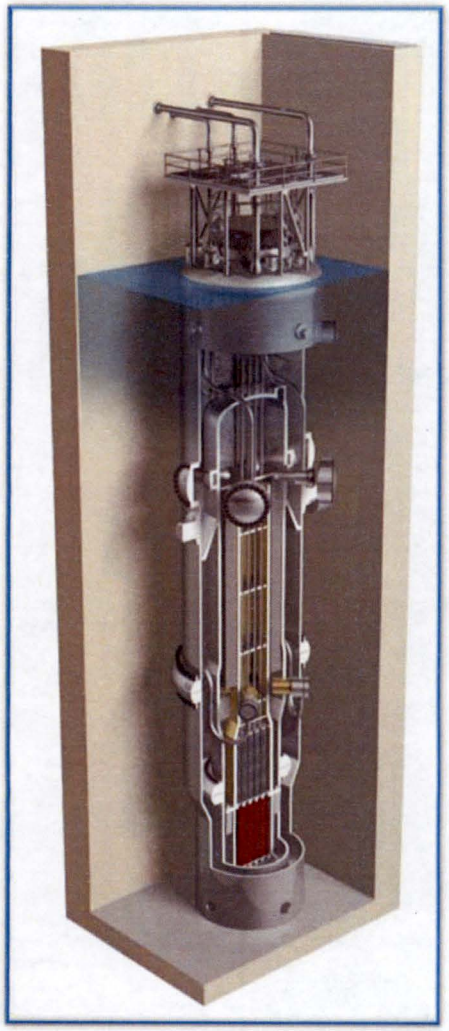


ACRS Presentation: NuScale Instrumentation and Controls Design Overview

Brian Arnholt
Supervisor, I&C Engineering
Rufino Ayala
I&C Engineer
Paul Infanger
Licensing Project Manager

August 23, 2018

PM-0618-60212
Revision: 0

NUSCALE™
Power for all humankind

Template #: 0000-21727-F01 R4

Purpose

- Provide an overview of the NuScale Instrumentation and Control (I&C) systems and highlights of the I&C systems design described in NuScale Final Safety Analysis Report (FSAR) Chapter 7

Abbreviations

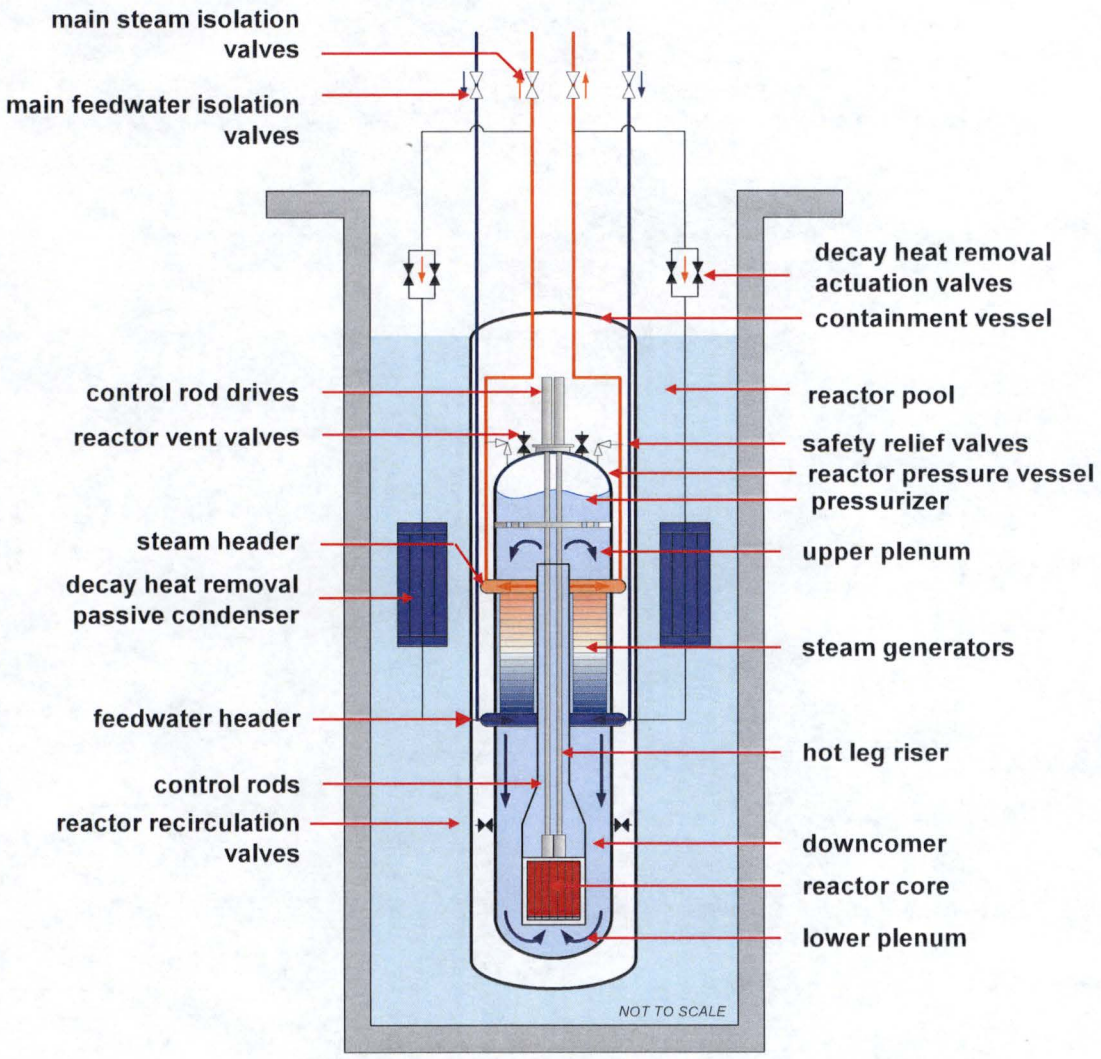
APL – actuation and priority logic
ASAI – application specific action item
CCF – common cause failure
CFDS – containment flood and drain system
CIS – containment isolation signal
CNT – containment system
CVCS – chemical and volume control system
D3 – diversity and defense-in-depth
DI&C – digital instrumentation and control
DHRS – decay heat removal system
ECCS – emergency core cooling system
EDSS – highly reliable DC power system
EDNS – normal DC power system
EIM – equipment interface module
ELVS – low AC voltage power system
ESFAS – engineered safety features actuation system
FPGA – field programmable gate array
HIPS – highly integrated protection system
HWM – hard-wired module
I&C – instrumentation and controls
ICIS – in-core instrumentation system
IEEE – Institute for Electrical and Electronics Engineers
ISM – input sub-module
MCS – module control system
MIB – monitoring and indication bus
MIB-CM – MIB communication module
MPS – module protection system
NPM – NuScale Power Module
NMS – neutron monitoring system
PAM – post-accident monitoring
PCS – plant control system
PPS – plant protection system
RMS – radiation monitoring system
RTB – reactor trip breaker
RTS – reactor trip system
SBM – scheduling and bypass module
SDB – safety data bus
SDIS – safety display and indication system
SFM – safety function module
SVM – scheduling and voting module
UTB – under the bioshield

