Multi-Channel Non-Safety VDUs

HICRc Task Work Group Meeting

March 29, 2007

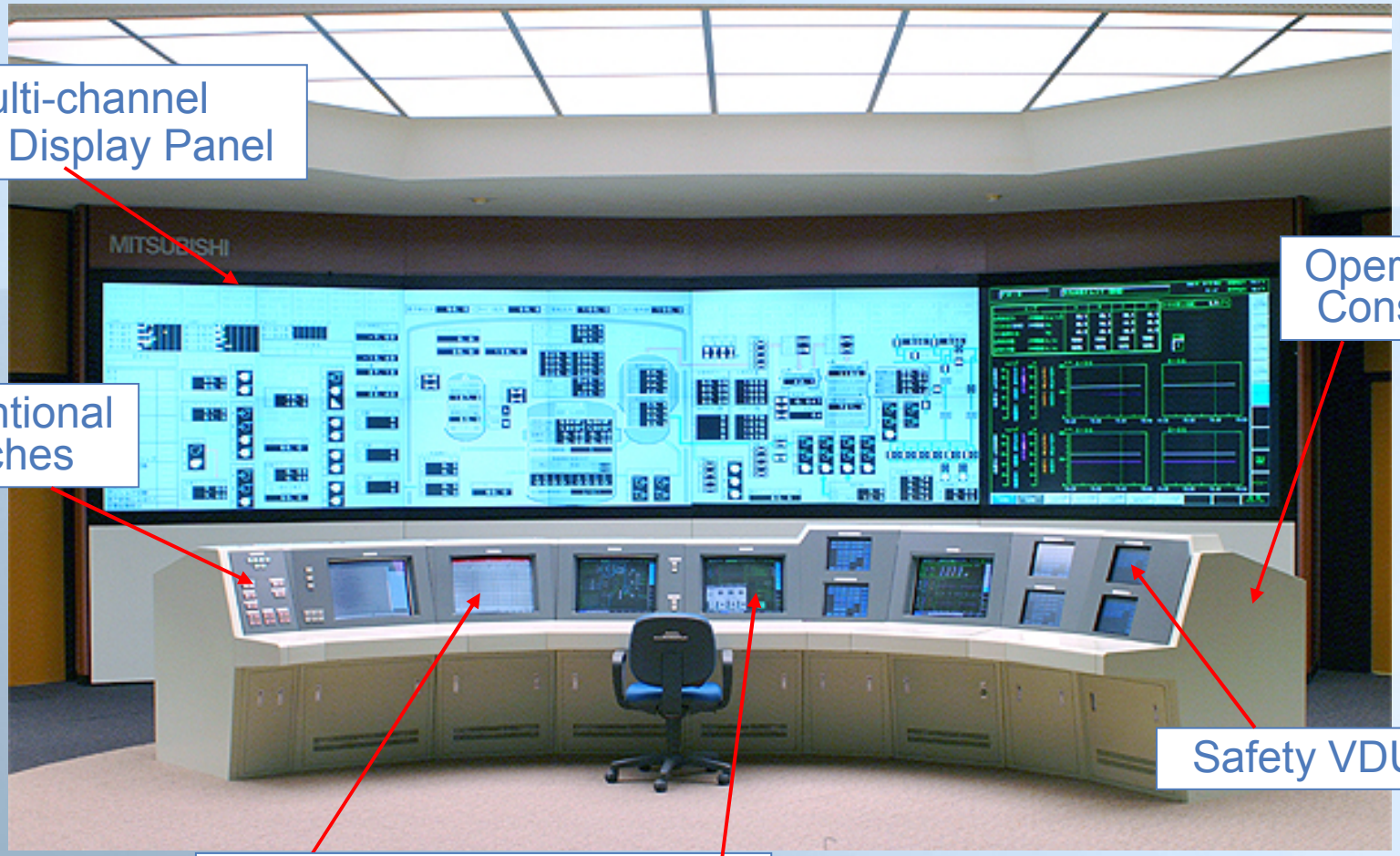
NEI

NUCLEAR
ENERGY
INSTITUTE

Objectives for Meeting

- Reach a common understanding regarding the purpose, benefits and implementation concepts for multi-channel non-safety VDUs, to facilitate better TWG communication during the development of related guidance.
- Reach agreement on the license-ability of high level implementation concepts that will form the basis of future guidance.

