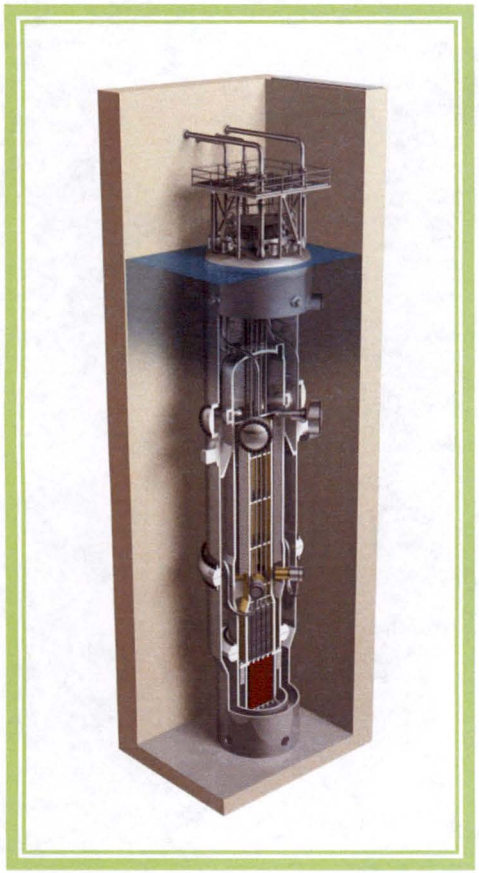
Enclosure 2:

"ACRS Presentation: Design of the Highly Integrated Protection System Platform Topical Report", PM-0217-52652, Revision 0, nonproprietary version

NuScale Power, LLC
1100 NE Circle Blvd., Suite 200 Corvallis, Oregon 97330 Office 541.360-0500 Fax 541.207.3928
www.nuscalepower.com

ACRS Presentation: Design of the Highly Integrated Protection System Platform Topical Report



Jason Pottorf

Instrumentation & Controls Lead Engineer

February 7, 2017

PM-0217-52652
Revision: 0

NuScale Power™
Template #: 0000-21727-F01 R0

Acknowledgement and Disclaimer

This material is based upon work supported by the Department of Energy under Award Number DE-NE0000633.

Agenda

- Purpose
  - overview of the Design of the Highly Integrated Protection System Platform Topical Report (TR-1015-18653)
- History of NRC interactions
- Highly integrated protection system (HIPS) platform design approach
- Topical report scope
- Representative architecture safety data path
- Prototype
- Summary

Abbreviations

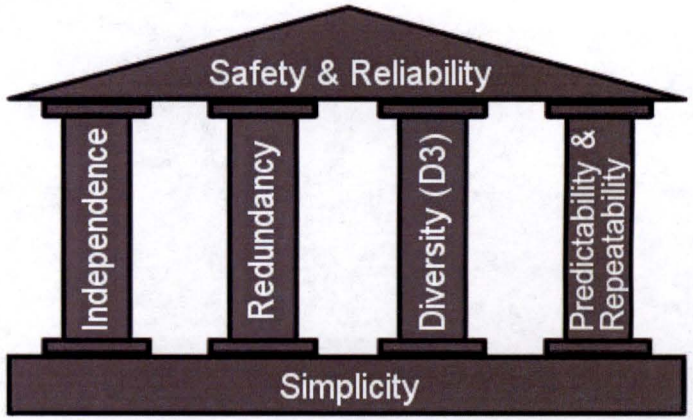
ADC – analog to digital conversion
APL – actuation priority logic
BIST – built-in self-testing
CCF – common cause failure
CM – communication module
CTB – calibration and test bus
D3 – diversity and defense-in-depth
DI&C – digital instrumentation and control
EIM – equipment interface module
ESFAS – engineered safety features actuation system
FAT – factory acceptance testing
FPGA – field programmable gate array
HIPS – highly integrated protection system
HWM – hard-wired module
ISM – input sub-module
MIB – monitoring and indication bus
MIB-CM – MIB communication module
MPS – module protection system
OTP – one time programmable
SBM – scheduling and bypass module
SDB – safety data bus
SDI – safety display and indication
SFM – safety function module
SRAM – static random-access memory
SVM – scheduling and voting module

