ROCK CREEK
INNOVATIONS, LLC

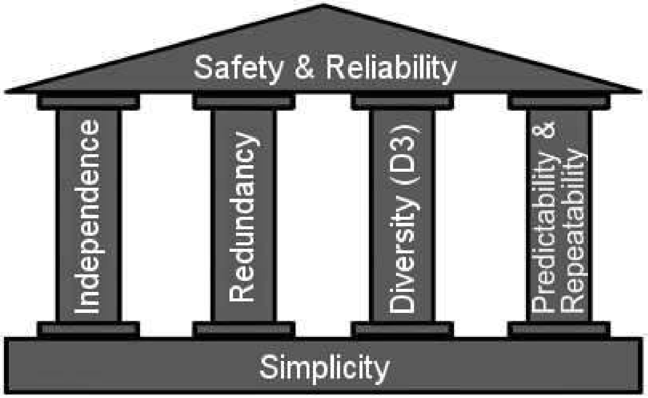
HIPS
highly integrated protection system

# Diversity within the Highly Integrated Protection System (HIPS)

Jason Pottorf
October 11th, 2018

# 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

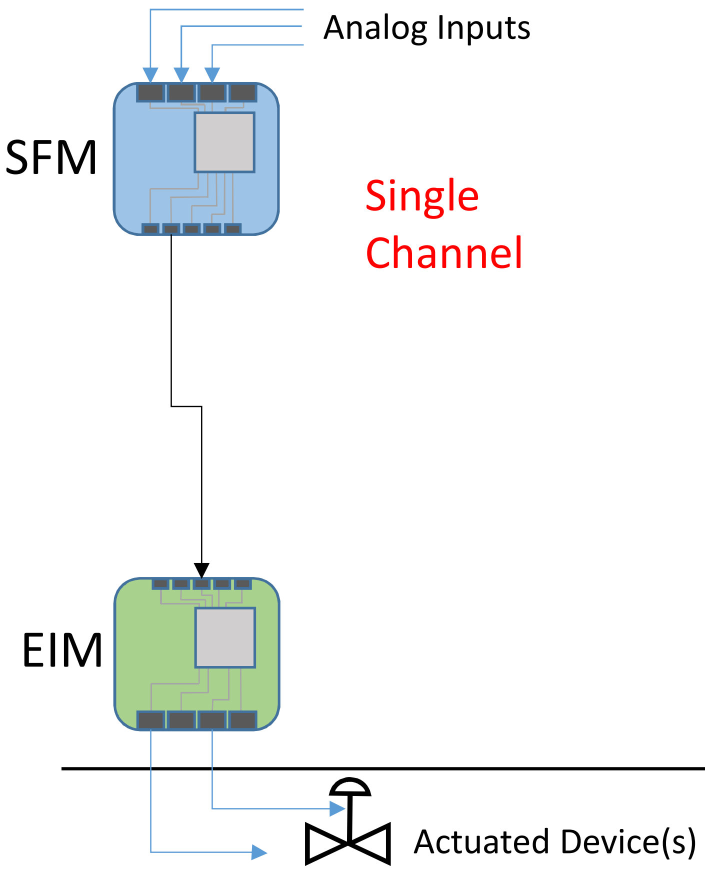


- Hybrid analog and digital system with field programmable gate array (FPGA) logic on modules implementing multiple deterministic finite state-machines
- Design concepts support meeting requirements and guidelines for safety-related applications (RG 1.153, IEEE Std. 603, RG 1.152, IEEE Std. 7-4.3.2,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

# Scalable HIPS Architecture

Main HIPS platform modules include

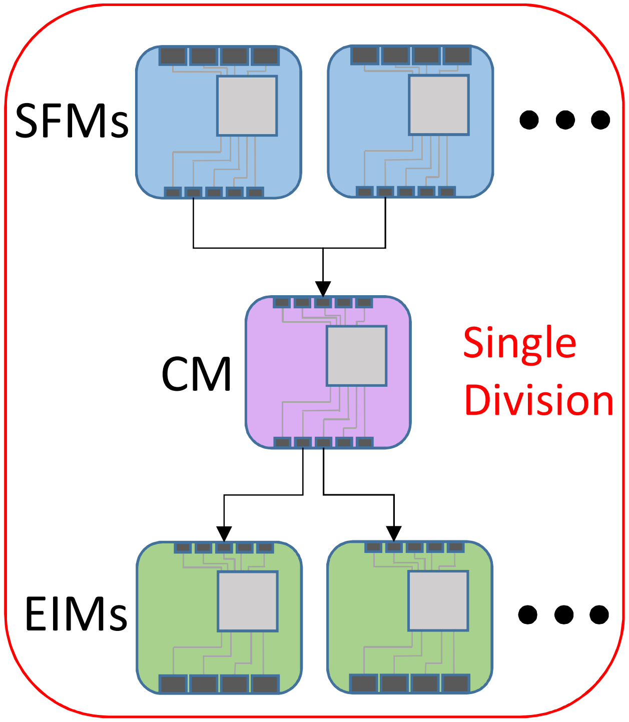
- Safety Function Module (SFM)
- Communication Module (CM)
- Equipment Interface Module (EIM)