Example Advanced MCR



Multi-channel Large Display Panel

Operator Console

Conventional Switches

Safety VDUs

Multi-channel VDUs

HSI Design Basis

- For all plant conditions, including DBA and safe shutdown, the primary operator interface is provided by
  - Non-safety Multi-channel LDP*
    - SDCV information and alarms significant to safety and power production
  - Non-Safety Multi-channel VDUs*
    - Selectable interface for all other information, alarms and controls
  - Conventional Class 1E switches
    - SDCV controls for system level actuation of safety functions
- Safety VDUs provide required Class 1E information and control for all safety functions

* Design for post seismic use is vendor dependent
LDP – Large Display Panel
SDCV – spatially dedicated, continuously visible

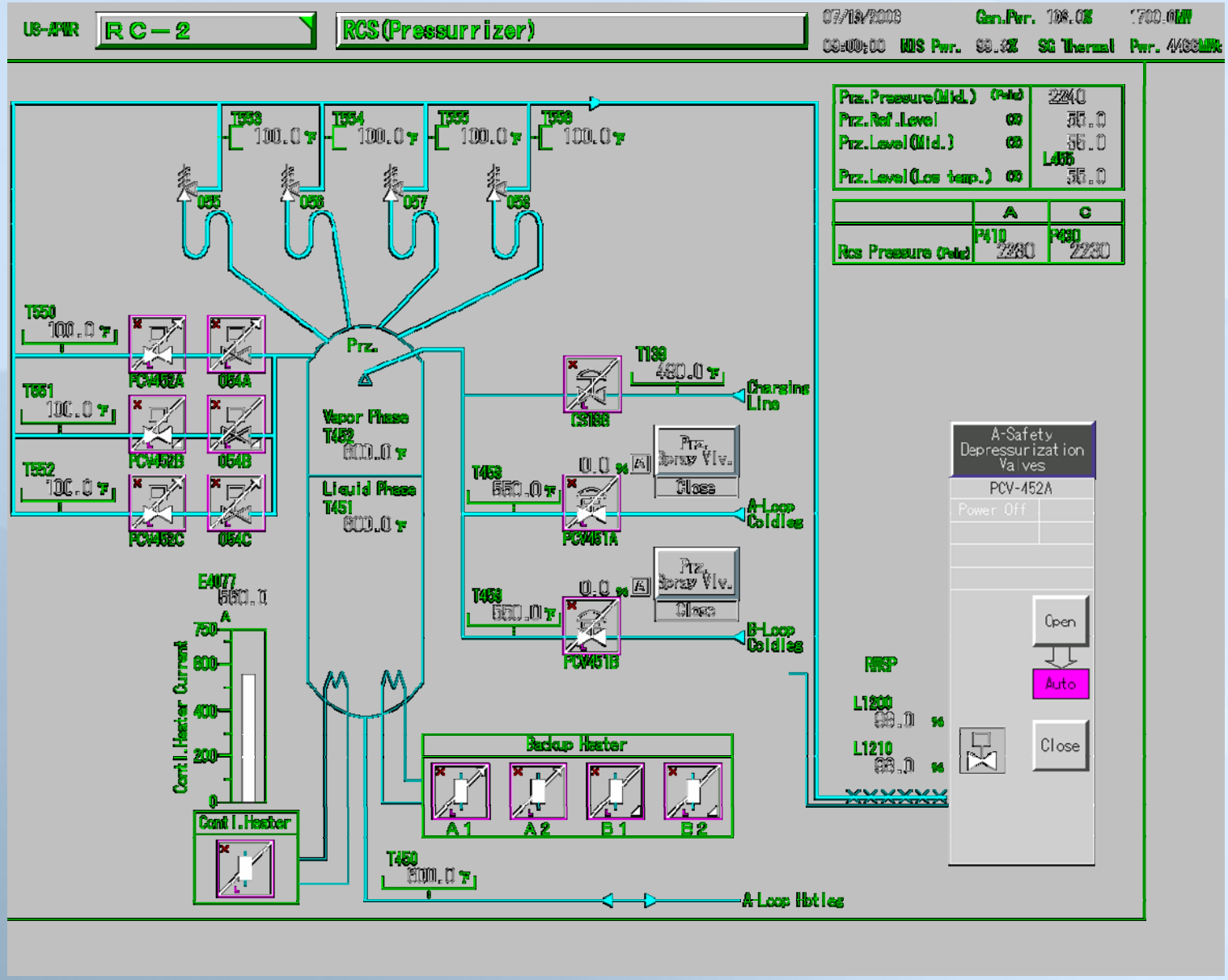
Multi-channel HSI Background

- Safety functions are monitored by multiple non-safety and safety instrumentation
  - e.g., narrow range - wide range, incores – excores
- Multiple safety and non-safety success paths exist for all critical safety functions
  - e.g., Charging - Safety Injection, Main Feed – Aux Feed, Sprays - Reliefs