History of NRC Interactions

- (Pre-submittal) Dec. 1 and 2, 2015 – Closed meeting and NRO ICE site visit to discuss various topics related to the I&C design, including the topical report (Corvallis, OR)
- Dec. 23, 2015 – NuScale submits Rev. 0 of TR-1015-18653, Highly Integrated Protection System (HIPS) Platform Topical Report to the NRC
- Feb. 19, 2016 – NRC acceptance letter issued for review of topical report
- March 24, 2016 – Meeting with NRC staff on HIPS platform details (Rockville, MD)
- April 20, 2016 – Meeting with NRC staff on compliance of HIPS platform design with NRC regulations and IEEE standards (Rockville, MD)
- May 24, 2016 – Meeting with NRC staff to discuss staff's draft RAIs on the HIPS platform topical report (Rockville, MD)
- June 22, 2016 – NRC issues RAIs on the HIPS Platform topical report
- July 6 – 7, 2016 – NRC audit of the HIPS platform prototype design documents (Rockville, MD)
- Aug. 19, 2016 – NuScale submits RAI responses to June 22 NRC RAIs
- Sept. – Oct. 2016 – NuScale and NRC hold teleconference calls on clarifications to RAI responses and follow-up clarification questions from NRC
- Nov. 4, 2016 – NuScale submits Rev. 1 to the HIPS platform topical report to the NRC
- Dec. 15, 2016 – NRO ICE visit to the NuScale Rockville office to review the prototype MPS factory acceptance testing (FAT) test specification and provide feedback ahead of the prototype MPS FAT Test audit
- Jan. 30 – Feb. 3, 2017 – NRC audit of the prototype MPS FAT (Wimborne Minster, UK)

HIPS Platform Design Approach

- The highly integrated protection system (HIPS) is designed to provide a robust platform for safety-related and important-to-safety applications
- Key design concepts incorporate the following fundamental design principles:
  - independence
  - redundancy
  - diversity and defense-in-depth (D3)
  - predictability and repeatability



- Hybrid analog and digital system with field programmable gate array (FPGA) logic on all modules implementing multiple deterministic finite state-machines
- Design concepts support meeting requirements and guidelines for safety-related applications (RG 1.153, IEEE Std. 603, RG 1.152, IEEE Std. 7-4.3.2, DI&C-ISG-04, SECY-93-087)