NuScale DCA Chapter 7 Structure

- NuScale Chapter 7 Design Certification Application Follows Design Specific Review Standard Framework
  - Section 7.0: Instrumentation and Controls - Introduction and Overview
    - System Architecture and Overview
    - Key System Descriptions
  - Section 7.1 Fundamental Design Principles
    - Independence
    - Redundancy
    - Predictability and Repeatability
    - Diversity and Defense-in-Depth
    - Simplicity
    - Hazards Analysis
  - Section 7.2 System Features
    - Design and system characteristics in accordance with IEEE 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations" and IEEE Std 7-4.3.2-2003, "IEEE Standard Criteria for Digital Computers and Safety Systems of Nuclear Power Generating Stations"

Section 7.0: Instrumentation and Controls - Introduction and Overview

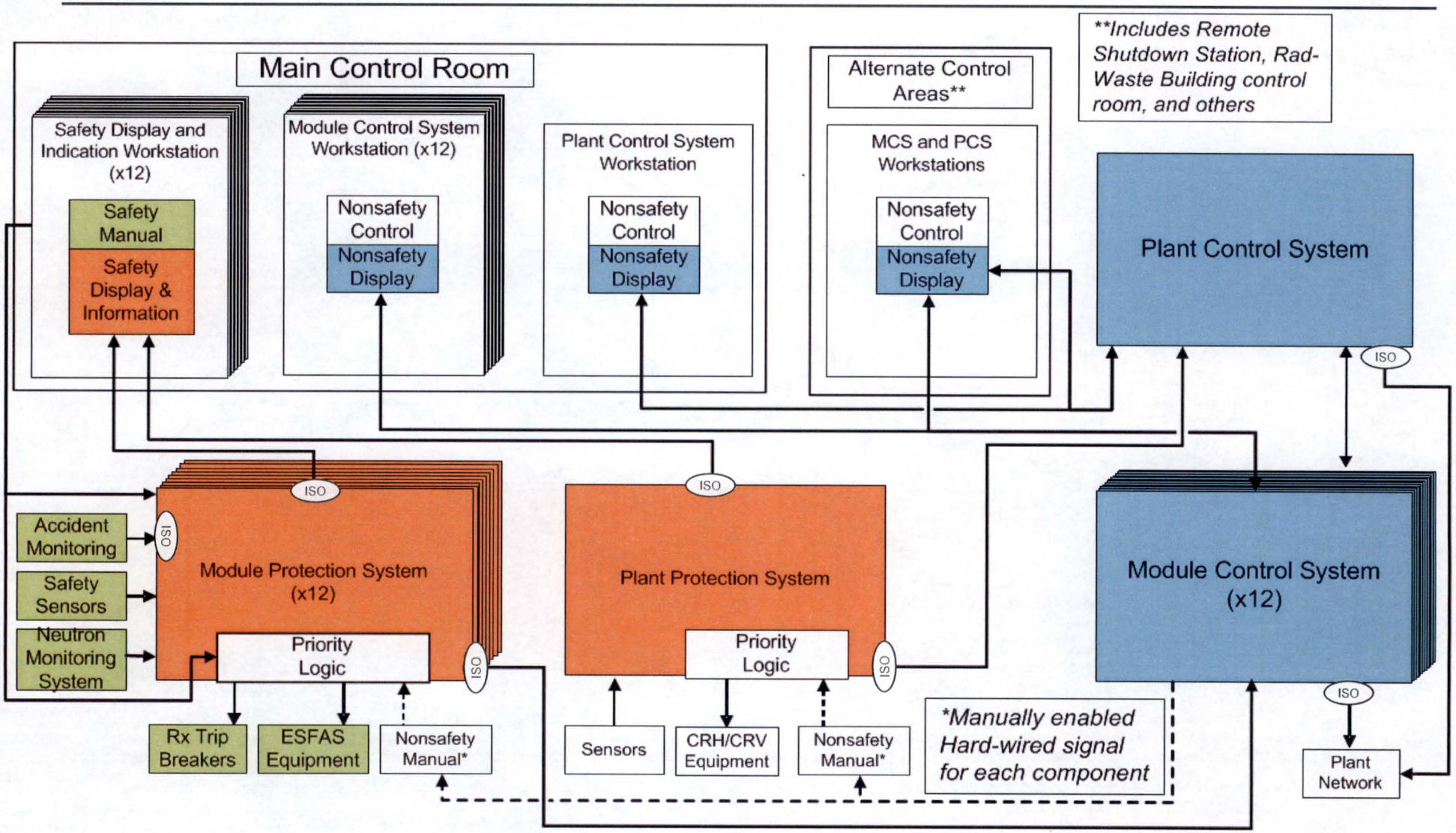
I&C System Design Basis



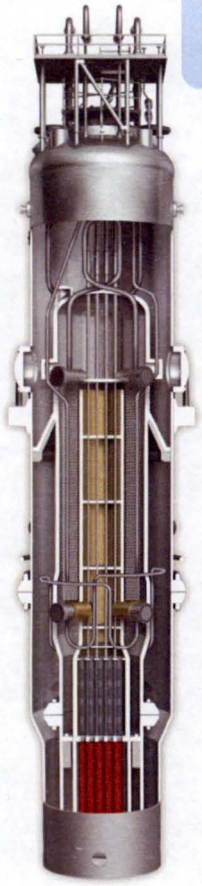
Safety I&C Platform

- Digital I&C system
- Use of FPGAs allows for diversification within the safety I&C platform
- Passive safety features result in a simpler safety I&C platform
- A simpler and more diversified design results in a more reliable safety I&C platform
- No safety-related pumps or fans to control
- Provide reactor trip breaker and pressurizer heater breaker trip signals
- Provide trip signals to solenoid operated valves
- On "loss of power" solenoids de-energize and associated valves fail in the "safe" position and reactor trip and pressurizer heater breakers open