# Scalable HIPS Architecture

Main HIPS platform modules include

- Safety Function Module (SFM)
- Communication Module (CM)
- Equipment Interface Module (EIM)

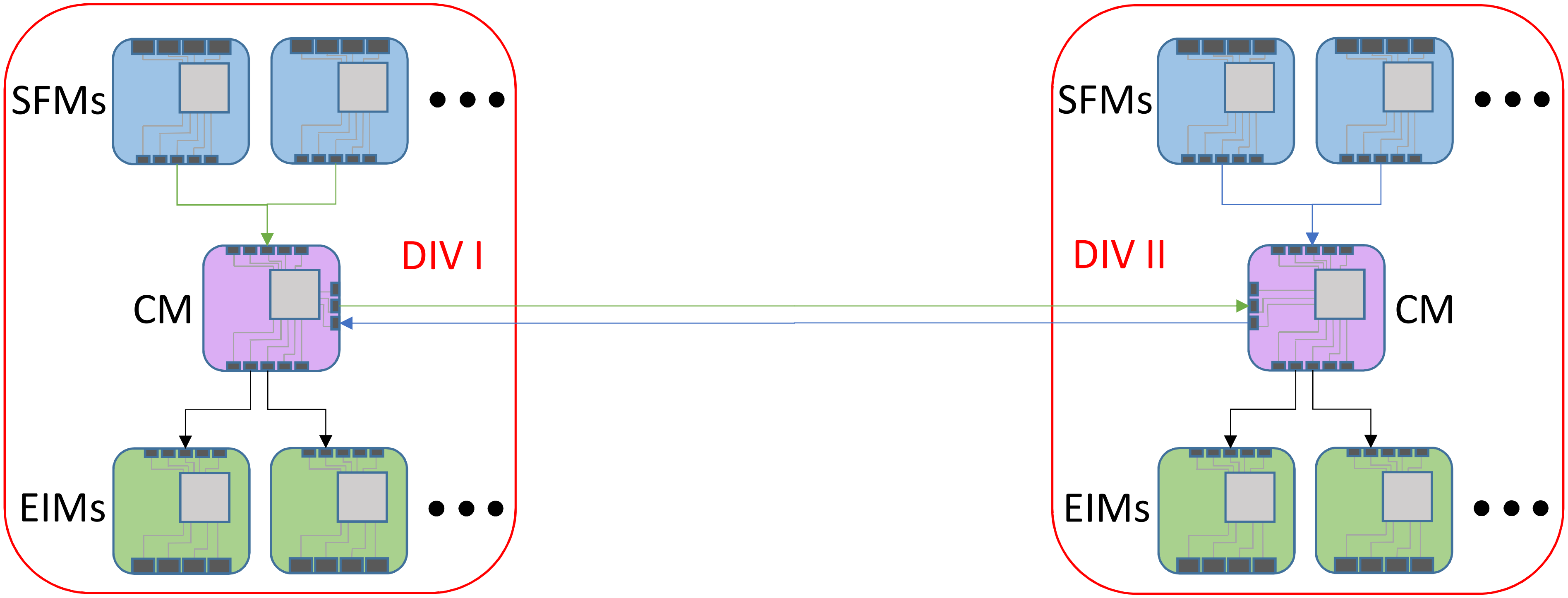


# Scalable HIPS Architecture

Main HIPS platform modules include

- Safety Function Module (SFM)
- Communication Module (CM)
- Equipment Interface Module (EIM)