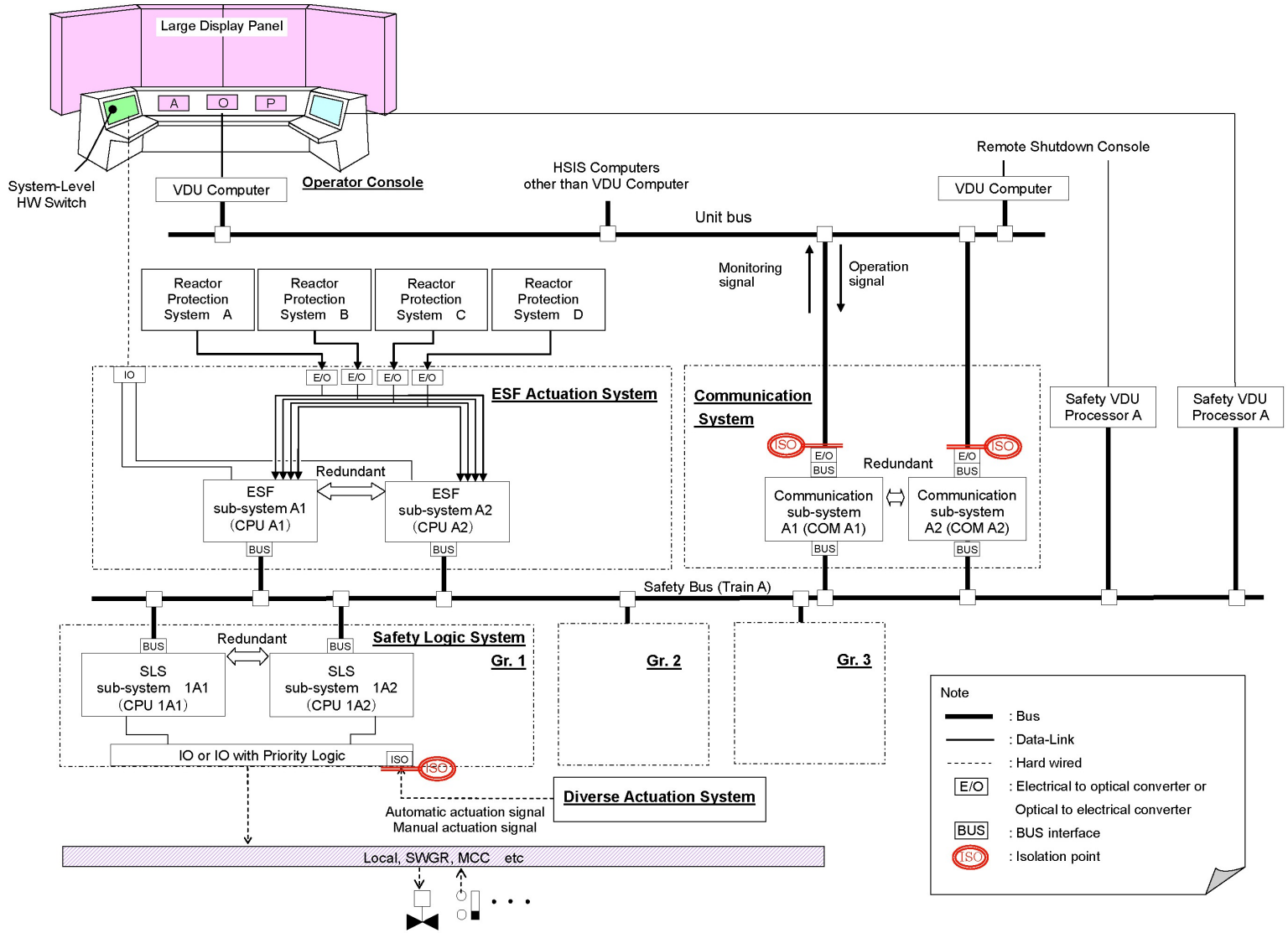
Multi-channel HSI Benefits

- Integrated safety and non-safety monitoring and control on the Multi-channel LDP and VDUs provide the following benefits
  - Continuous awareness of critical safety functions while immediate focus may be plant maneuvering and power production.
  - A single operator can execute procedures that historically involve multiple operators to coordinate multiple safety divisions and non-safety systems. This simplifies task coordination for maintaining critical safety functions.
  - Operators can execute computer based procedures with integrated information and manual controls (eg. embedded or via hyperlinks).
  - Minimizes operator transitions between safety and non-safety VDUs, thereby reducing operator workload during critical plant situations.
- Benefits reduce operator task burden, reduce potential for human error

