ITAAC.

Presentation Outline



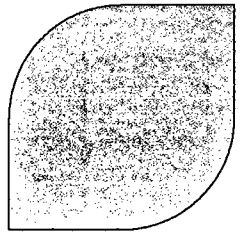
- Design Rationale for Data Communications Between SAS Divisions
- Regulations for independence between redundant portions of safety systems.
- Independence implemented between SAS divisions.



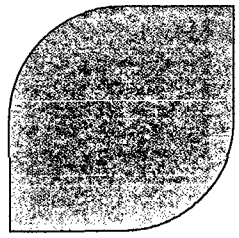
Design Rationale for Data Communications Between SAS Divisions

AREVA

Data Communication Between SAS Divisions

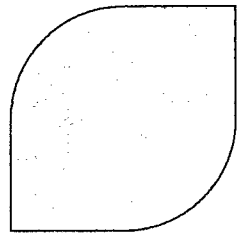


- **There are 3 types of functions in SAS that utilize information from multiple divisions:**
  - ◇ **Automatic Control Functions** – communicate sensor measurements between redundant divisions utilizing 2nd min / 2nd max signal selection.
  - ◇ **Automatic Actuation Functions** – communicate "on/off" binary signals for voting logic and actuation commands between divisions for alignment and interlock functions.
  - ◇ **Human-System Interface Functions** –
    - **Communicate "on/off" binary signals between divisions for manual operator actions that require actuation signals in multiple divisions (e.g., manual grouped commands).**
    - **Communicate sensor measurements between divisions to make redundant information available on a single display.**