I&C Architecture Overview



Module-Specific I&C Systems



Module Protection System (MPS) — Digital FPGA-based

The MPS is a digital, FPGA-based system that monitors process variables and provides automatic initiating signals in response to out-of-normal conditions, providing protection against unsafe NPM operation during steady state and transient power operation. Each NPM has a single dedicated MPS — A1

Neutron Monitoring System (NMS) — Analog

The neutron monitoring system (NMS) is an analog system comprised of three sub-systems:

- NMS-excore subsystem provides neutron flux data to the MPS for reactor trips — A1
- NMS-flood subsystem provides information to the MPS for post-accident monitoring during conditions when CNV is flooded — B2
- NMS-refuel subsystem provides neutron flux signals to the PCS during refueling operations (plant-level) — B2

Module Control System (MCS) — Digital-distributed control system

The MCS is a distributed control system which provides the Human System Interface and controls for monitoring and control of NPM specific plant components that are associated with the NPM balance-of-plant control functions. — B2

Incore Instrument System (ICIS)

The ICIS monitors the neutron flux distribution within the reactor core and provides core inlet and exit temperature information to the MPS for monitoring core cooling during post-accident conditions — B2

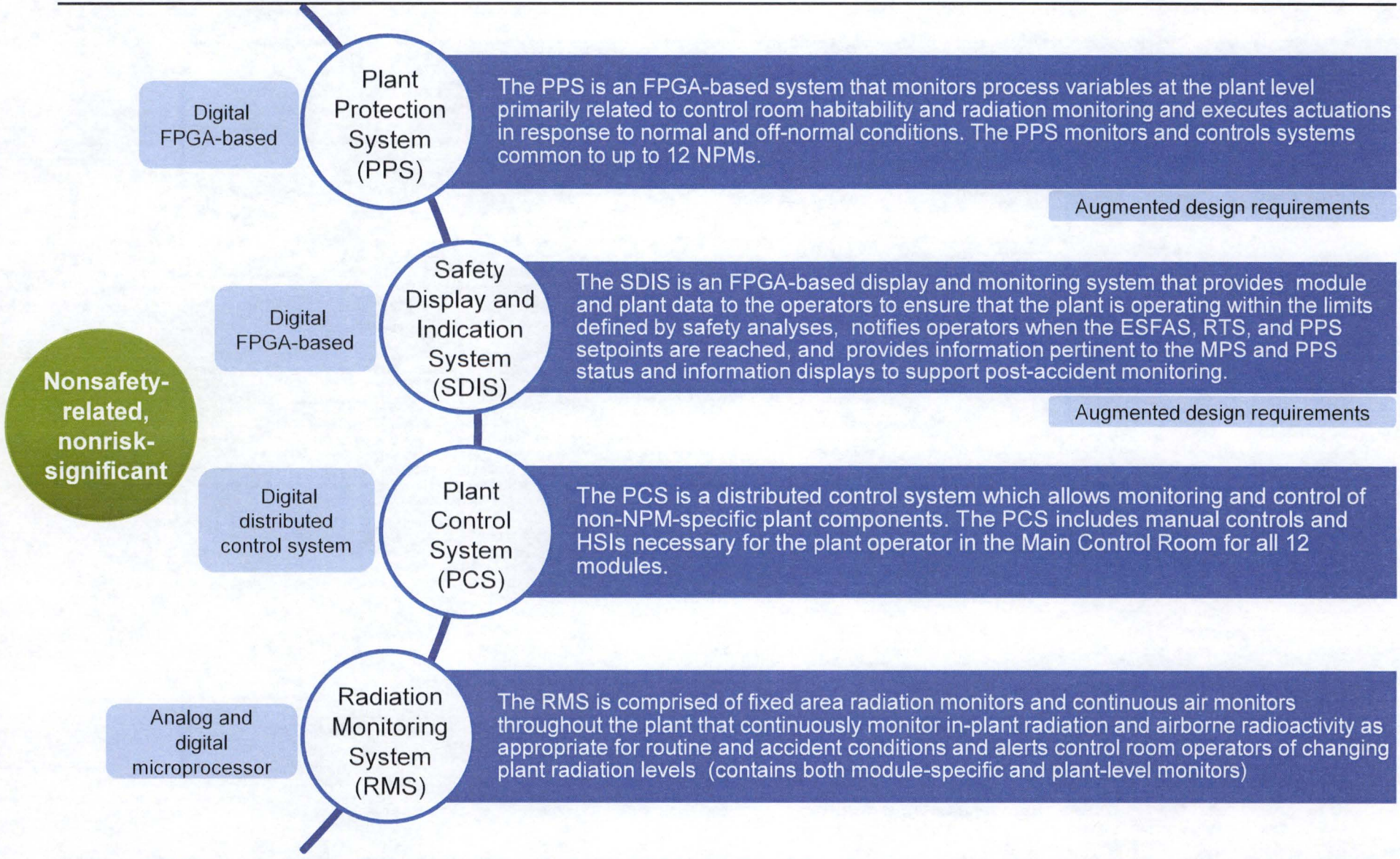
A1 - Safety-related, risk-significant

B2 - Nonsafety-related, not risk-significant

PM-0618-60212
Revision: 0

Template #: 0000-21727-F01 R4

Plant-Level I&C Systems

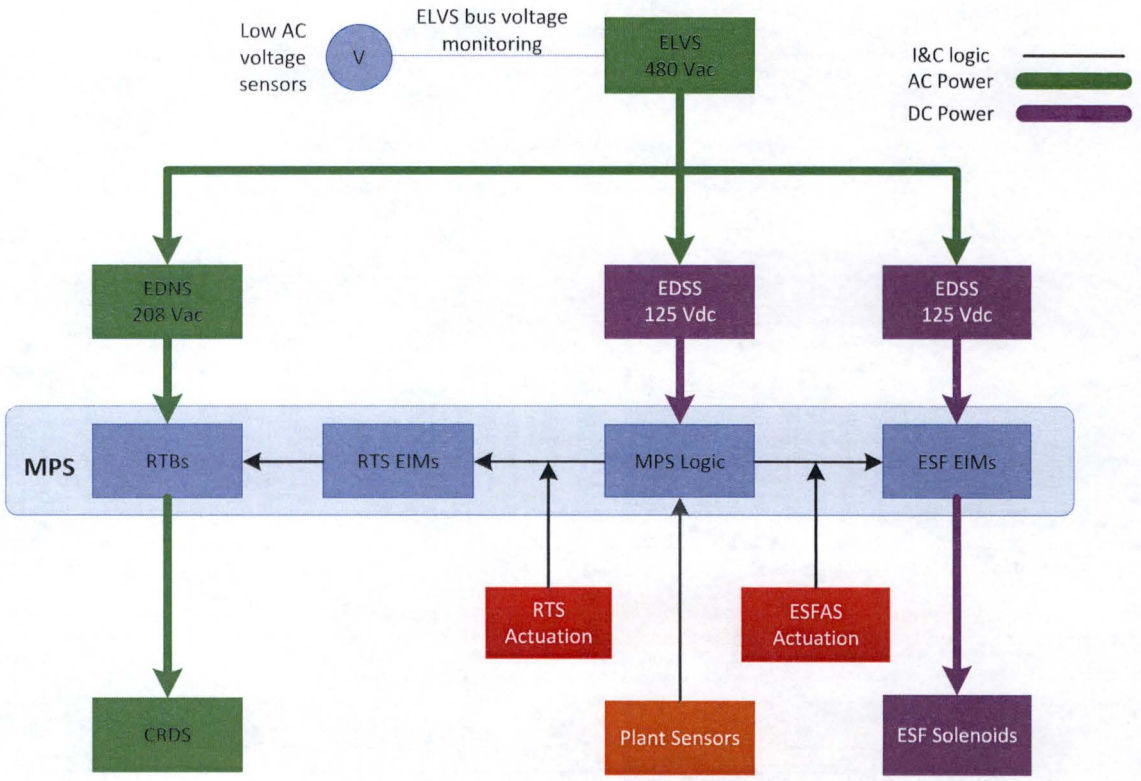


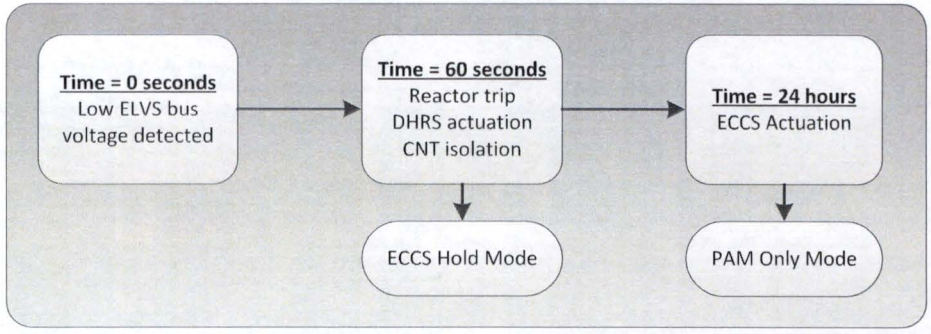
