NuScale Power™

LO-0415-13815

April 29, 2015

Docket: PROJ0769

U.S. Nuclear Regulatory Commission
ATTN: Document Control Desk
One White Flint North
11555 Rockville Pike
Rockville, MD 20852-2738

SUBJECT: Submittal of presentation materials entitled "NuScale Integrated Protection System Architecture," Revision 0, (PM-0415-13814) for use during a public meeting on May 6, 2015 (NRC Project No. 0769)

A public meeting between NuScale Power, LLC (NuScale) and the NRC technical staff is scheduled for May 6, 2015, to discuss various topics related to digital instrumentation and controls, including the NuScale integrated protection system architecture.

Enclosure 1 is the presentation entitled "NuScale Integrated Protection System Architecture" for this meeting. This enclosure contains no regulatory commitments.

Please feel free to contact me at 301-770-0472 or at smirsky@nuscalepower.com if you have any questions.

Sincerely,

Steven Mirsky

Steven Mirsky
NuScale Washington DC Licensing Manager

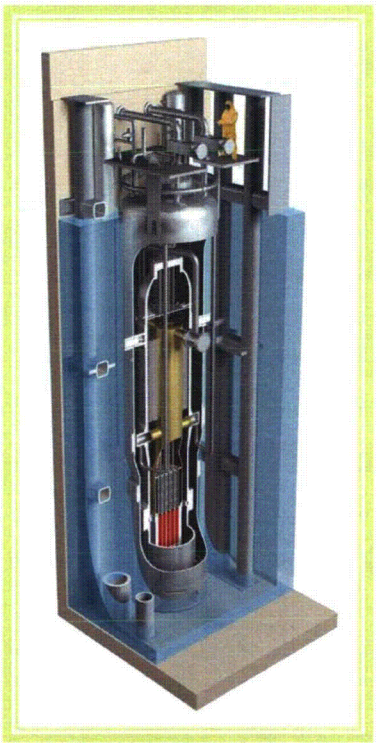
Distribution: Greg Cranston, NRC, TWFN-6E7
Jenny Gallo, NRC, TWFN-6E7
Michael Mayfield, NRC, TWFN-6E4
Omid Tabatabai, NRC, TWFN-6E7
Mark Tonacci, NRC, TWFN-6E7

Enclosure 1: "NuScale Integrated Protection System Architecture", PM-0415-13814-NP, Revision 0, nonproprietary

NuScale Power, LLC
1100 NE Circle Blvd., Suite 200 Corvallis, Oregon 97330 Office 541.360.0500 Fax 541.207.3928
www.nuscalepower.com