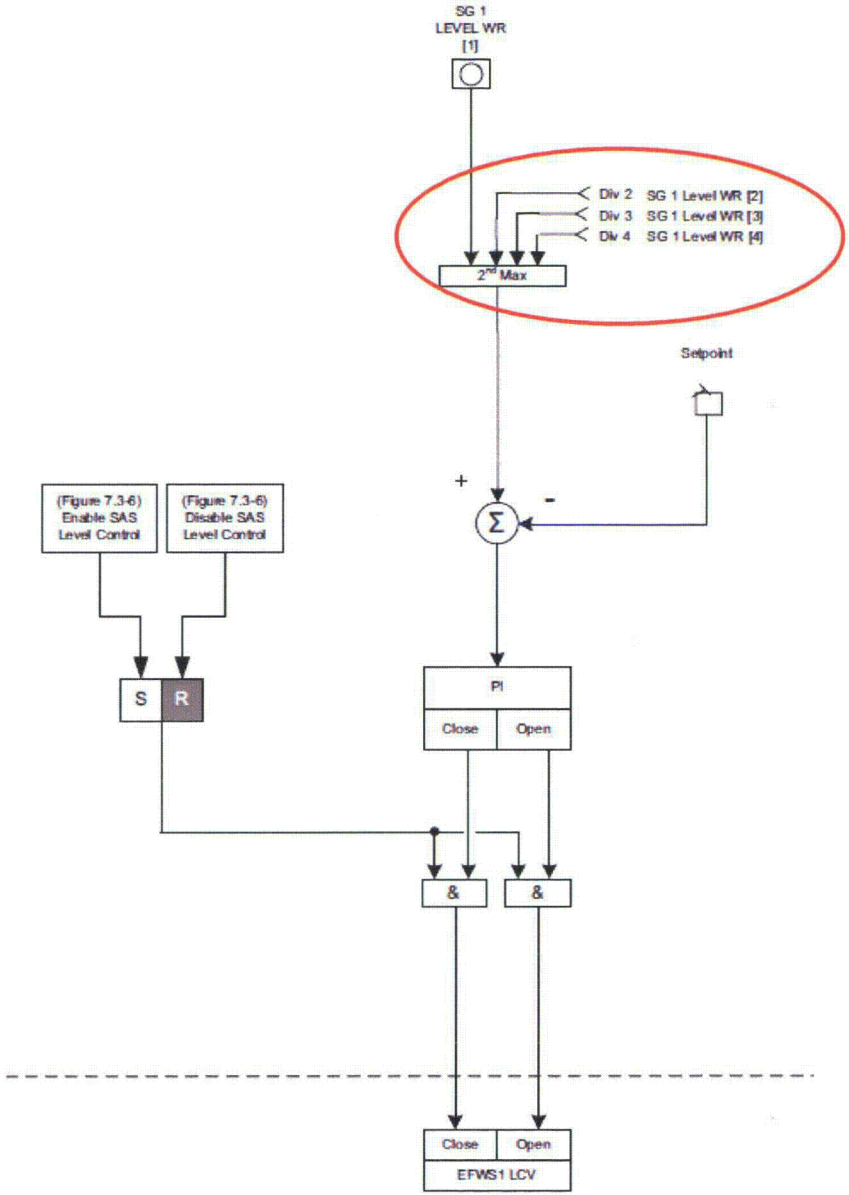


Automatic Control Functions

Data Communication Between Divisions: Automatic Control Functions



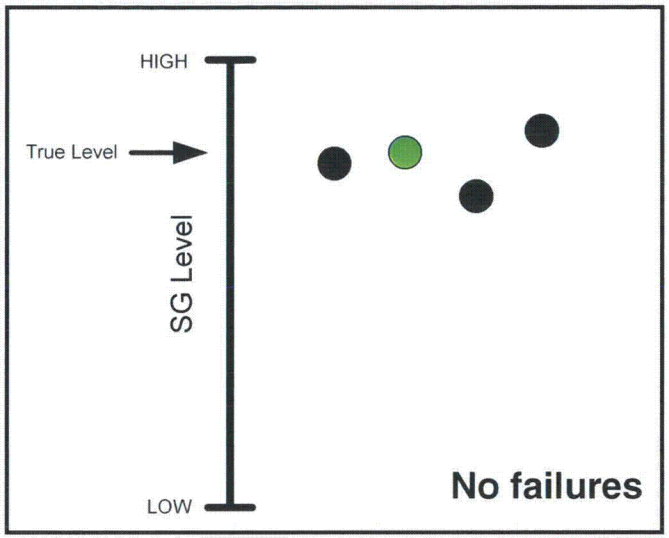
- **Design rationale for having communications between SAS divisions:**
  - ◇ Use of redundant sensor measurements allows safety related control functions to be performed correctly with sensors out of service for maintenance or lost to a failure.
  - ◇ This is a safety enhancement compared to using only one division's sensors to perform the function.
  - ◇ 2nd min / 2nd max signal selection achieves the enhancement while preserving independence. A failure in any one division has no impact on the safety function in any other division.

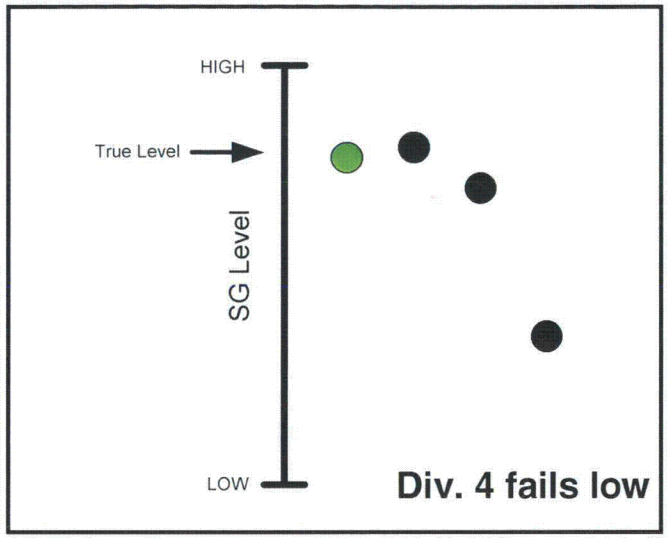


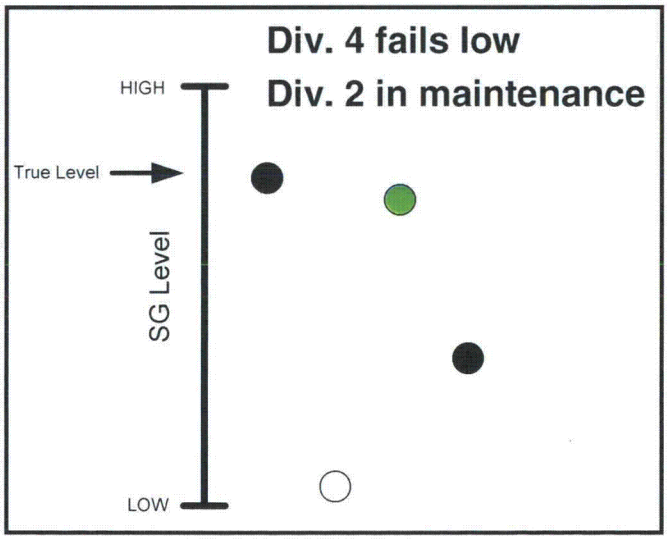
Example of Shared Data Communication Between SAS Divisions for Control

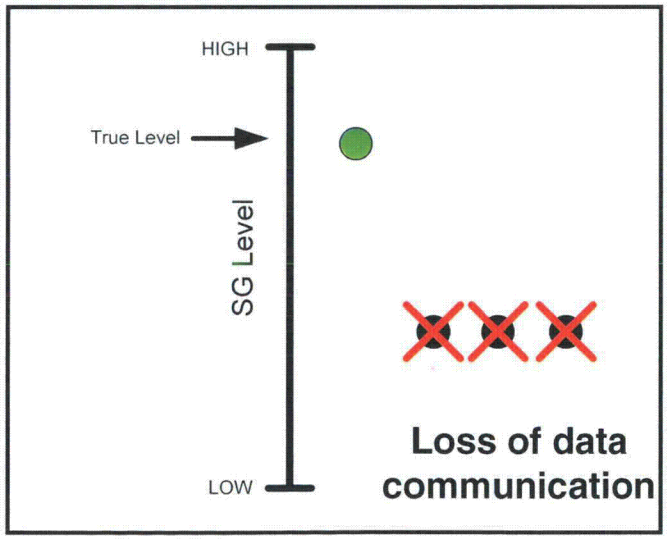
AREVA

2nd max Signal Selection: Examples









- In case of single failures, the control function uses an accurate measurement.
- In case of single failure in one division and maintenance in another, the control function uses an accurate measurement.
- In worst case (loss of data communication), division enters "silo" operation and uses it's own sensor measurement.