Module Protection System

- The NuScale safety-related MPS design is based on topical report TR-1015-18653-P-A, "Design of the Highly Integrated Protection System Platform" (HIPS TR).
- The safety-related I&C systems design basis conforms to the following without deviation or exceptions:
  - IEEE 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations"
  - IEEE Std 7-4.3.2-2003, "IEEE Standard Criteria for Digital Computers and Safety Systems of Nuclear Power Generating Stations"
  - Staff Requirements Memorandum to SECY 93-087, ""Policy, Technical and Licensing Issues Pertaining to Evolutionary and Advanced Light-water Reactor Designs"
- Major components:
  - Four separation groups of sensor inputs, electronics and trip determination
  - Class 1E DC-DC power converters/isolation devices
  - Reactor trip and pressurizer heater trip breakers
  - Two divisions of RTS and ESFAS voting and actuation components
  - Two divisions of hard-wired manual actuation switches
  - Nonsafety-related 24 hour timers
  - Nonsafety-related maintenance workstations
- MCR isolation switches provided in Remote Shutdown Station.

Loss of AC Power

- NuScale I&C Architecture provides for nonsafety-related post-accident monitoring (PAM) functions.
- Performed by MPS, PPS and SDIS and MCS for Type B, C and D, and other systems for Type E
- MPS "PAM-only" mode supports long-term PAM variable monitoring
- Sensors that support long-term PAM functions remain energized for 72 hours.
- Battery Mission Times
  - EDSS-MS Channel A & D – 24 hours (ECCS Hold Mode)
  - EDSS-MS Channel B & C – 72 hours (PAM Support)
  - EDSS-C Division I & II – 72 hours (PAM Support)