D111
NRO

NuScale Integrated Protection System Architecture



Jason Pottorf
Supervisor, I&C Engineering

Gregg Clarkson
Senior Digital I&C Consultant

May 6, 2015

PM-0415-13814-NP
Revision: 0

NuScale Power™

Protection System Design Approach

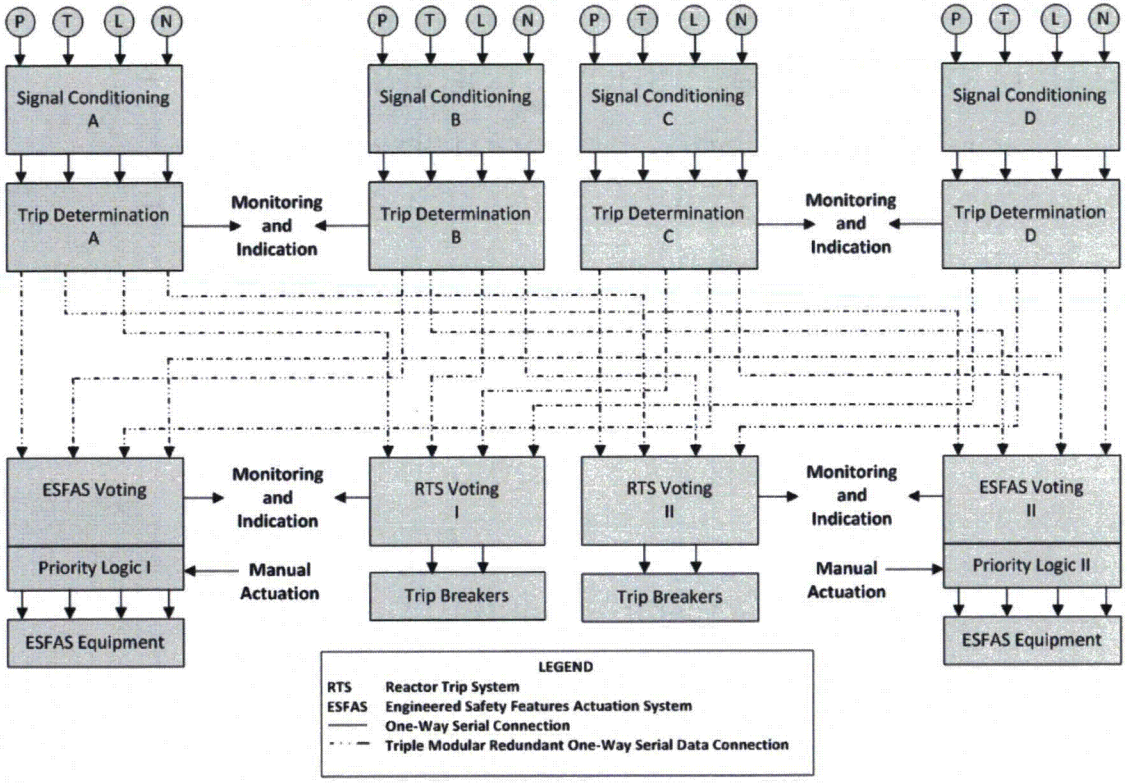
- Hybrid digital and analog system architecture
- Key design attributes
  - independence
  - redundancy
  - determinism
  - simplicity
  - diversity
  - testing and diagnostics
- Diversity inherent to the architecture without the complexity of adding “extra” systems
- Safe, simple, and elegant to complement the NuScale reactor design

NuScale Power™

Hybrid Protection System

- Hybrid digital and analog protection system
  - Embraces the best of each technology
  - Digital pros
    - improved diagnostics
    - improved testability
    - reduced maintenance, i.e., calibration frequency
  - Analog pros
    - proven approach
    - independence of functionality
    - reduced complexity
    - licensing basis is well established
  - FPGA usage for digital portions is closer to established analog designs than microprocessor-based systems
  - All manual actuations are achieved with analog circuity only, no digital
  - Independent safety functions; a well-established design approach
  - Inherent built-in cyber security protection

Module Protection System (MPS)