Topical Report Scope

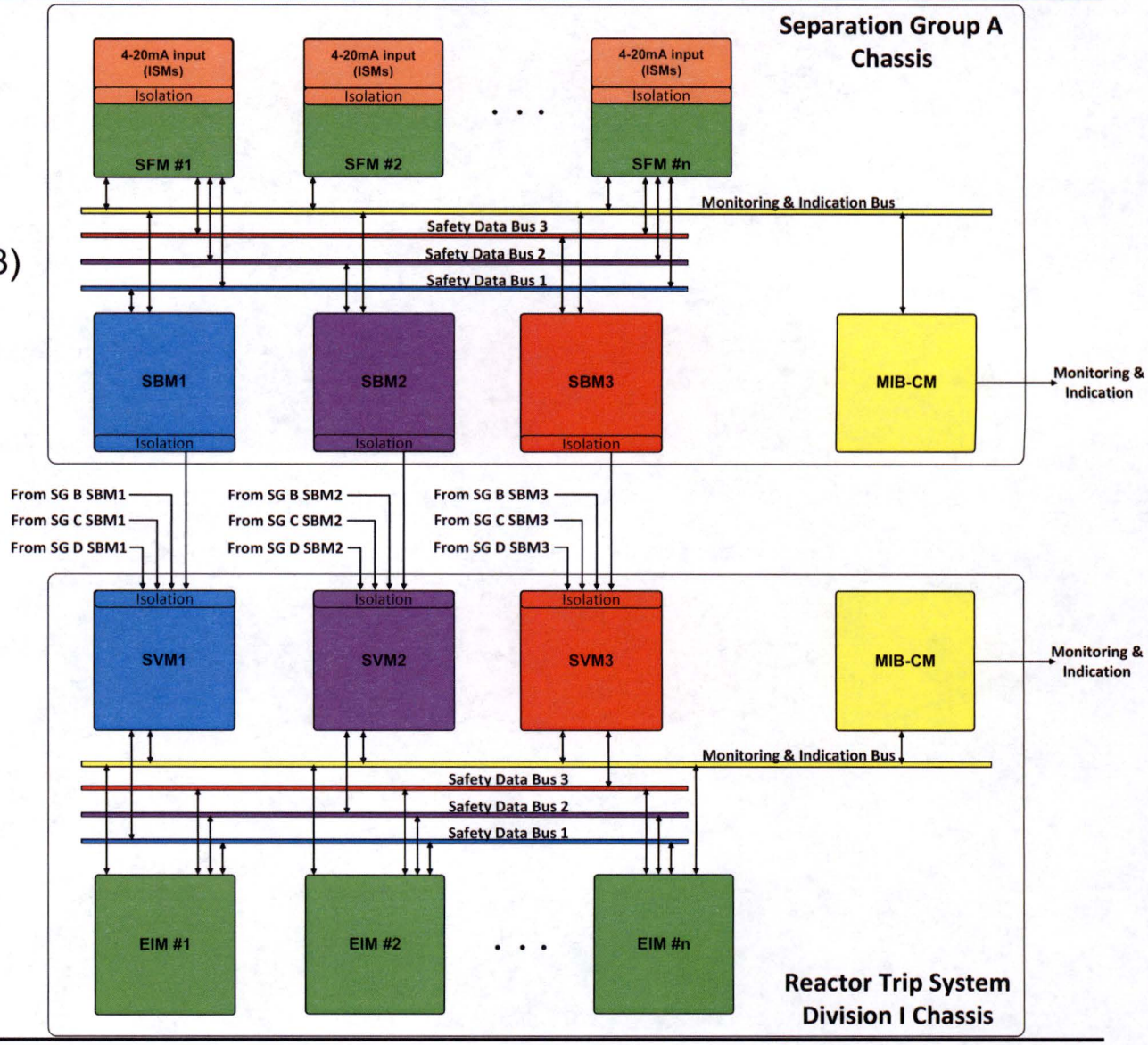
The HIPS platform consists of the HIPS chassis and a system of modules that are interchangeable between chassis

Module Name	Abbreviation	Description/Use
Safety Function Module	SFM	Signal conditioning and actuation determination of safety function(s). Provides scaled value of input process to nonsafety controls and safety display for monitoring purposes (FPGA and analog).
Communications Module	CM	Controls, collects, and transmits information between HIPS modules or to external components (FPGA and analog).
Equipment Interface Module	EIM	Provides final equipment actuation output and includes priority logic circuitry for automatic and manual actuation inputs (FPGA and analog).
Hardwired Module	HWM	Converts hardwired contact inputs into logic levels for direct connection on dedicated backplane traces to a particular module as per the detail application design (analog only).

The HIPS platform is an FPGA-based platform – there is no executable software within the runtime environment

Representative Architecture Safety Data Paths

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



Prototype

- Development of a NuScale prototype module protection system (MPS) began in October 2015 based on the HIPS platform
- Hardware scope includes:
  - two SFMs and four CMs (three SBMs and an MIB-CM) for one separation group of input
  - two EIMs and four CMs (three scheduling and voting modules [SVMs] and an MIB-CM) for one division of engineered safety features actuation system (ESFAS)
- Remaining scope of the MPS simulated with LabVIEW
- Prototype FAT completed February 2, 2017, no issues identified