HIPS TR Application Specific Action Items

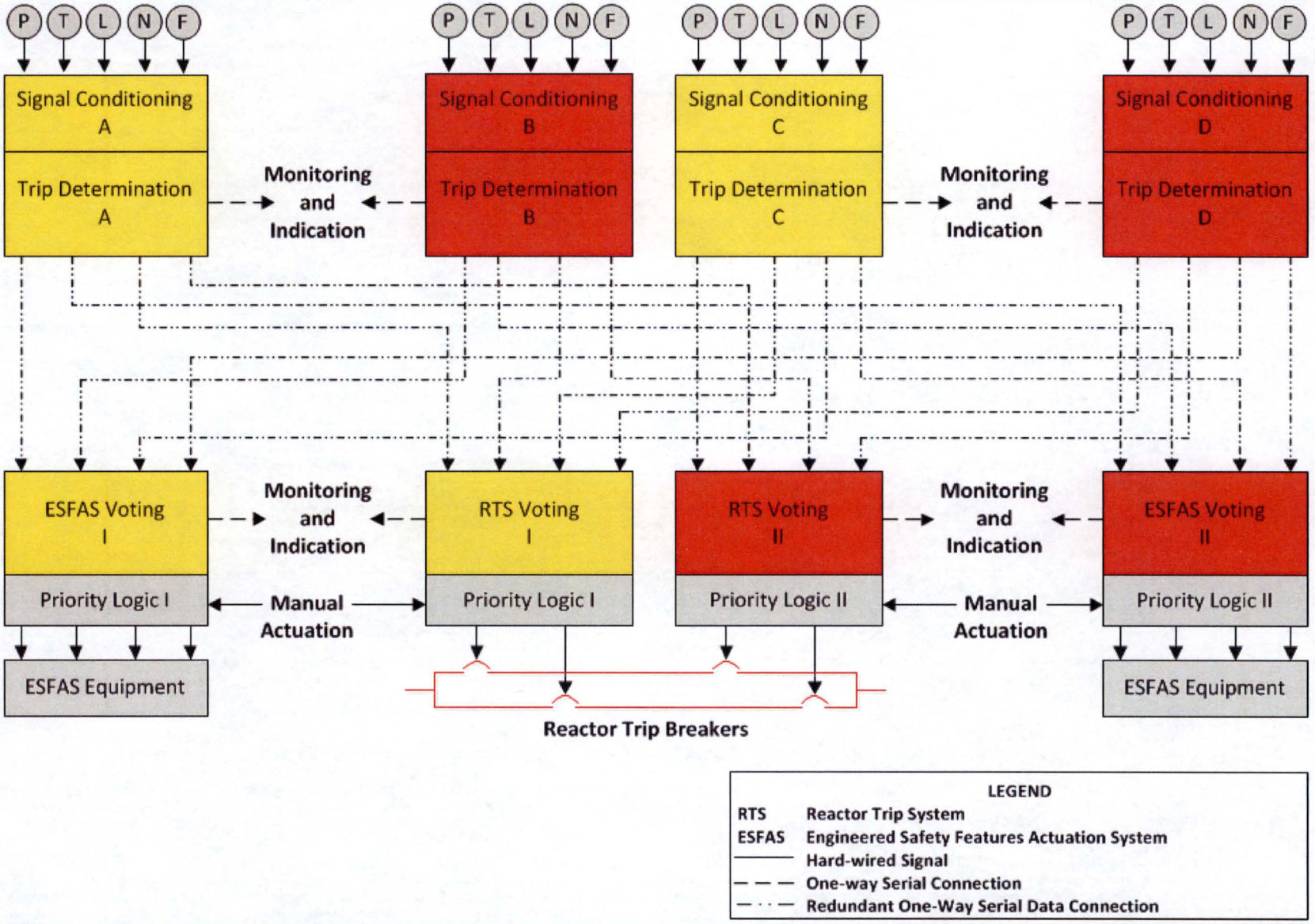
- FSAR addresses all 65 ASAIs in HIPS TR.
- FSAR Table 7.0-2 provides cross-references for all 65 ASAIs from HIPS TR.

Table 7.0-2: Highly Integrated Protection System Topical Report (HIPS TR) Application Specific Information Cross References

HIPS TR Application Specific Action Item Number	Section 7.0 - Introduction and Overview				Section 7.1- Fundamental Design Principles								Section 7.2 - System Characteristics													
	7.0.1	7.0.2	7.0.3	7.0.4	7.1.1	7.1.2	7.1.3	7.1.4	7.1.5	7.1.6	7.1.7	7.1.8	7.2.1	7.2.2	7.2.3	7.2.4	7.2.5	7.2.6	7.2.7	7.2.8	7.2.9	7.2.10	7.2.11	7.2.12	7.2.13	7.2.14	7.2.15
1	x				x																					
2				x																						
3[1]					x																					
▪ ▪ ▪																										
▪ ▪ ▪																										
▪ ▪ ▪																										
63									x																	
64									x																	
65									x																	

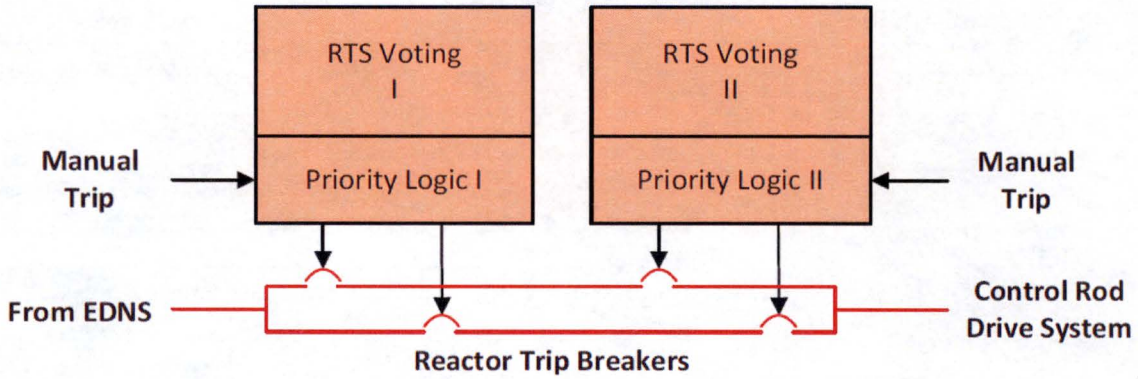
Note 1: For ASAIs 3 through 6, the overall conformance of the MPS to IEEE Std 603-1991, IEEE Std 7-4.3.2-2003, Digital I&C ISG-04 and SRM for SECY-93-087 is described in Section 7.1.1.

MPS Top-Level Architecture

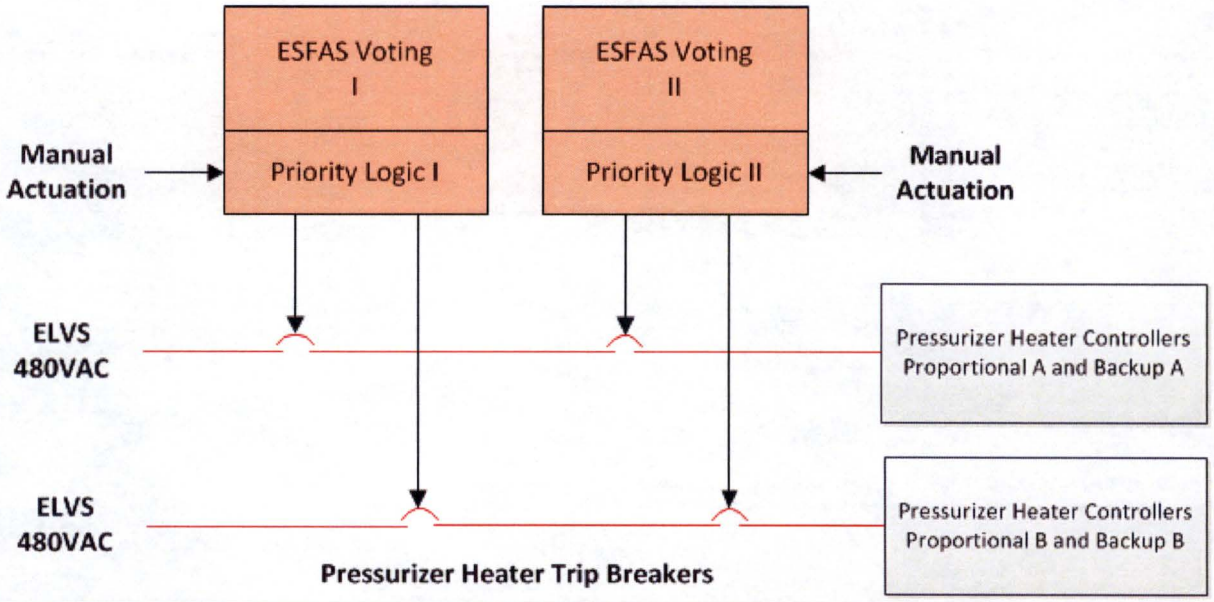


MPS Breaker Configuration

- Four reactor trip breakers, two per division



- Four pressurizer heater trip breakers, two per division



Each breaker opens upon loss of power to the under voltage coil.
A shunt trip coil is provided as a nonsafety-related diverse means to open the breakers