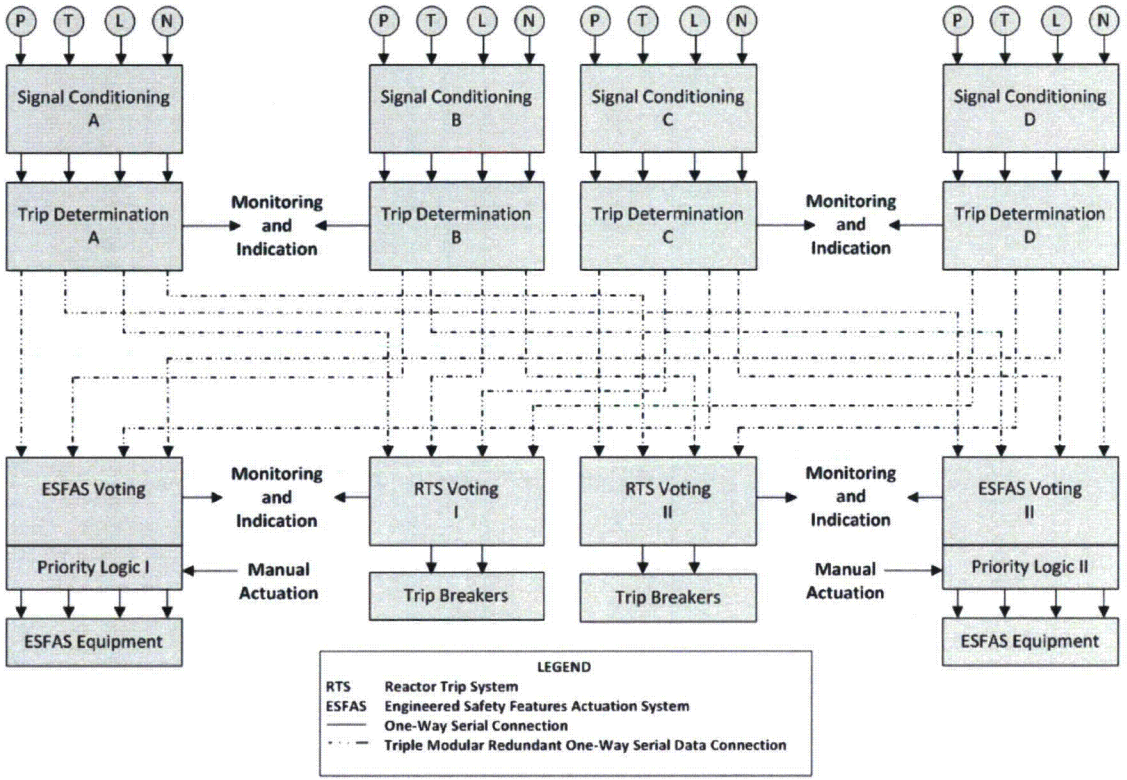


MPS Architecture

- Four separation groups of input sensors and detectors
- Four separation groups of signal conditioning
- Four separation groups of trip determination
- Two divisions of reactor trip system (RTS) voting and reactor trip breakers
- Two divisions of engineered safety features actuation system (ESFAS) voting and engineered safety features (ESF) equipment

NuScale Power™

Module Protection System (MPS)

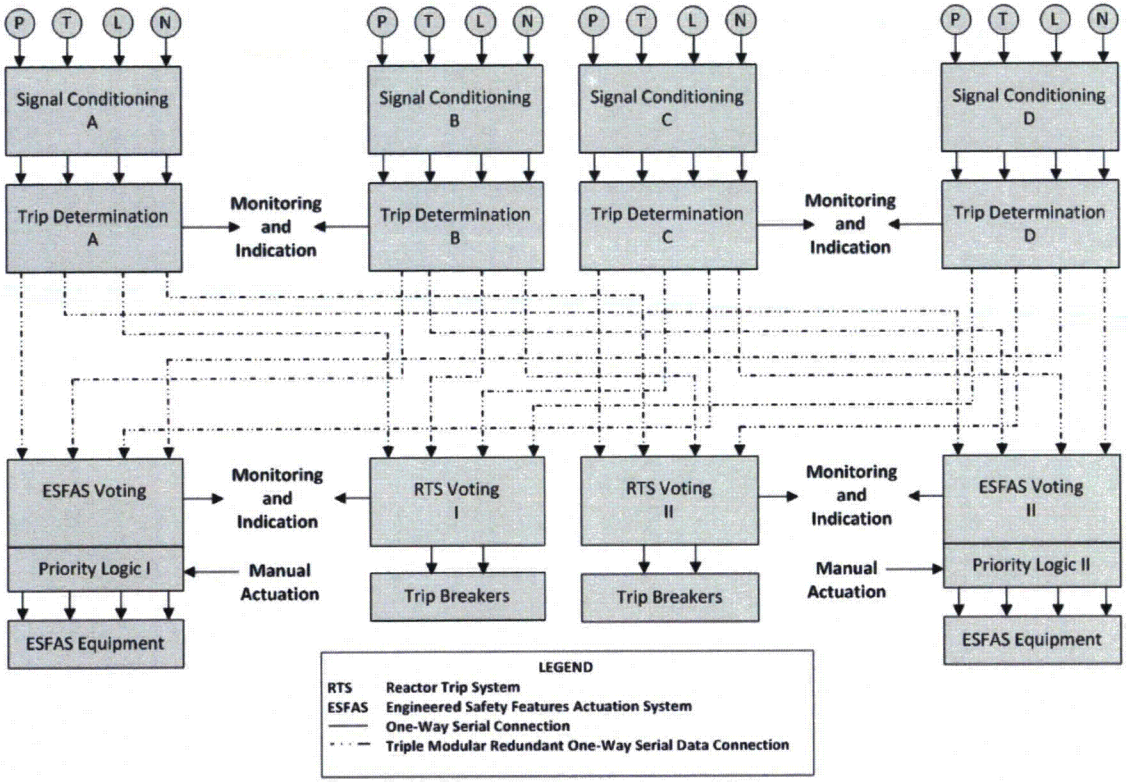


Sensors and Detectors

- Responsible for measuring different process parameters such as pressure, temperature, level, and neutron flux
- Each process parameter is measured using different sensors and is processed by different algorithms, which are executed by independent logic engines

NuScale Power™

Module Protection System (MPS)