Valid sensor measurement

Measurement used in control function

Sensor in maintenance

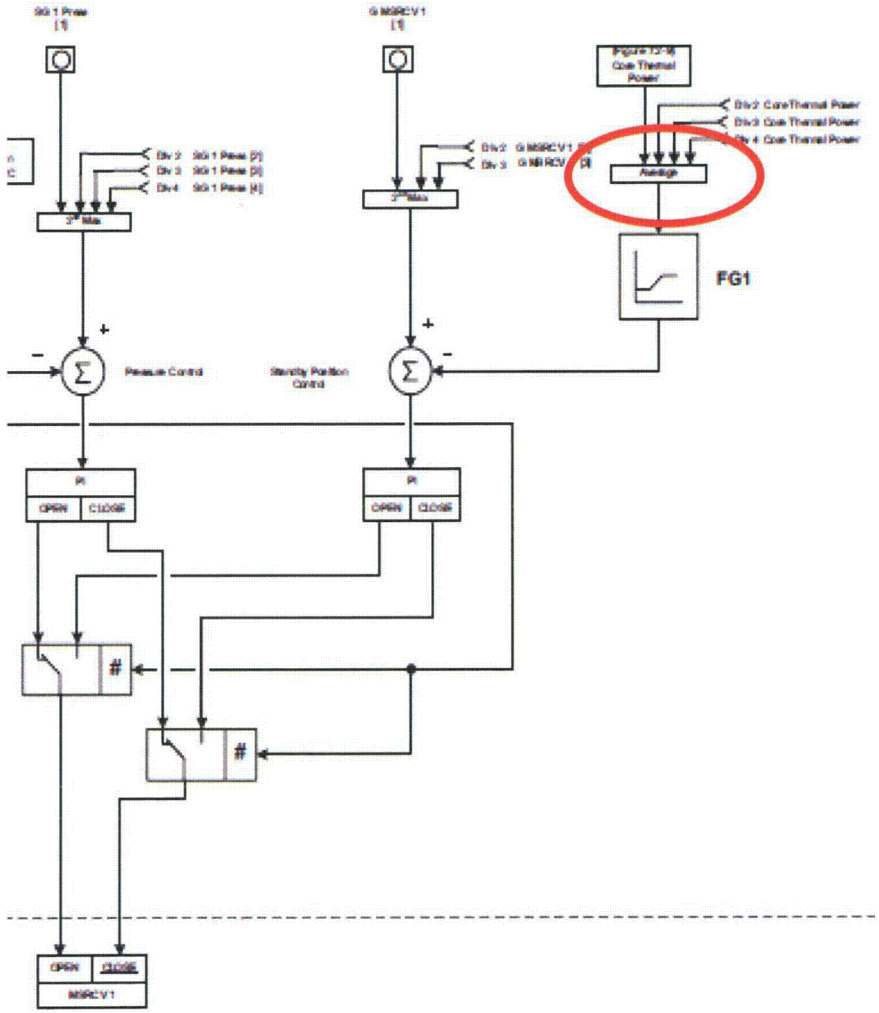
Invalid sensor measurement

AREVA

Specific NRC Concern Regarding Data Communication Between SAS Divisions

- **NRC staff stated during the June 25, 2010 meeting that:**
  - "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:
    - Main Steam Relief Control Valve Control for ESF functions"

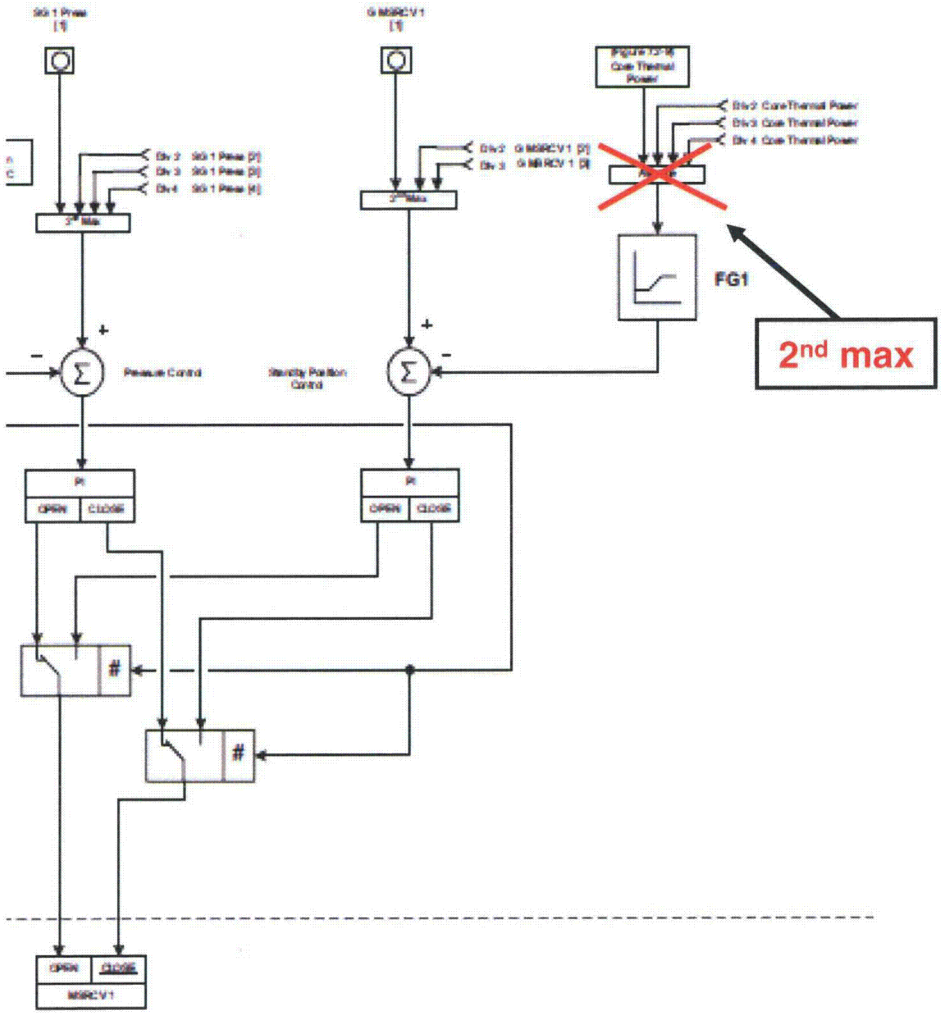
- **AREVA believes that the staff concern was related to the use of the "average" functionality in the MSRCV function.**