Nonsafety System Segmentation

- Segmentation is used as a defensive and preventative measure in the MCS architecture. Segmentation provides functional independence between major control functions preventing against a failure in one controller group from causing an undesirable condition in another controller group.
- Preventive and limiting measures are determined by a susceptibility analysis that considered malfunctions and spurious actuations, as set forth in NRC DI&C-ISG-04, Section 3.1, staff position 5.
- Control groups were evaluated for effect on:
  - reactivity addition to the reactor coolant system
  - primary coolant pressure increase or decrease
  - primary coolant temperature increase or decrease
  - primary coolant level increase or decrease
  - radioactive material release to the environment

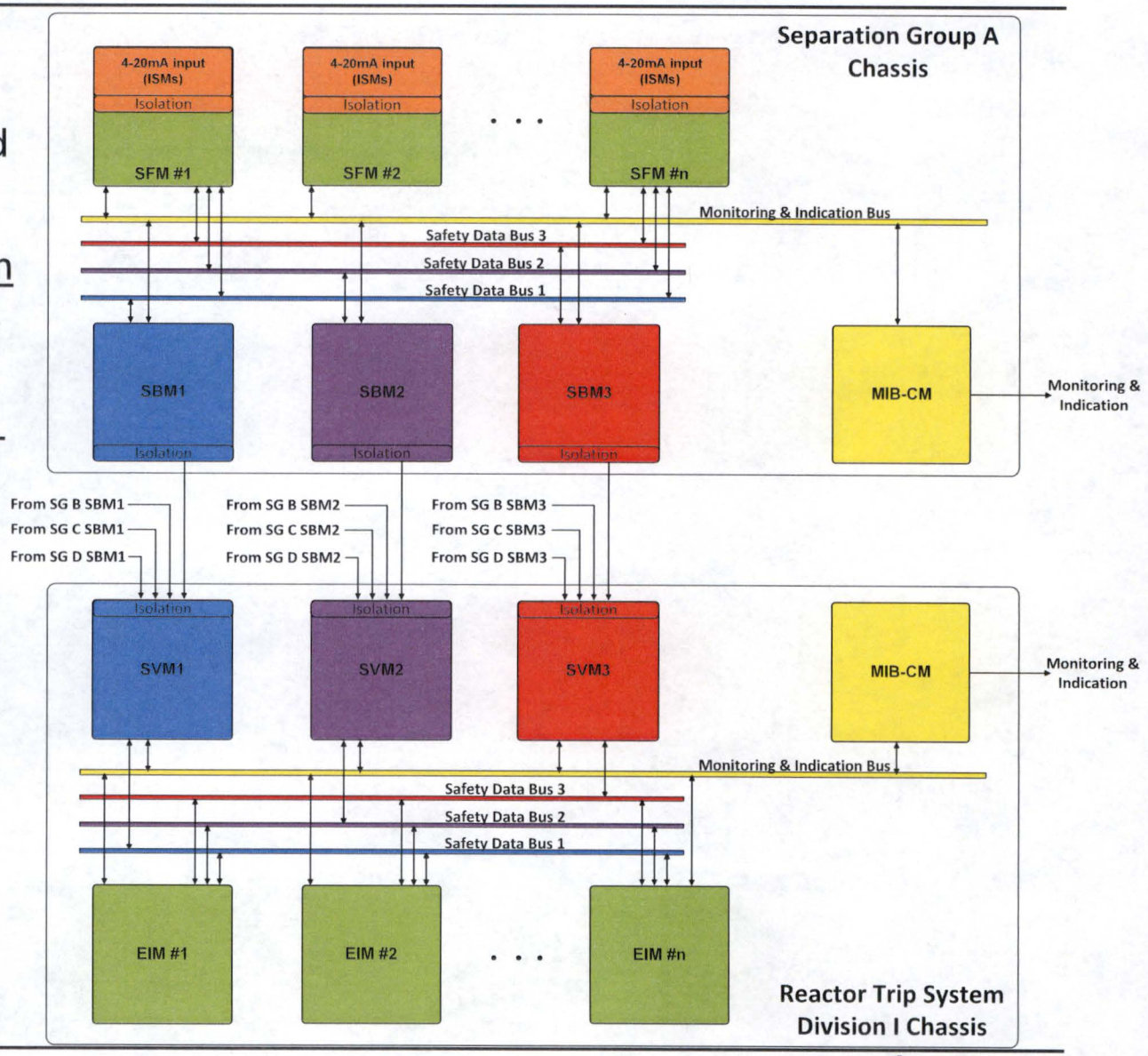
Section 7.1 Fundamental Design Principles

Fundamental Design Principles

- Independence
- Redundancy
- Predictability and Repeatability
- Diversity and Defense-in-Depth
- Simplicity

Independence

- The MPS and NMS are designed with physical, electrical, communication and functional independence.
- One-way communication from safety to nonsafety systems through isolated data paths.
- Separation of safety and non-safety communications on different communication busses.
- MCS control of safety-related components via hard-wired isolated inputs from MCS (no digital signals)



Safety Data Paths (1, 2, 3)
Safety Data Path 1
Safety Data Path 2
Safety Data Path 3
Monitoring and Indication Path

Redundancy

- FSAR Section 7.1.3
- Four separation groups, two divisions of MPS
- Four channels of safety-related NMS
  - MPS and NMS meet single failure criterion
- Post-accident monitoring channels
  - No PAM Type A variables
  - PAM Type B and C variables meet single failure criterion
- Nonsafety I&C Systems incorporate redundancy principles for high reliability, asset protection

Predictability and Repeatability

- FSAR Section 7.1.4
- The MPS applies the deterministic features of the HIPS platform.
- The MPS response time is accounted for in the plant safety analysis actuation delays.