Example Multi-Channel VDU Screen



Example System Architecture

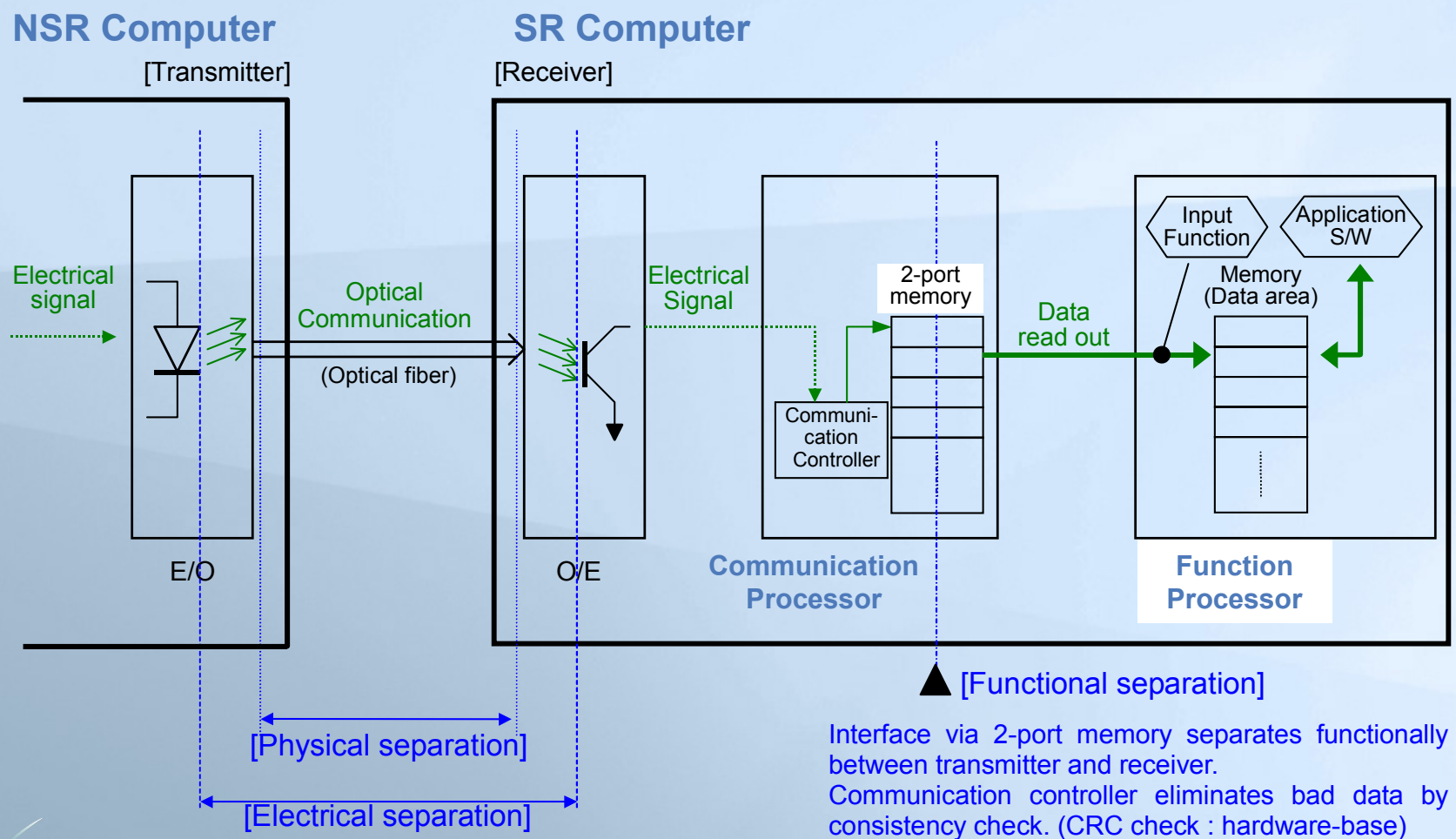


Configuration of Engineered Safety Features Actuation System and Safety Logic System