Summary

- The HIPS platform is based on the fundamental I&C design principles of
  - independence
  - redundancy
  - diversity and defense-in-depth
  - predictability and repeatability
- The HIPS platform was developed to provide a simple and reliable solution for nuclear power plant I&C applications which support meeting the guidelines and the requirements of the NRC's regulatory guides and IEEE standards applicable to safety-related and important-to-safety applications
- The HIPS platform is based upon FPGA technology which has been previously approved by the NRC for safety-related applications
- The licensing topical report (LTR) demonstrates how the HIPS platform key design concepts meet the fundamental I&C design principles
- The LTR also describes testing and diagnostic concepts and how the key design concepts are implemented to achieve overall simplicity

NuScale Power™

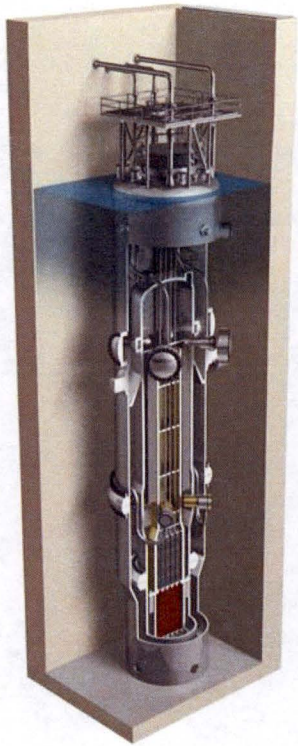
6650 SW Redwood Lane, Suite 210
Portland, OR 97224
503.715.2222

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

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

1933 Jadwin Ave., Suite 205
Richland, WA 99354

http://www.nuscalepower.com



Supplemental Slides

Independence

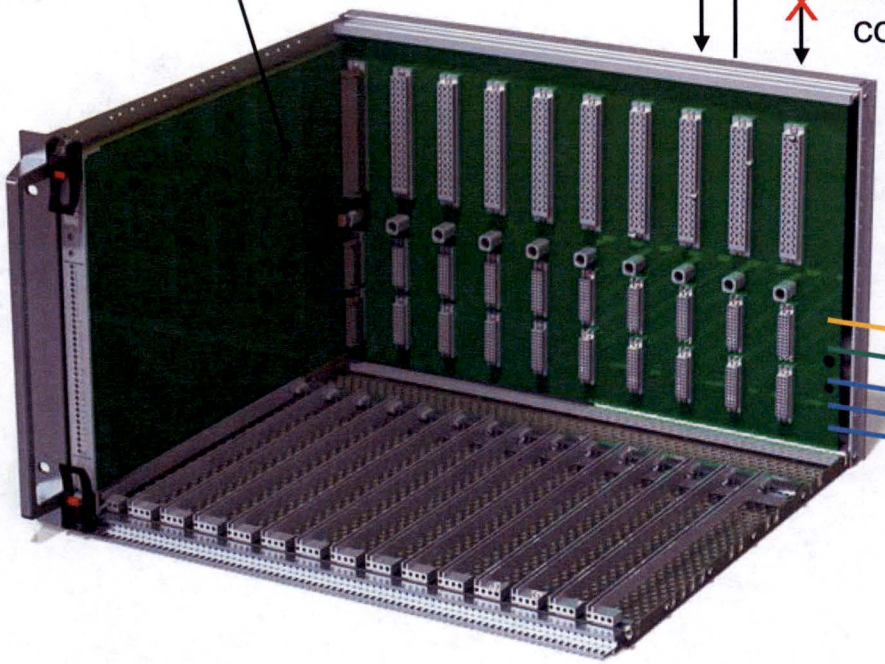
- All HIPS modules operate independently and asynchronously
- SFM independence features
  - galvanic isolation between different inputs (ISMs) on an SFM
  - functional independence of each SFM (unique FPGA images)
  - functional logic for the safety data paths, monitoring, and calibration/testing are independent from each other
  - optocoupler isolation between FPGA and input signals
- CM independence features
  - only one-way isolated communications allowed for interdivisional communications or communications outside of the platform
- EIM independence features
  - actuation priority logic (APL) is composed of discrete components independent of the FPGA logic
  - manual actuation and nonsafety inputs connect directly to the APL (isolation via HWM and not input to FPGA)
  - all inputs and outputs are individually isolated from EIM discrete logic circuitry