Two Divisions of Input and Actuation



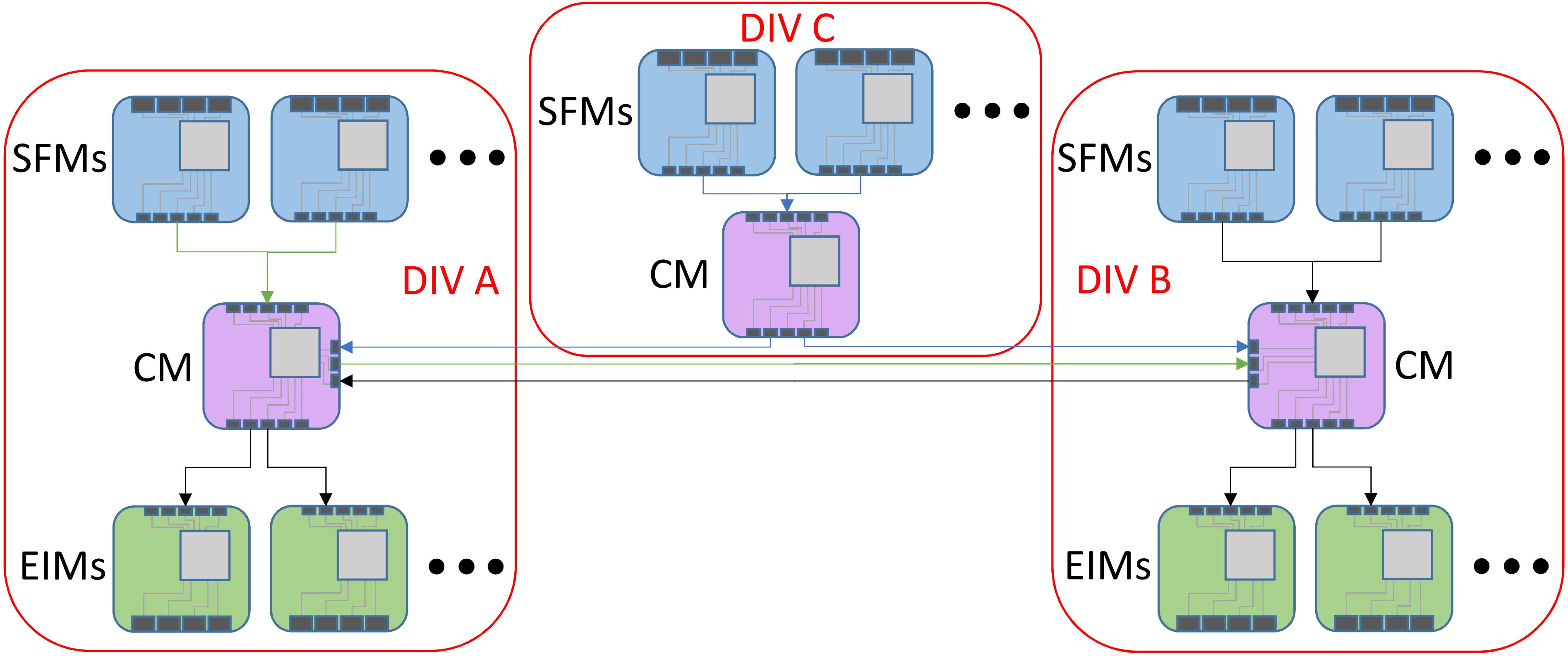
2018 Rock Creek Innovations, LLC

# Scalable HIPS Architecture

Main HIPS platform modules include

- Safety Function Module (SFM)
- Communication Module (CM)
- Equipment Interface Module (EIM)

Three Groups of Input with Two Divisions of Actuation



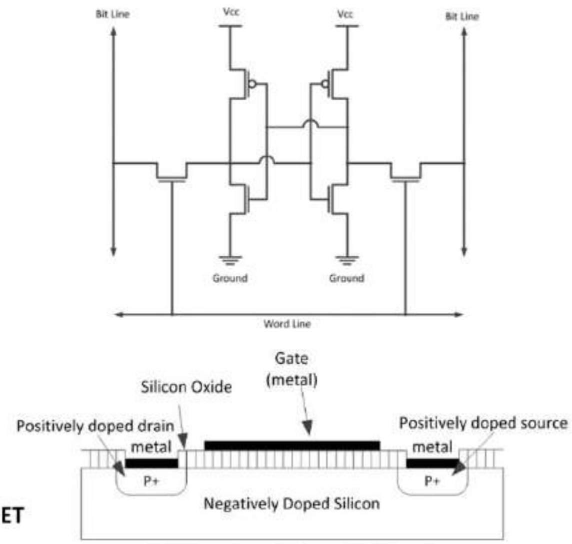
# HIPS Diversity Attributes

- Software CCFs must be addressed and there are two primary strategies:
  - Quality Assurance Processes
  - Diversity*
- Types of diversity addressed with the HIPS platform:
  - Equipment
  - Design
  - Human
  - Functional
    - Logic
    - Hardware