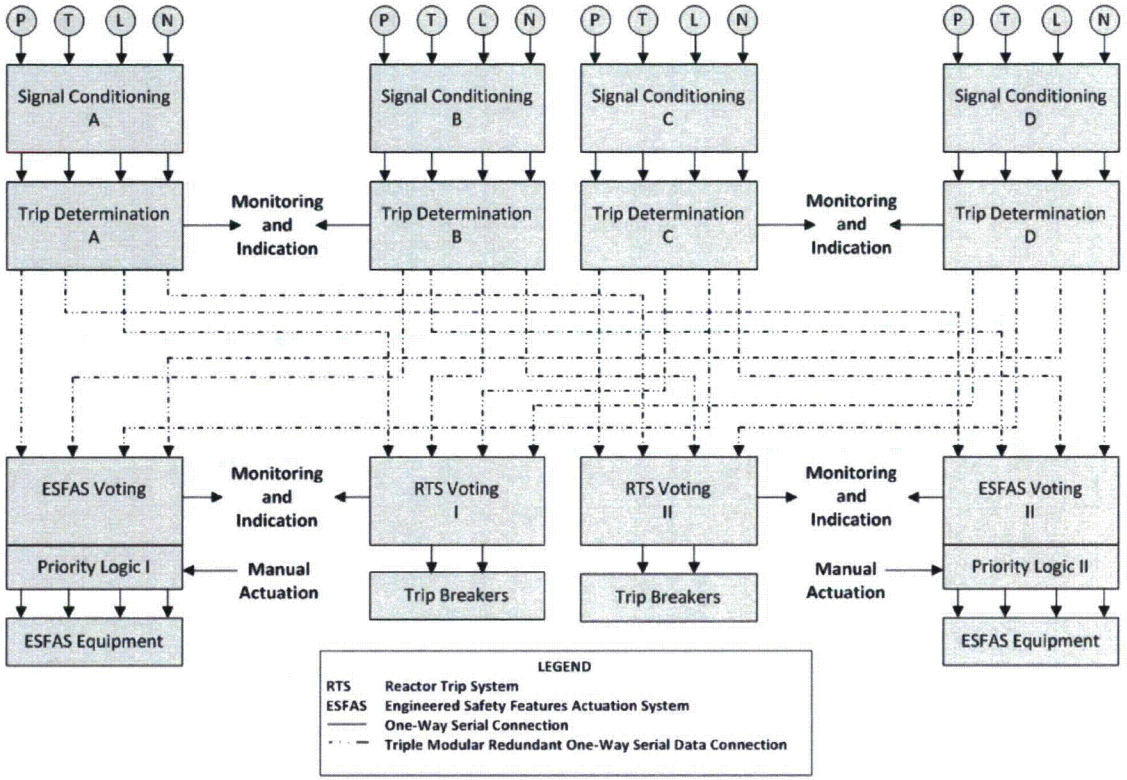


Signal Conditioning

- Process sensors provide inputs to the signal conditioning block
- Signal conditioning is composed of multiple input modules that are responsible for conditioning, measuring, filtering, and sampling field input signals
- Each input module is dedicated to a specific input type
- An input module is comprised of an analog circuit and a digital circuit
- The analog signal conditioning circuitry is responsible for converting analog voltages or currents into a digital representation
- The digital portion of the input module is located within the logic engine
- The logic engine performs all input module control, integrity checks, and digital filtering functions

NuScale Power™

Module Protection System (MPS)