AREVA

Specific NRC Concern Regarding Data Communication Between SAS Divisions

- A design change will be made to replace the "average" function with a "2nd max" function.
- This design change makes all SAS automatic control functions consistent.

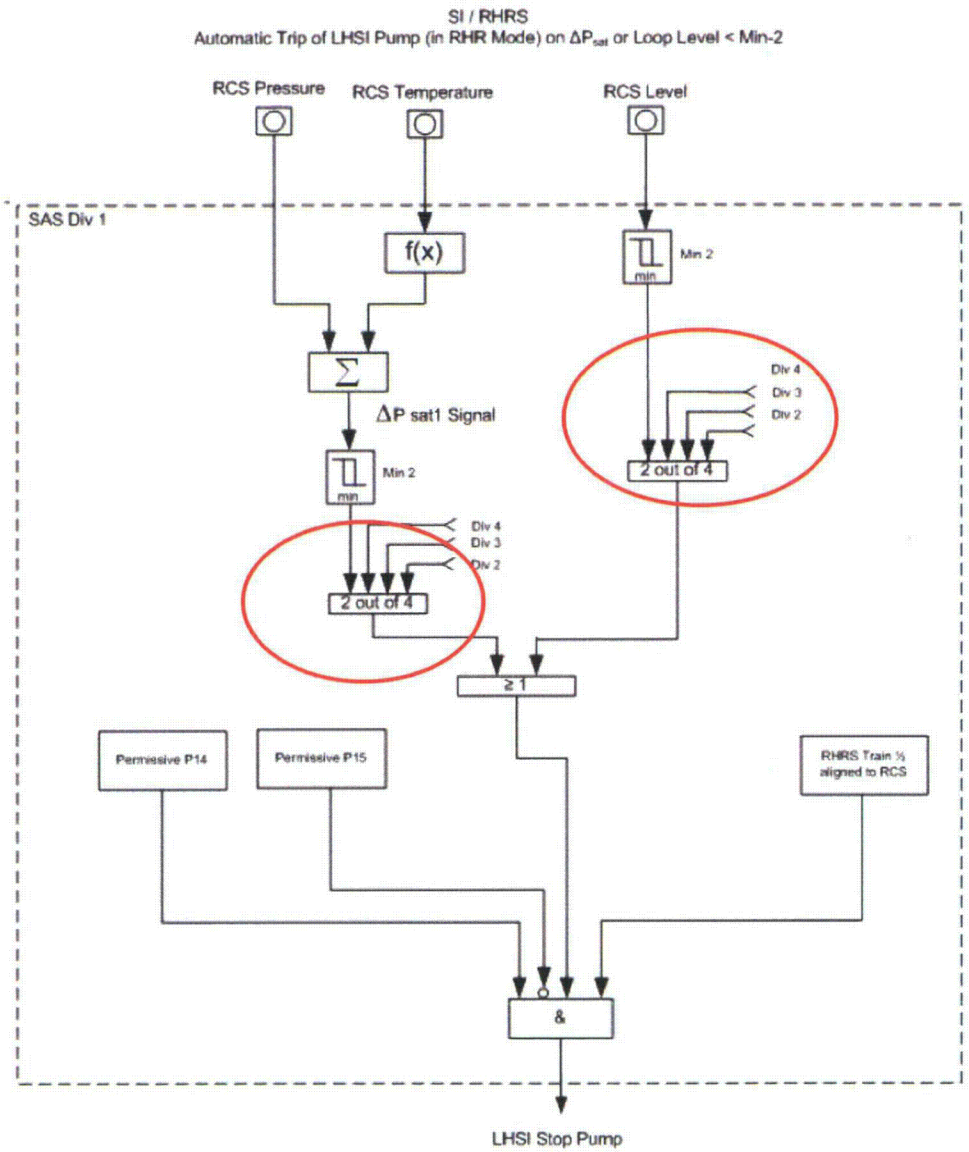


AREVA

Automatic Actuation Functions: 2 Cases
1.) Using voting logic similar to PS
2.) Without voting logic