Diversity and Defense-in-Depth

- FSAR Section 7.1.5
- D3 strategy relies on platform/technology diversity for defense against common-cause failures
  - diversity for the platform technology is achieved through different FPGA chip technologies and their associated development tool sets
- Approach simplifies the D3 Diversity Assessment and narrows scope of coping analysis required for digital-based sensors.

Sensor Diversity

- Coping Analysis performed (summarized in FSAR Table 7.1-18) to address potential digital-based CCF vulnerabilities associated with digital-based sensors for pressure, level and flow measurements.
- Coping analysis included a full evaluation of all design basis events analyzed using best-estimate methods to analyze a postulated digital-based sensor CCF.
  - In some cases, the event never progressed to a trip condition using best-estimate analytical methods.
  - In other cases, diverse, non-digital sensors initiated the trip condition.

Result → D3 coping analysis acceptance criteria met

Section 7.2 - System Features

Control of Access

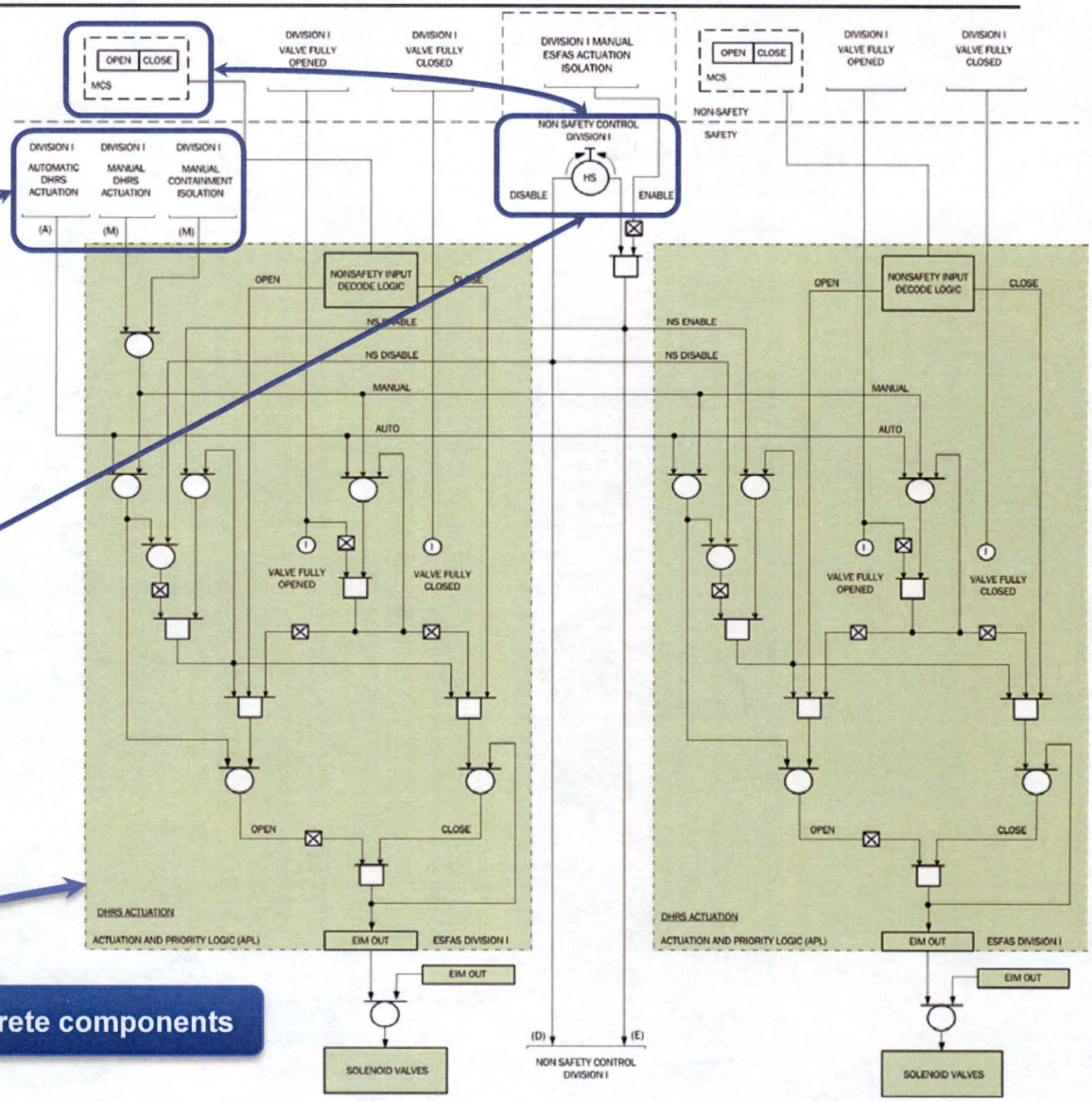
- MPS design conforms to IEEE 603-1991, Section 5.9, "Control of Access" and Secure Development and Operational Environment requirements of Regulatory Guide 1.152, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants," Revision 3.
  - Physical protection: locked cabinets/rooms.
  - MPS design does not provide for remote access capability.
  - Physical and logical controls prevent modification of MPS FPGA Logic while in service.
  - Limited set of MPS tunable parameters (i.e., setpoints) can be modified when SFM is bypassed and special equipment is used.