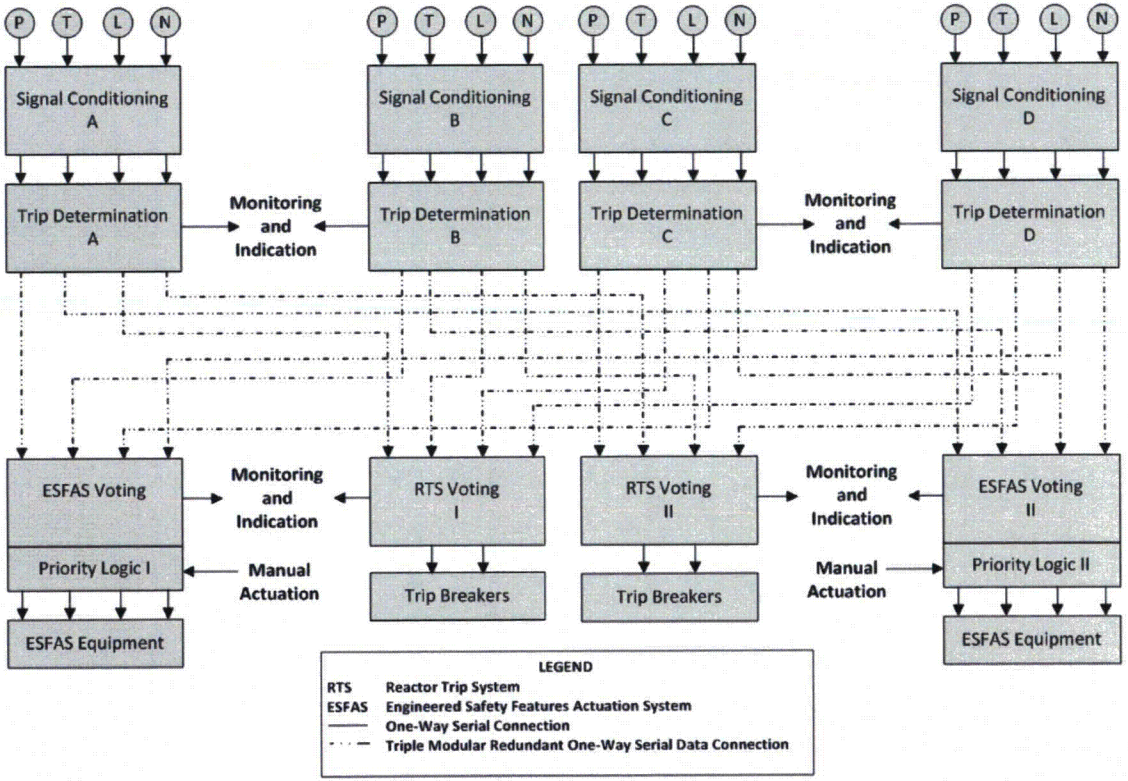


Trip Determination

- The trip determination block receives process input values from the signal conditioning block
- Composed of independent safety function modules, where a specific module implements a single set of safety functions
- A set of safety functions may consist of a group of functions related to a primary variable, such as a high and low trip from the same pressure input
- Each safety function module contains a unique logic engine dedicated to implementing one set of safety functions
- Implementation results in the processing logic of each safety function module being unique and therefore different than all other safety function modules

NuScale Power™

Module Protection System (MPS)