SR-NSR
Communication Interface

- Electrical independence
  - Fiber Optics
- Communication independence
  - Separate function and communication processors with no handshaking ensures deterministic asynchronous processing of safety logic functions
- Only predefined data can be transferred
  - No file transfer capability in safety system
  - Predefined communication data sets reject unknown data
- No ability to alter safety software through NSR communication interface except during maintenance bypass or out of service conditions
- Additional protection against cyber threats
  - Administrative controls per NEI 04-04 for safety & non-safety systems
  - Two-way communication only with NEI 04-04 controlled systems

Example Communication Buffer



Interface via 2-port memory separates functionally between transmitter and receiver.
Communication controller eliminates bad data by consistency check. (CRC check : hardware-base)

SR-NSR
Functional Independence

- To ensure no adverse safety function interaction, logic <u>in safety function processor</u> prioritizes SR over NSR signals
  - Examples of functions available from NSR VDU
    - NSR can initiate operating bypasses
      - Only after permissive setpoint is reached
      - Bypass is automatically removed if permissive clears
    - NSR can change safety component position
      - Before ESF actuation or after ESF actuation signal clears
      - NSR cannot block ESF system level actuation
    - NSR can reset ESF system level actuation latch
      - Only after clear setpoint is reached

NEI

SR-NSR
Functional Independence

- Other functions from NSR VDU being considered
  - NSR can initiate channel maintenance bypasses
    - Interlocks prevent multiple bypasses of like channels
  - NSR can override completed ESF system level actuation
    - Only at component level
    - Only with two distinct and deliberate manual control actions
    - SR logic must receive and process each distinct signal

NEI

Maintenance Bypass

- Failure Considerations
  - Assumptions
    - Four channel protection system with 2/4 logic
    - One channel already in bypass
    - Plant AOO or DBA requiring protective action
    - Failure in NSR VDU or erroneous operator action causes spurious bypass command
  - Additional Failure Examples
    1. No additional failures
       - Safety interlock prevents additional bypass leaving 3 functional safety channels
    2. Additional single failure of interlock in one safety channel
       - Failure of interlock results in 2 channels bypassed, leaving 2 functional safety channels
    3. Additional single failure of one safety channel
       - Safety interlock prevents additional bypass, leaving 2 functional safety channels

NEI

ESF Component Override

- Failure Considerations
  - Assumptions
    - Plant AOO or DBA requiring protective action
    - N+1 trains
    - Protective action completed in all trains
    - Failure in NSR VDU or erroneous operator action causes spurious override command
  - Additional Failure Examples
    1. No additional failures
       - No component repositioning occurs because safety logic is waiting for second signal to satisfy 2-signal interlock. N+1 trains remain functional.
    2. Additional single failure of one train
       - No component repositioning occurs because safety logic is waiting for second signal to satisfy 2-signal interlock. N trains remain functional.
    3. Additional single failure of 2-signal interlock logic in one train
       - Component in one train erroneously repositions. N trains remain functional.

NEI

NSR
Failure Consideration

- It is not practical to develop safety system interlock logic for all NSR signals
  - Interlocks may preclude operator judgment
    - e.g., relief valve open demand
  - Interlocks may require complex logic and inter-channel communication
    - e.g., accumulator valve close demand
- Credible failures must be considered that may result in erroneous generation of these control command signals

Credible NSR Failures

- Continuous generation of a single spurious control command is credible
  - Affects a single safety or non-safety component, which is bounded by the safety analysis
  - Can be blocked by disabling NSR from Safety VDU
- A failure resulting in multiple spurious control commands is not credible, based on key design features
  - Control commands are generated by a series of multiple software blocks which generate various components of the communication message
    - e.g., Source tag, component tag, command, prefix, suffix, CRC
  - Spurious actuation would require multiple software block failures that each produce intelligent meaningful data

Multi-Channel VDU Quality

- Not Class 1E
- Elevated important to safety software quality for safety relevant functions, including computer based procedures
  - e.g., appropriate SIL in IEEE1012
- Tested to seismic qualification levels to demonstrate functionality for OBE and SSE* (vendor dependent)

*Operating basis earthquake, Safe shutdown earthquake

HFE Considerations

- HFE program confirms plant safety during degraded HSI conditions
  - e.g., minimum staffing, loss of all non-safety HSI, use of only Safety HSI
  - Accident mitigation
  - Safe shutdown
  - Short term continued stable operation (vendor dependent)

Summary

- Non-safety Multi-channel VDUs offer significant operational benefits
  - Reduced operator task burden
  - Reduced potential for human error
- These benefits can be achieved without degrading the reliability of the SR functions.