Data Communication Between Divisions: Automatic Actuation Functions; Case 1

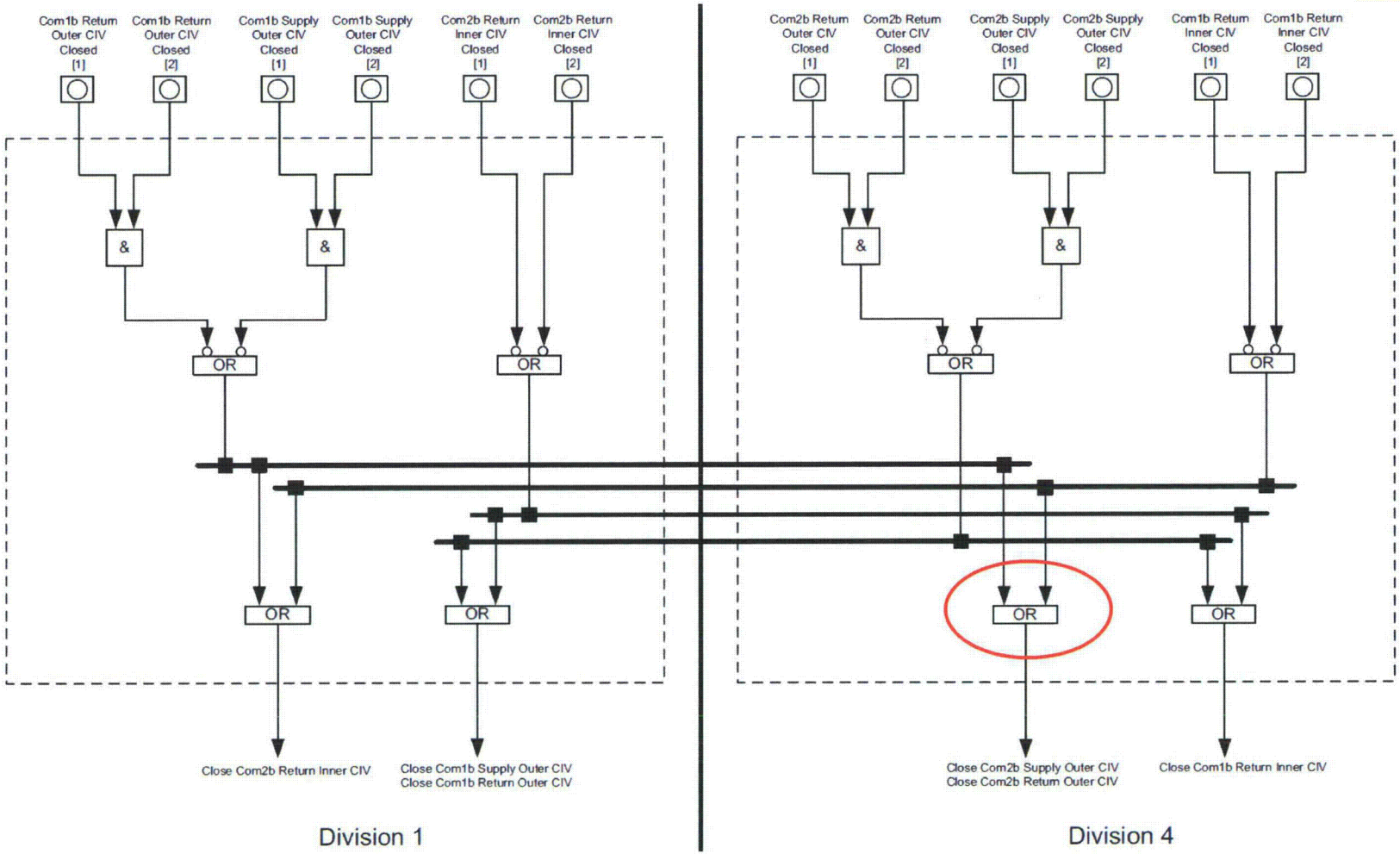
- **Design rationale for having communications between SAS divisions for automatic actuations using voting logic:**
  - ◇ Sharing of redundant setpoint comparison results allows safety related functions to be performed correctly despite a single failure. This is a safety enhancement.
  - ◇ Increase in reliability and availability of the system due to use of voting logic which reduces the probability of spurious actuations and decreases the impact of having a division out for maintenance. This is a safety enhancement.
  - ◇ Voting logic achieves these safety enhancements while preserving independence. A failure in any one division has no impact to the safety function in any other division.
  - ◇ Design rationale for these SAS functions is similar to the rationale for voting logic in the protection system.
  - ◇ NRC has indicated that sharing information via data communication for the purpose of performing voting logic is acceptable.



Example of Data Communication Between SAS Divisions for Automatic Actuation using voting logic

AREVA

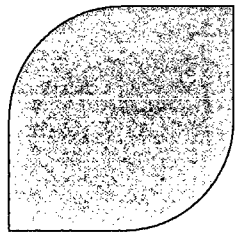
Component Cooling Water Containment Isolation Valve Interlock