Independence (continued)

FPGA logic on any module cannot be modified while installed in a chassis

All interdivisional data communication is through one-way isolated fiber optic ports on the CMs

Bidirectional interdivisional data communication is not allowed



Separate and dedicated communications logic for each data bus within a chassis

No capability for remote access to the system

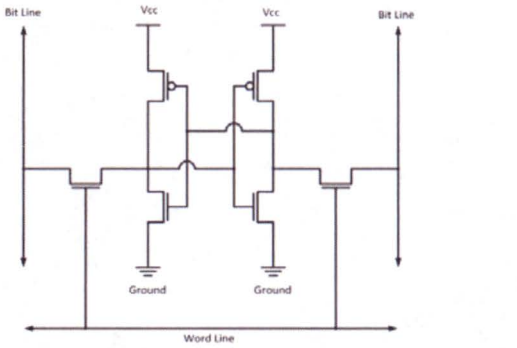
Redundancy

- Specific system architecture must be evaluated separately to confirm it meets the single failure criterion
- HIPS platform internal redundancy
  - redundant power supply feeds to all HIPS modules
  - triple redundant safety data paths allow for communication error detection and limits a fault to a single bus without compromising safety actuations
  - loss or removal of a CM generates an alarm but does not result in trip or actuation of the end device
  - redundant safety data communications and EIM configuration allows for online maintenance (hot swapping of modules)
  - internal redundancy results in simplified self-testing circuitry

Diversity

- Equipment diversity
  - the FPGA portion of an SFM, CM, and EIM is the only portion of the HIPS platform vulnerable to software logic-based common cause failures (CCFs)
  - the HIPS platform requires at least two different FPGA architectures (one time programmable [OTP] or flash-based and static random-access memory [SRAM-based])
- Design diversity
  - intentional differences are required in the software tools used for FPGA development

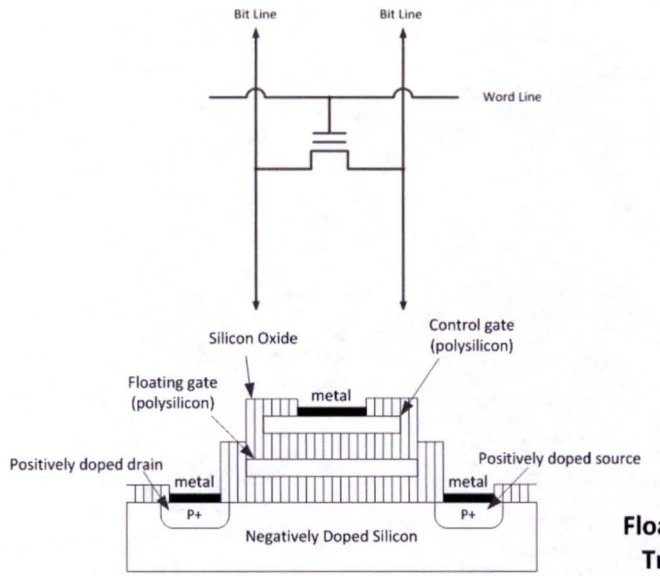
SRAM Cell



Standard MOSFET Transistor

PMOS transistor is shown. NMOS transistor would have positively doped silicon with negatively doped supply and drain