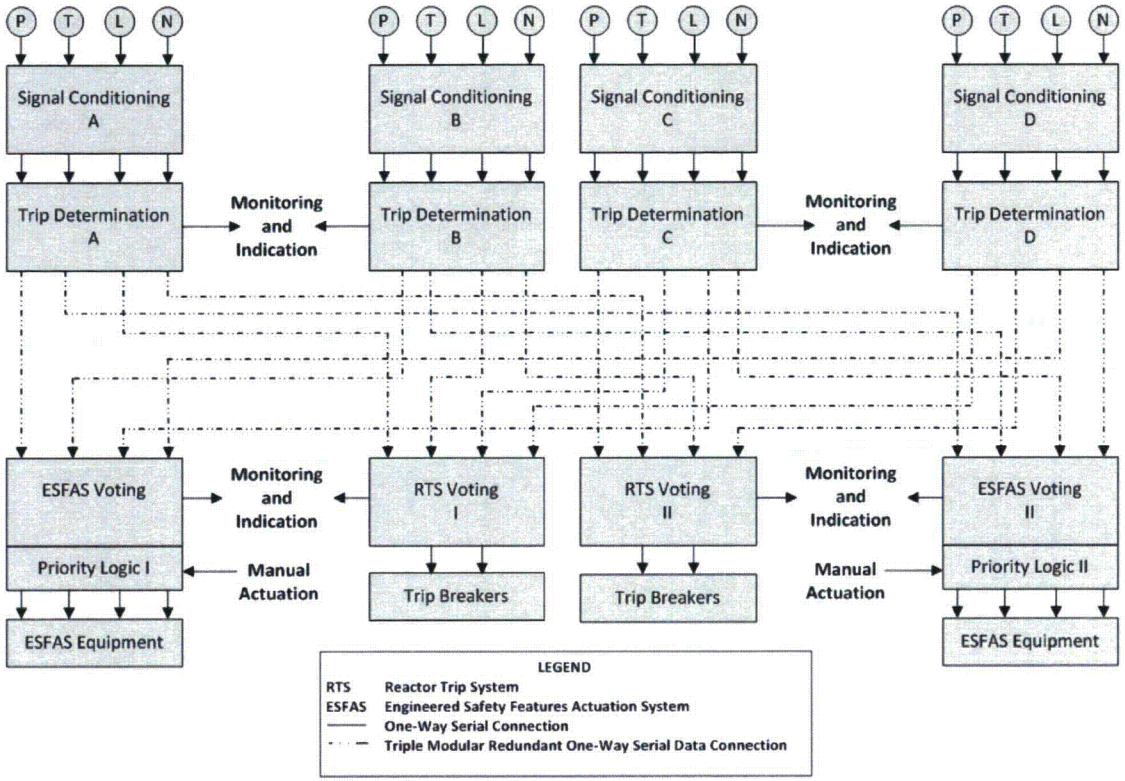


Trip Determination, cont.

- Process input values are communicated via a deterministic path and are provided to a specific safety function module
- Input values then converted to engineering units to determine what safety function or set of safety functions is implemented on that specific safety function module
- Safety function module can make a reactor trip determination, ESFAS actuation determination, or both.
- Reactor trip determination is based, if required, on a predetermined set point, and provides a trip or no-trip demand signal to each RTS division via an isolated transmit only serial data path
- ESFAS actuation determination, if required, is based on a predetermined set point, and provides an actuation or do-not-actuate demand signal to each ESFAS division via an isolated transmit-only serial data path.

NuScale Power™

Module Protection System (MPS)

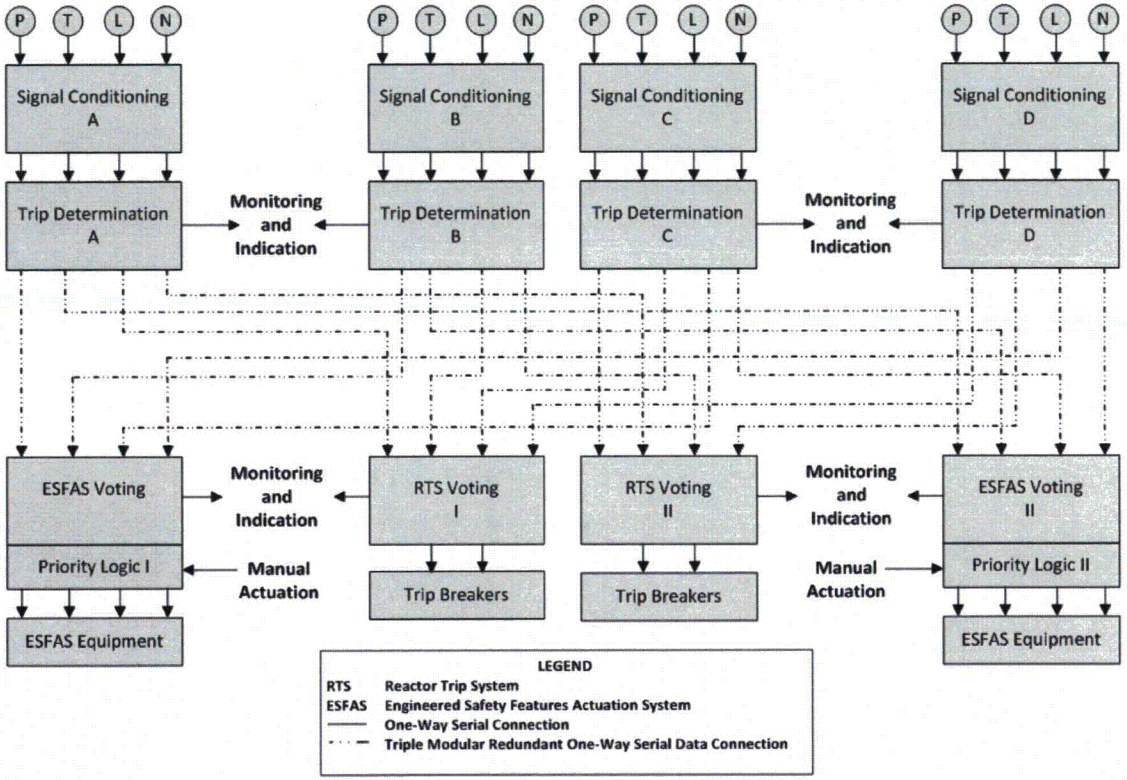


Reactor Trip System (RTS)