Automatic and Manual Controls

- All MPS RTS/ESFAS functions occur automatically.
- MPS provides for manual actuation via hard-wired switches in main control room as backup to automatic functions:
  - reactor trip
  - ECCS actuation
  - decay heat removal actuation
  - containment isolation
  - demineralized water system isolation
  - chemical and volume control system isolation
  - pressurizer heater trip
  - low temperature over pressure protection

Actuation Priority Logic

- APL circuit provides for prioritization of safety-related signals
  - Automatic/Manual RTS/ESFAS actuation commands have highest priority.
  - Enable control of safety-related components from nonsafety-related MCS via Enable Nonsafety Control Switch MCS hard-wired interfaces



Non-digital (no software) circuit -- comprised of discrete components

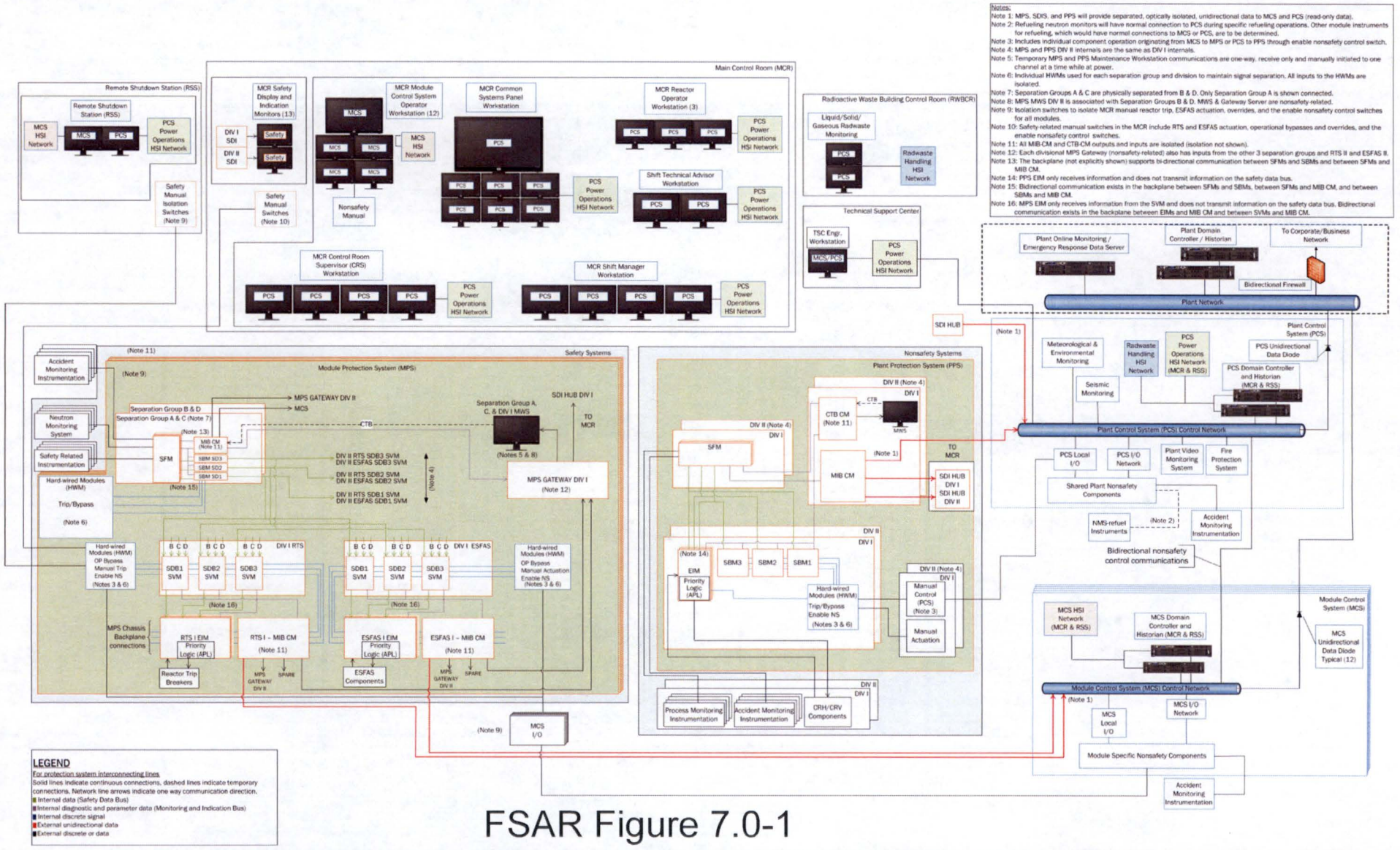
Conclusion

- NuScale FSAR follows the new Chapter 7 DSRS structure
  - Overall resulted in more streamlined, efficient review.
- The NuScale I&C design meets regulatory requirements contained in IEEE 603-1991, IEEE 7-4.3.2-2003 and SRM to SECY-93-087.
- The I&C architecture and systems incorporate the fundamental design principles with an overall focus on simplicity.
- NuScale passively safe design results in a simple I&C design solution – no complicated functions
  - Simple RTS/ESFAS functions (simple comparators, simple functions)
  - No closed/open loop control – all safety-related functions are "de-energize to actuate"
  - Safety function is accomplished by the removal of electrical power (e.g., reactor trip breakers open on loss of power)

Appendix:

FSAR Figure 7.0-1, I&C Architecture Diagram

NuScale I&C Architecture



FSAR Figure 7.0-1

Portland Office
6650 SW Redwood Lane,
Suite 210
Portland, OR 97224
971.371.1592

Corvallis Office
1100 NE Circle Blvd., Suite 200
Corvallis, OR 97330
541.360.0500

Rockville Office
11333 Woodglen Ave., Suite 205
Rockville, MD 20852
301.770.0472

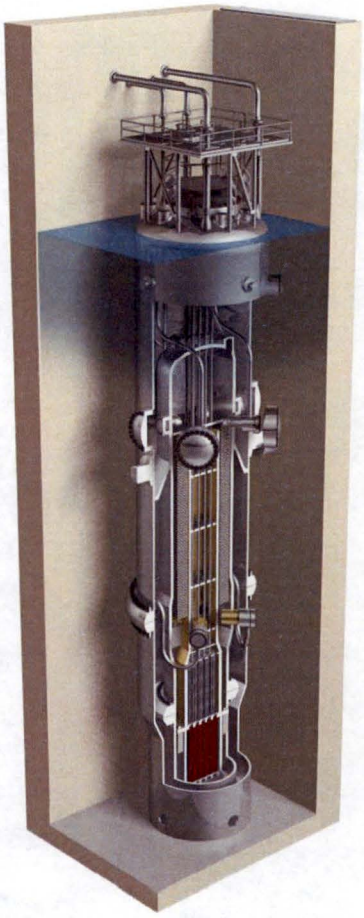
Charlotte Office
2815 Coliseum Centre Drive,
Suite 230
Charlotte, NC 28217
980.349.4804

Richland Office
1933 Jadwin Ave., Suite 130
Richland, WA 99354
541.360.0500

Arlington Office
2300 Clarendon Blvd., Suite 1110
Arlington, VA 22201

London Office
1st Floor Portland House
Bressenden Place
London SW1E 5BH
United Kingdom
+44 (0) 2079 321700

http://www.nuscalepower.com
Twitter: @NuScale_Power



NUSCALE™
Power for all humankind