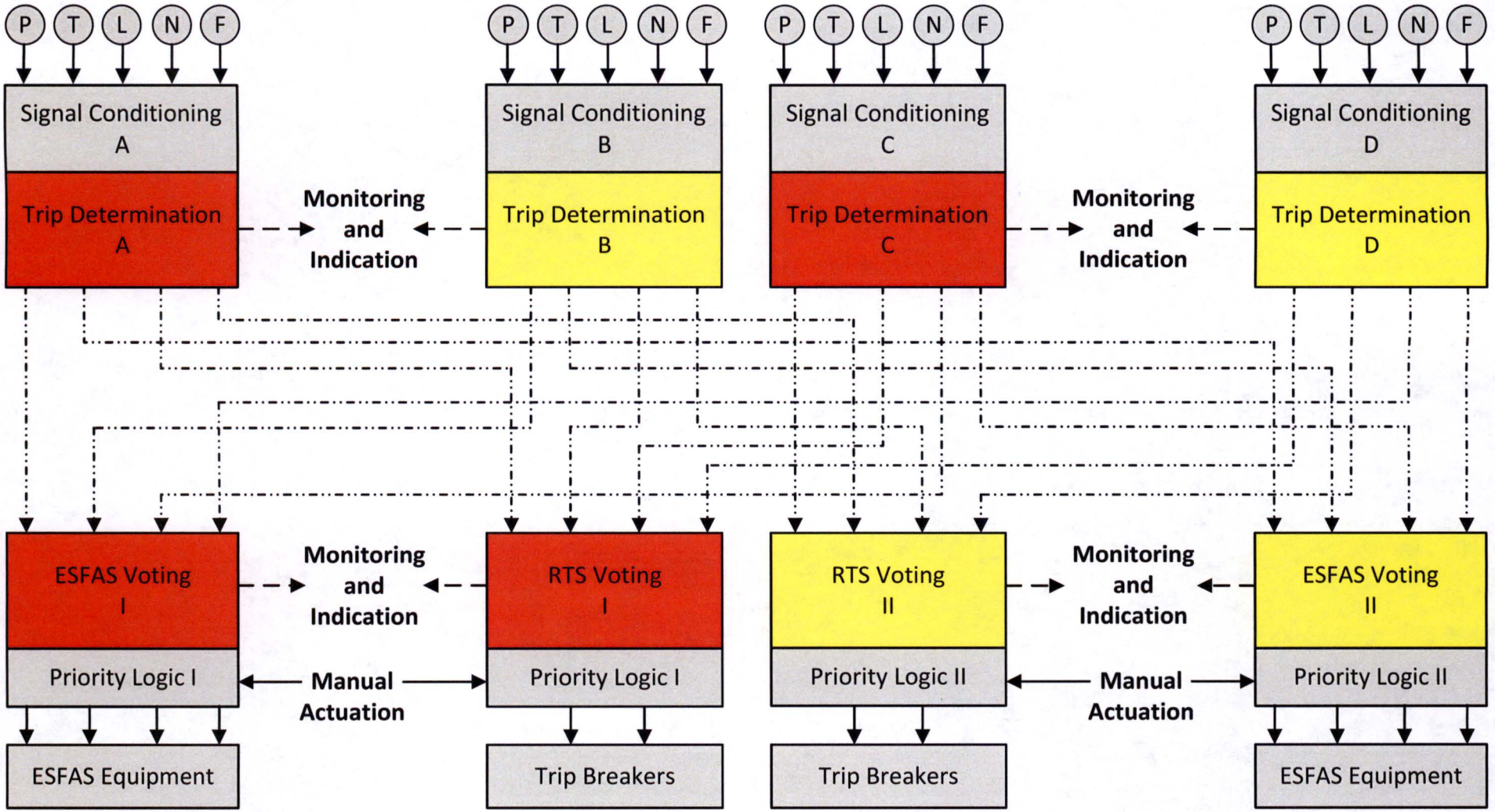
Flash Cell



Floating Gate Transistor

Can have positively doped silicon with negatively doped supply and drain

Diversity (continued)