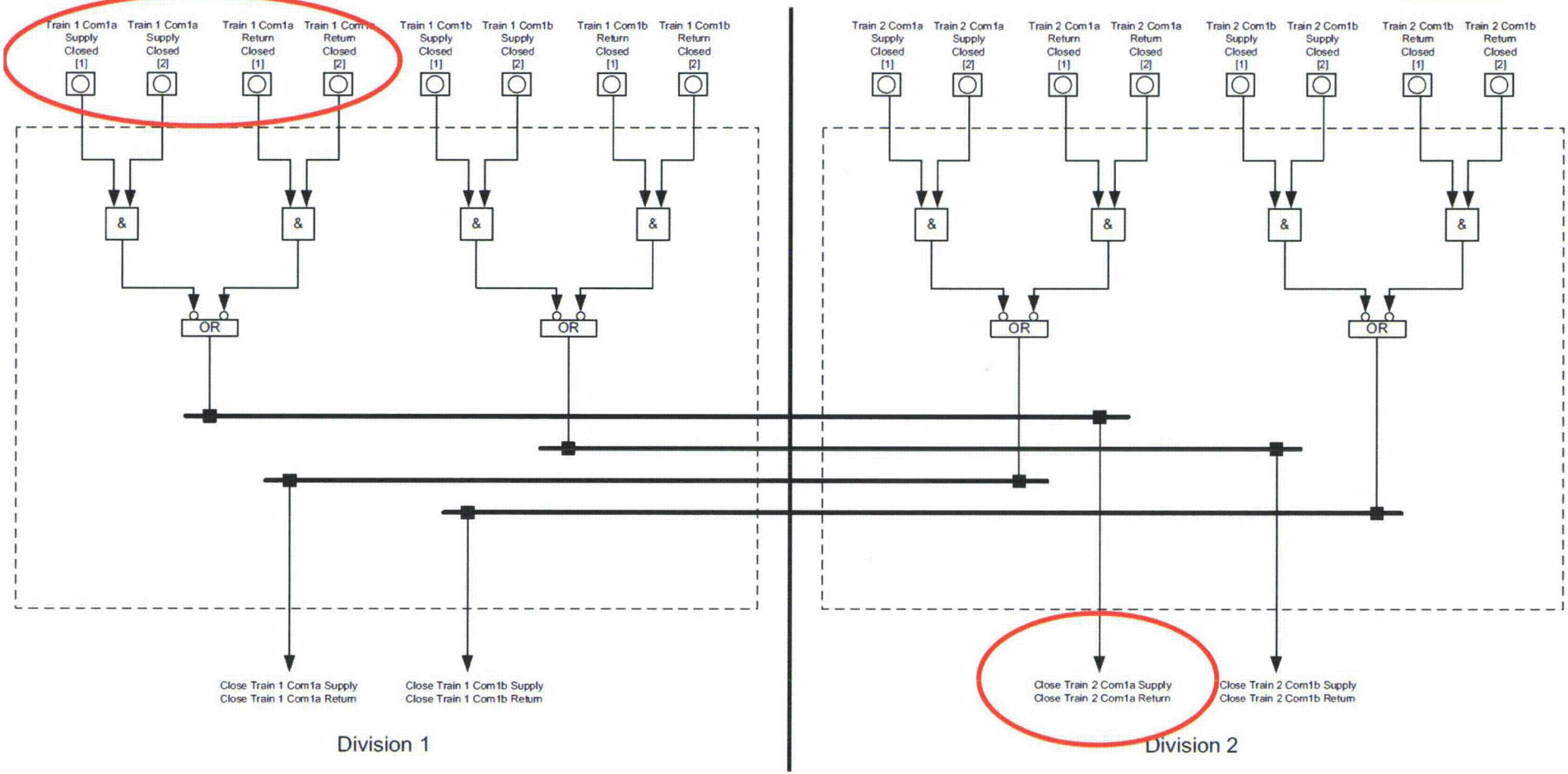
Example of Data Communication Between SAS Divisions for Automatic Actuation using voting logic

AREVA

Data Communication Between Divisions: Automatic Actuation Functions; Case 2



- **Design rationale for having communications between SAS divisions for Automatic Actuations without voting logic:**
  - ◇ Sharing of actuation commands between divisions is needed when one division's sensors are used to affect another division's actuator.
  - ◇ This type of data communication supports the required safety function by maintaining safety related electrical division alignment. An actuator powered by a certain electrical division must receive its actuation signal from I&C powered from the same division.
  - ◇ Communication isolation is achieved by the standard TXS techniques for interference free communication.
  - ◇ Single failure analysis demonstrates that no single failure results in failure to perform the safety function.