- The RTS is a sub-system within the MPS and keeps the reactor operating within a safe region by automatically shutting down the reactor whenever the limits of safe operation are approached
- Each of two RTS divisions receives inputs from all trip determination blocks via isolated receive-only serial data paths
- The trip inputs are combined in the RTS voting logic so that two or more reactor trip inputs from the trip determination modules produce an automatic reactor trip output signal that actuates the reactor trip breakers associated with that division
- A manual trip capability also provides a direct trip of the reactor trip breakers as well as input to the automatic actuation to ensure the sequence is maintained

NuScale Power™

Module Protection System (MPS)



Engineered Safety Features Actuation System (ESFAS)

- Consists of two divisions of actuation logic arranged so that no single failure can prevent a safeguards actuation when required, and no single failure in a single measurement channel can generate an unnecessary safeguards actuation
- Provides both automatic and manual initiation of critical protection functions, such as decay heat removal, emergency core cooling, and containment isolation
- Each of two ESFAS divisions receives inputs from all trip determination modules via isolated receive-only serial data paths
- Specific actuation logic and voting occur within the ESFAS block
- When the ESFAS logic and voting determine an actuation is required, the ESFAS sends the actuation demand signal to a dedicated analog priority logic circuit, which actuates appropriate ESF equipment

NuScale Power™

Design Attributes of the MPS

Independence

- The MPS is designed to ensure a high level of independence between the key elements
  - four separation groups of sensors and detectors
  - four separation groups of trip determination
  - two divisions of the RTS
  - two divisions of the ESFAS
  - two divisions of the ESF equipment
- Based on the inputs to a safety function module, the MPS implements a safety function or group of safety functions independently within each of the four separation groups. Safety function independence is maintained from the sensor to the trip determination output. This method of independence ensures that a failure within independent safety functions does not propagate to any of the other safety function modules.
- Communication of data within the MPS is transmitted or received via triple module redundant, independent, optically isolated, one-way communication paths. This communication scheme ensures that a safety function is not dependent on any information or resource originating outside its division to accomplish its safety function. Fault propagation between Class 1E divisions is prevented by one-way optical isolation of the divisional trip signals.

Redundancy

- The MPS design incorporates redundancy in multiple areas of the architecture. The redundancy within the MPS includes four separation groups of sensors and detectors, trip determination, and two divisions of RTS and ESFAS circuitry.
- The MPS uses two-out-of-four voting so that a single failure of an input process signal will not prevent a reactor trip or ESF equipment actuation from occurring when required. Additionally, a single failure of an input process signal will not cause spurious or inadvertent reactor trips or ESF equipment actuations when they are not required.

Design Attributes of the MPS

Determinism

The MPS incorporates a deterministic design. All logic is implemented in fixed logic and/or finite-state machines, and all safety data are communicated in a fully deterministic manner.