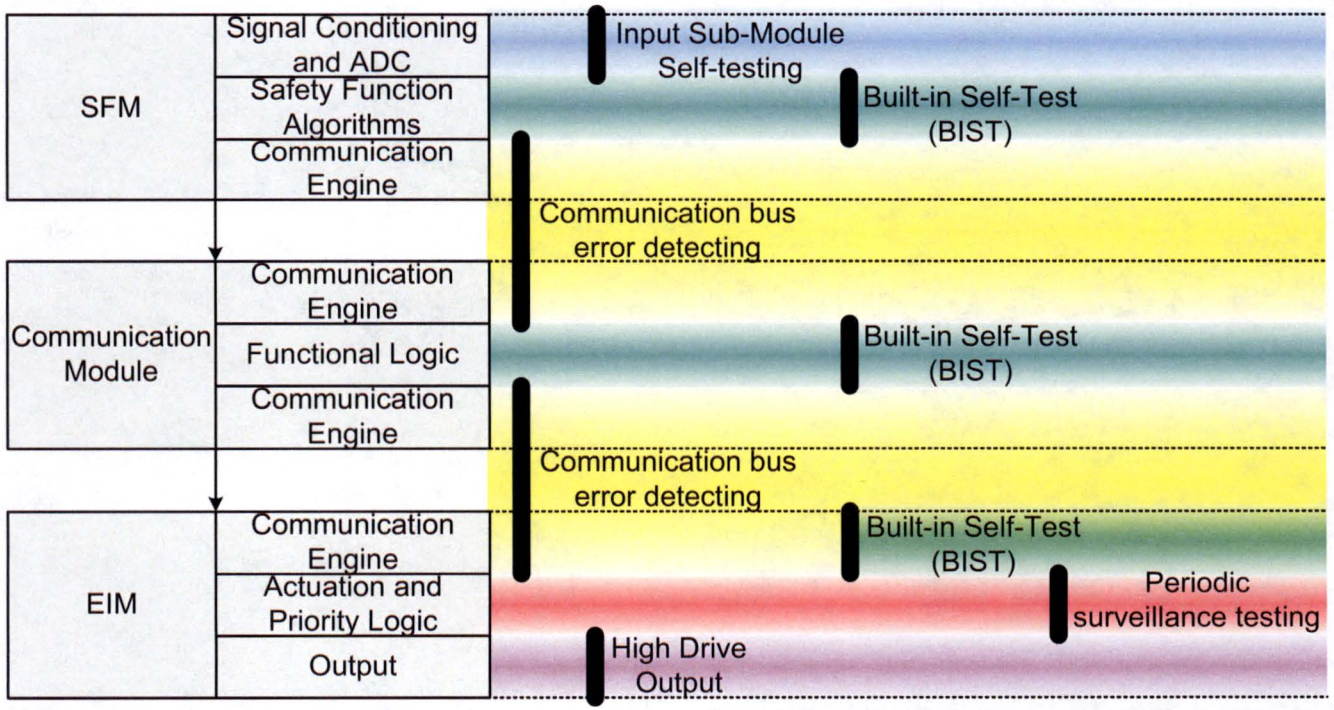


Predictability and Repeatability

- A single clock base is used for logic performed on each module's FPGA as well as being used to derive the safety data bus (SDB) bit frequency and sampling bits on the communication buses
- Safety functions are processed by three redundant sets of dedicated logic to provide error detection and fault tolerance
- Intradivisional communications within a chassis are implemented with a master-slave communication protocol using simple differential RS-485 virtual point-to-point or multi-drop bus communication
- Master and slave modules communicate asynchronously
- All SDB communication transactions have identical duration

Calibration, Testing, and Diagnostics

- In-chassis calibration of set points/tunable parameters can be performed for the SFM when the SFM is taken out of service; all other modules are either unable to be changed or only capable of changes when removed from the chassis
- All components, except the discrete APL of the EIM, have self-testing capabilities to ensure the information transmitted to the next step in the safety data path are correct
- Each module ensures that it is functioning correctly and the error checking on the communication buses ensure correct transfer of data



Simplicity

- There is no executable software within the HIPS platform runtime environment
- Each module functions autonomously on its own single clock domain
- Inherent SFM independence results in simpler trip determination logic
- Use of triple module redundancy within a division provides simpler self-testing schemes and maintenance, and also improves availability
- FPGA functions implemented with finite states machines to achieve deterministic behavior
- Deterministic behavior allows use of a simple communication protocol using predefined message structure with fixed time intervals
- Asynchronous communication avoids complex synchronization techniques