Component Cooling Water Switchover Valve Interlock

AREVA

Human-System Interface Functions

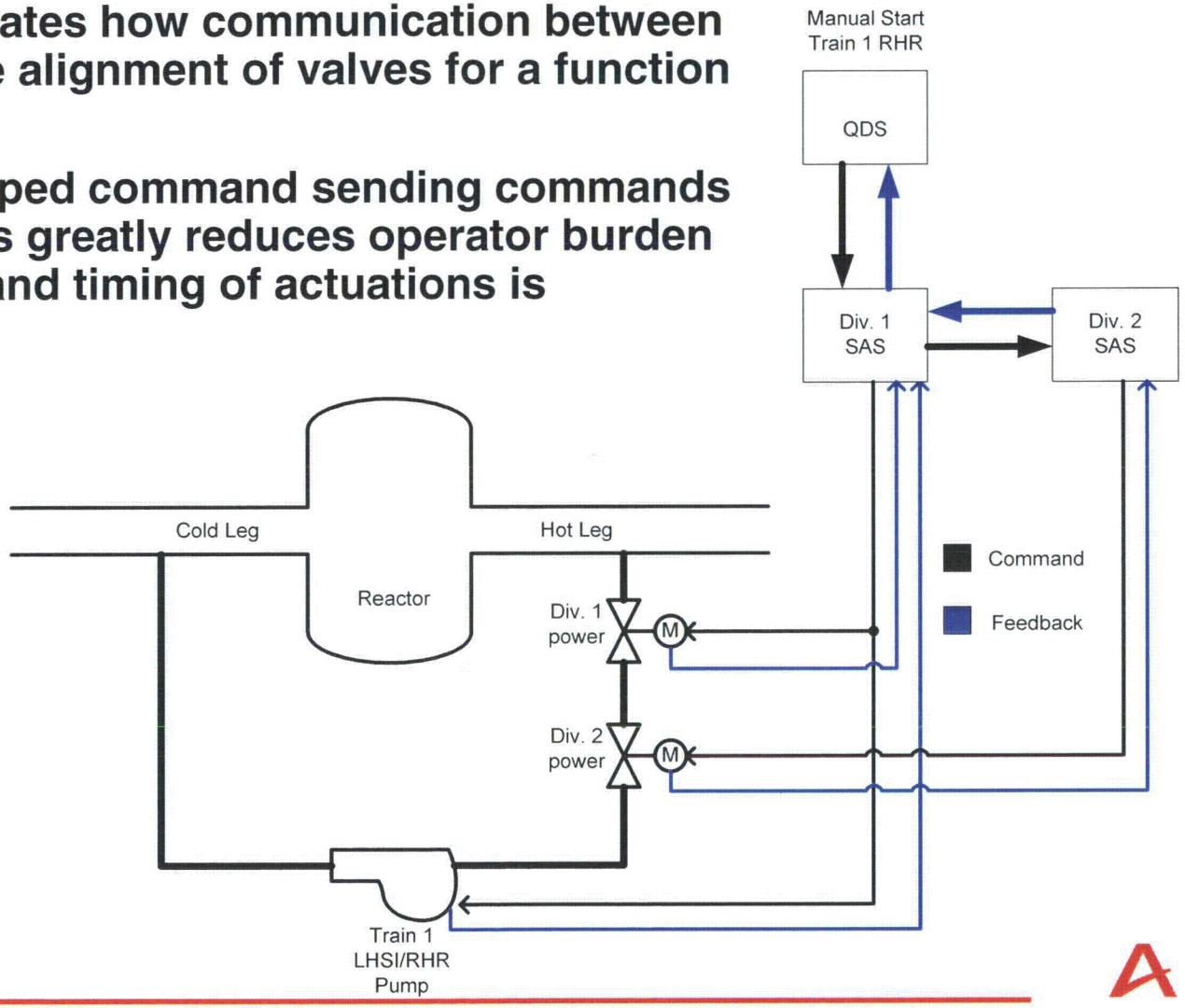
AREVA

Data Communication Between Divisions: Human-System Interface Functions

- **The ability to consolidate data from multiple divisions is vital to leveraging the advantages of a digital control room for human factors considerations.**
  - In general, manual grouped commands, four division parameter comparisons, and consolidated monitoring and control functions improve situational awareness and minimize the secondary tasks required by operators.
- **Functional requirements analysis, operating experience reviews, and human reliability analysis will be considered during the initial allocation of functions to manual grouped commands, automation or individual component commands.**
- **These functions decrease operator workload when using the safety related HSI, which reduce the chance for human error, thereby enhancing safety.**

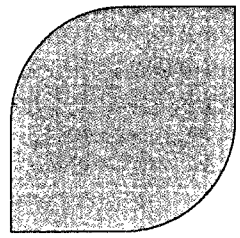
Data Communication Between Divisions: Human-System Interface Functions

- This example illustrates how communication between divisions to achieve alignment of valves for a function could be designed.
- The use of the grouped command sending commands to multiple divisions greatly reduces operator burden and assures order and timing of actuations is maintained.



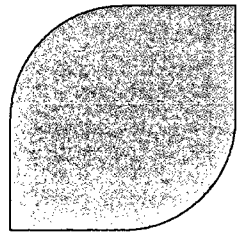
AREVA

Data Communication Between Divisions: Human-System Interface Functions



- The manual command signal is sent from SICS Division 1 to SAS Division 1 which then sends a command signal to Division 2 to align the suction valves.
- The command signal that is sent to SAS Division 2 in the previous slide uses the same communication techniques as all TXS communications between safety divisions.
- Feedback signals are then sent back to the Division 1 SICS (via both Div. 1 and Div. 2 SAS) so that all of the process parameters necessary to confirm the completion of the action are available in one location.

Data Communication Between Divisions: Safety-related Human-System Interface Functions (cont.)



- **The need for multi-divisional grouped commands or multi-divisional displays is validated by task analysis that identifies cases where the operator may experience (e.g.):**
  - ◇ Task complexity
  - ◇ Multiple events causing high workload
  - ◇ Ambiguous data
  - ◇ Data necessary to make decisions that is too physically separated
  - ◇ Difficulty comparing or contrasting data
  - ◇ Task timeline constraints

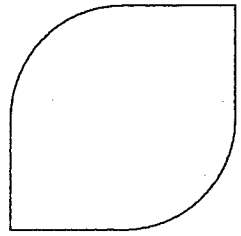
Data Communication Between Divisions: Human-System Interface Functions (cont.)

- The capability to share data between divisions and send commands to multiple divisions, when justified via task analysis, allows the HSI designer to create task or function based displays that mitigate the challenges to the operator.

- Using data communication between SAS divisions for this purpose enhances safety by improving operator performance.

The HFE program analyses provide the criteria governing use of data communications between divisions for HSI purposes. The results of these analyses identify the specific functions that will be implemented in this manner.

Data Communication Between Divisions: Human-System Interface Functions (cont.)



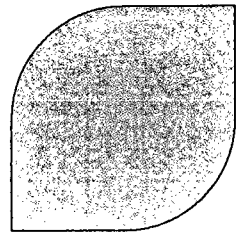
- Design rationale is consistent with:
  - IEEE 603 Clause 5.14 and 10CFR50.34 (f) both require human factors be considered in the design of the safety systems.
  - The AREVA NP Human Factors Engineering Program, including analyses and design process, which is described in Chapter 18 of the FSAR.
  - The desire to mitigate risk-significant human actions identified by the HRA which focuses on designing to minimize the opportunity for human error (e.g. SI switchover during SGTR event which is identified as a risk significant human action in the PRA).