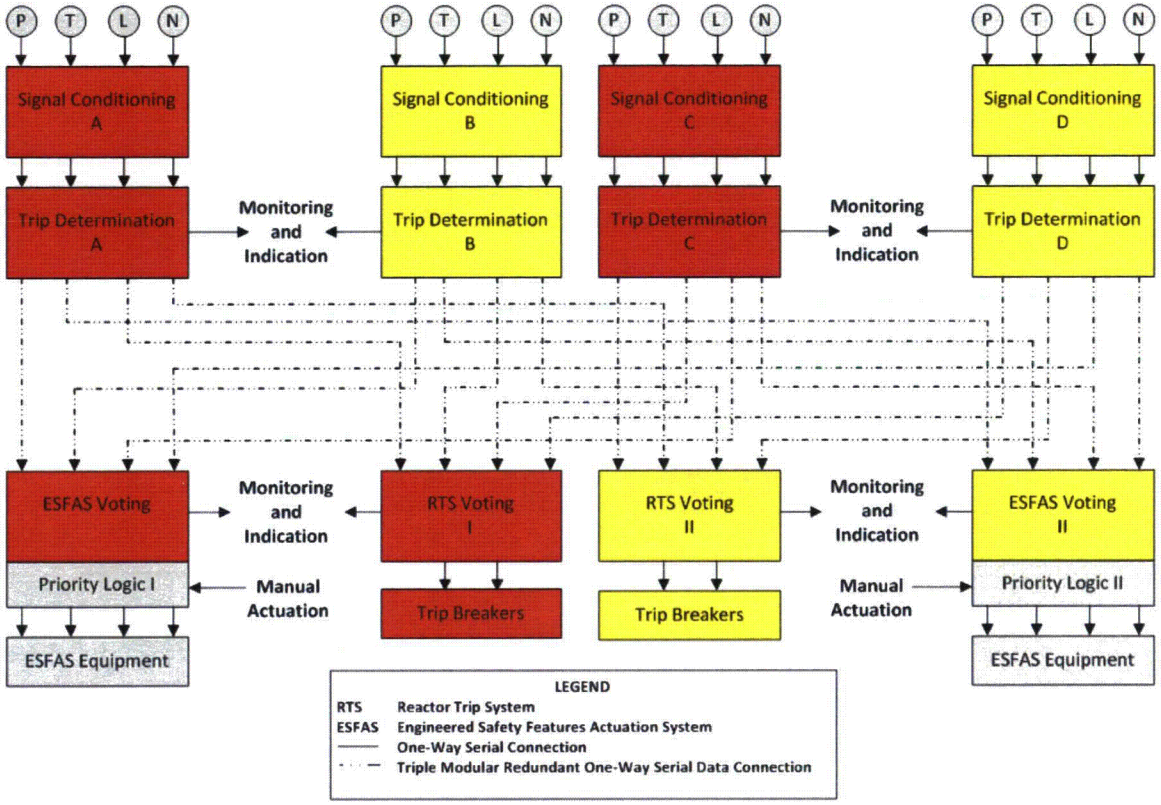
- Each module employs specific logic implemented in fixed logic and/or individual finite-state machines specific to the particular function or functions performed by the module.
- Ensures the behavior of the logic can be predetermined. The fixed logic and/or finite-state machine receives inputs specific to the function performed by the module. The decision made by the fixed logic and/or finite-state machine relates only to a specific function, and its outputs, in turn, relate only to this specific function.
- Allows for exhaustive testing of the functionality, including all possible inputs and outputs of the state machine.
- All safety-related data within the MPS are communicated using a deterministic protocol. This protocol functions in a cyclic manner and maintains this cyclic behavior for all conditions.

Simplicity

The MPS architecture is designed specifically for the NuScale reactor module. Its design is intended to complement the safe and simple attributes of the NuScale reactor design. The key design techniques include the following:

- The design is based on a symmetrical architecture of four separation groups and two trip or actuation divisions. Each of the four separation groups is functionally equivalent to the others, and each of the two divisions is functionally equivalent. Two-out-of-four voting is the only voting strategy utilized.
- The logic is implemented in relatively simple fixed logic or finite-state machines dedicated to a particular safety function or group of safety functions.
- All communications are based on simple, deterministic protocols, and all safety data are communicated via redundant, one-way communication paths.
- Diversity attributes are designed to be inherent to the architecture without the additional complexities of "extra" systems based on completely different platforms.

Design Attributes of the MPS



Multi-Layered Diversity

- Intentionally implemented to eliminate the concern for software-based or software logic-based common cause failures (CCF)
- Diversity attributes incorporated
  - functional diversity
  - signal diversity
  - hardware diversity*
  - equipment diversity*
  - software diversity*
  - design diversity*

*Shown in diagram with red and yellow elements

NuScale Power™

Design Attributes of the MPS

Transient/Event	Safety Function	Safety Function Parameter	A	C	B	D
A-Loss of Feedwater	A1	High Steam Temperature	✓	✓	✓	✓
	A2	High Reactor Pressure	✓	✓	✓	✓

Transient/Event	Safety Function	Safety Function Parameter	A	C	B	D
A-Loss of Feedwater	A1	High Steam Temperature	CCF	CCF	✓	✓
	A2	High Reactor Pressure	✓	✓	✓	✓

Multi-Layered Diversity, cont.

Example of impact of CCF mitigated by multi-layered approach to diversity

- Top diagram provides an example of two safety functions that mitigate a single reactor transient or event.
- Bottom diagram illustrates the result of the multi-layered diversity and how the CCF is bounded such that the safety function A1 is completed by 'B' and 'D' and safety function A2 is completed by 'A', 'B', 'C', and 'D'.

NuScale Power™

NuScale Power™

6650 SW Redwood Lane, Suite 210
Portland, OR 97224
503.715.2222

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

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

6060 Piedmont Row Drive South, Suite 600
Charlotte, NC 28287
704.526.3413

http://www.nuscalepower.com