Regulations for independence between SAS divisions

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 5.14 "Human Factors "**
  - ◇ Human factors shall be considered at the initial stages and throughout the design process to assure that the functions allocated in whole or in part to the human operator(s) and maintainer(s) can be successfully accomplished to meet the safety system design goals, in accordance with IEEE Std 1023- 1988.

Compliance with IEEE 603-1998 Clause 5.6.1 – Data Communication Between SAS Divisions

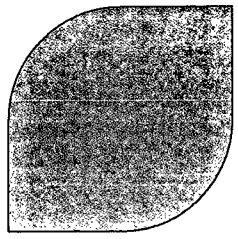


IEEE 603-1998, Clause 5.6.1 (via 10 CFR 50.55a(h))

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 SAS 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 – Data Communication Between SAS Divisions (Cont.)



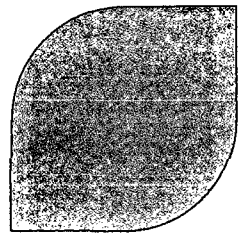
◇ **IEEE 603-1998 Clause 5.6.1 is satisfied if the safety function can be performed in the presence of postulated accident conditions and any credible single failure.**

◇ **Approach to demonstrate compliance:**

- Account for, or disposition, postulated accident conditions.
- Postulate a credible single failure anywhere in the SAS.
- Identify system design features that assure the failure does not prevent performance of the safety function by redundant means (e.g., physical separation, electrical isolation, communication isolation).

◇ **U.S. EPR FSAR Tier 1, Section 2.4.4 contains ITAAC for detailed single failure analysis of SAS.**

FSAR Implementation of IEEE 603, Clause 5.6.1 for SAS



- **Requirement:**
  - **The safety function can be performed in the presence of postulated accident conditions and any credible single failure**
- **Critical design characteristics:**

Capture in Tier 2

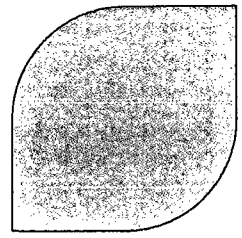
  - Loss of communication between redundant divisions, due to single failure, does not prevent performance of the safety function.
  - Communication error resulting in incorrect information from any one division, due to single failure, does not prevent the performance of the safety function.
  - Loss of a sensor in one division does not prevent performance of the safety function.

- **Information inspected to verify critical design characteristics:**

Capture in Tier 1

  - Communication software code that is associated with receipt of data from another division.
  - Communication software code that is associated with signal selection and voting functions.
  - Communication network diagrams and component design.

Compliance with IEEE 603-1998 Clause 5.14 – Data Communication Between SAS Divisions (Cont.)

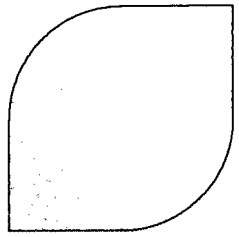


IEEE 603-1998, Clause 5.14 (via 10 CFR 50.55a(h))

Human factors shall be considered at the initial stages and throughout the design process to assure that the functions allocated in whole or in part to the human operator(s) and maintainer(s) can be successfully accomplished to meet the safety system design goals, in accordance with IEEE Std 1023- 1988.

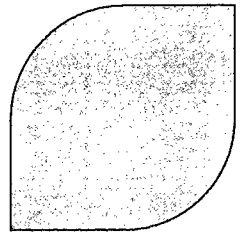
- **U.S. EPR FSAR Tier 2, Chapter 18 and Tier 1, Section 3.4 demonstrate compliance to IEEE 603-1998 Clause 5.14**
- **The following program commitments were considered in meeting the regulations:**
  - ◇ **IEEE 603-1998 Clause 5.14 is satisfied if the design of the safety system HSI follows a human factors program that meets the criteria in IEEE 1023. The AREVA NP human factors program conforms to IEEE 1023 by applying the criteria in NUREG 0711 as directed by the SRP.**
  - ◇ **Tier 2, Chapter 18 of the U.S. FSAR and the associated implementation plans provide the program necessary to show compliance.**
  - ◇ **ITAAC in Tier 1, Chapter 3.4 contain the commitments to provide the staff the necessary acceptance criteria for closure**

Summary



- There are clear design rationale for using data communication between SAS divisions to enhance plant safety.
  - ◇ The inventory of automatic control functions that share redundant sensor measurements between divisions enhance performance of the safety functions.
  - ◇ The inventory of automatic actuation functions that share binary signals between divisions enhance performance of the safety functions or support mechanical and electrical system divisional alignment.
  - ◇ The inventory of functions using data communications between divisions for HSI purposes will be determined by application of the HFE program.
- Communication isolation between SAS divisions is achieved by the previously approved TXS communication techniques for interference free communication.
- Independence between SAS divisions is demonstrated through single failure analysis, taking into account accident conditions.

Path to Closure



- **Revision to Tier 2, Chapter 7**
  - ◇ **Include design rationale for communication between SAS divisions in Tier 2.**
  - ◇ **Include critical design features in Tier 2.**
- **Revision to Tier 1, Section 2.4.4**
  - ◇ **Include information to be inspected to verify critical design features in Tier 1.**