# Equipment Diversity

- The FPGA portion of a HIPS module 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])
- Inherent differences include physical architecture, logic storage cell, power off characteristics, chip configuration

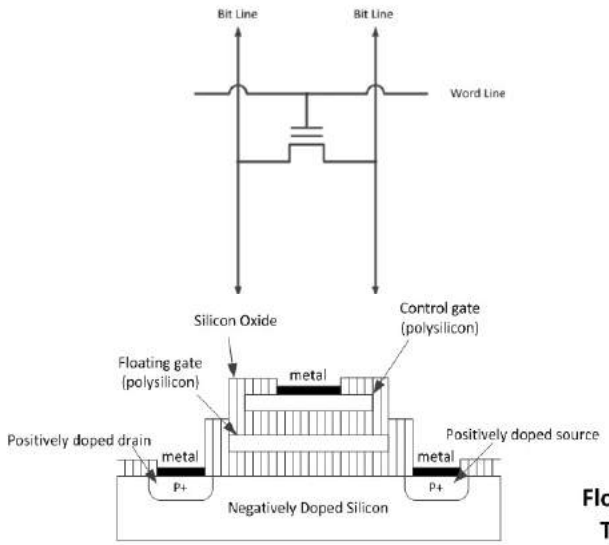
**SRAM Cell**



**Standard MOSFET Transistor**

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

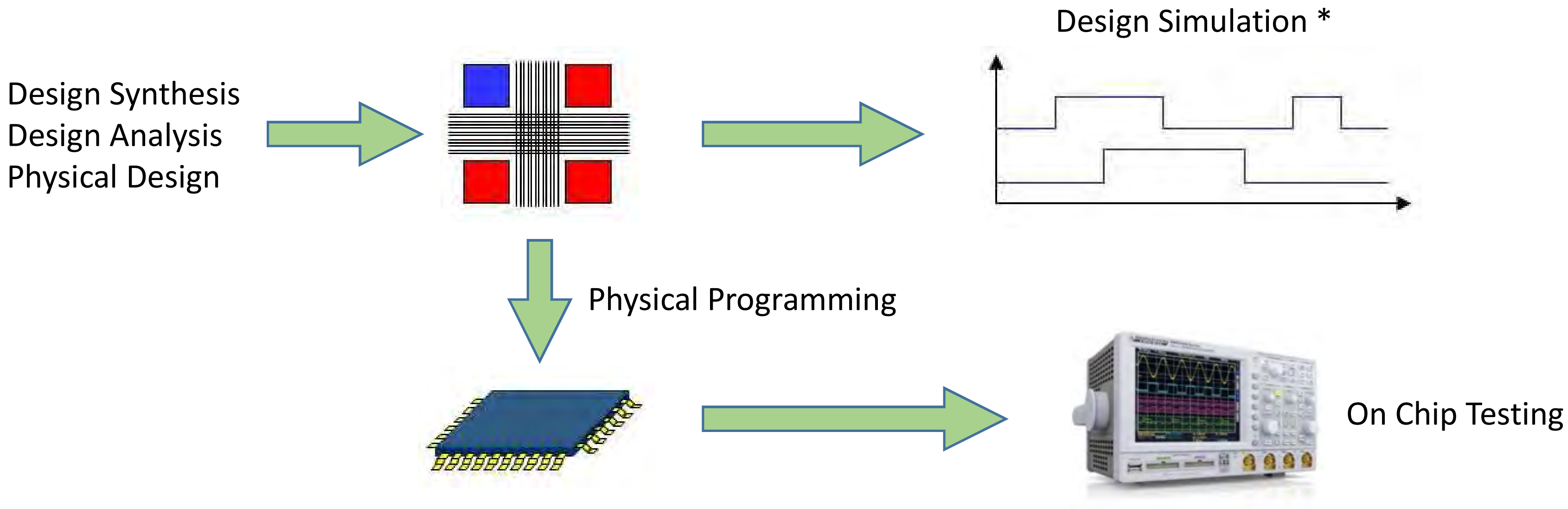
**Flash Cell**



**Floating Gate Transistor**

Can have positively doped silicon with negatively doped supply and drain

# Design Process Diversity



Design Synthesis
Design Analysis
Physical Design

Design Simulation *

Physical Programming

On Chip Testing

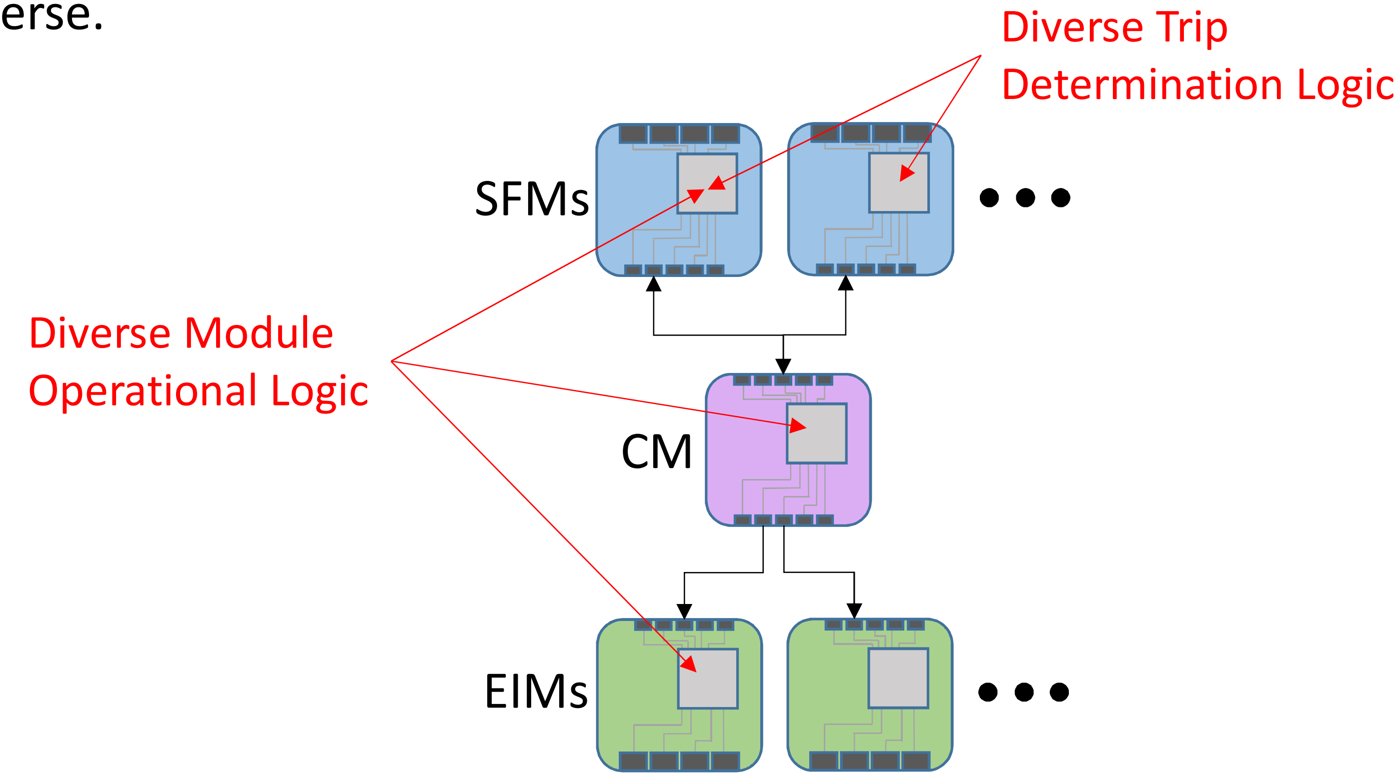
| Differences | Diversity Type | FPGA #1 | | FPGA #2 |
|---|---|---|---|---|
| | | OTP | Flash FPGA | SRAM FPGA |
| Design Synthesis Tool(s) | Intentional | Tool Suite A | Tool Suite A | Tool Suite B |
| Design Analysis Tool(s) | Intentional | | | |
| Physical Design Tool(s) | Intentional | | | |
| Design Simulation Tool(s) | Intentional | | | |
| Physical Programming Tool(s) | Intentional | | | |
| iV&V Design Simulation Tool(s)* | Intentional | Tool Suite Different than Suite A and Suite B | | |

# Human Diversity

- The approved HIPS platform does not require a diverse design development team
  - MIT hazards analysis: *“almost all serious accidents caused by software have involved errors in the requirements, not in the implementation of those requirements in software code.”*
  - Nat’l Research Council study conclusion: *“use of different programming languages, different design approaches meeting the same functional requirements, different design teams, or different vendors’ equipment used to perform the same function is not likely to be effective in achieving diversity.”*
- Different FPGA development paths begin from a single implementation-neutral requirements specification
- Human diversity is an implicit attribute of the FPGA equipment, chip design, and software tool diversity; however, it is not explicitly defined nor verified in the HIPS platform diversity strategy

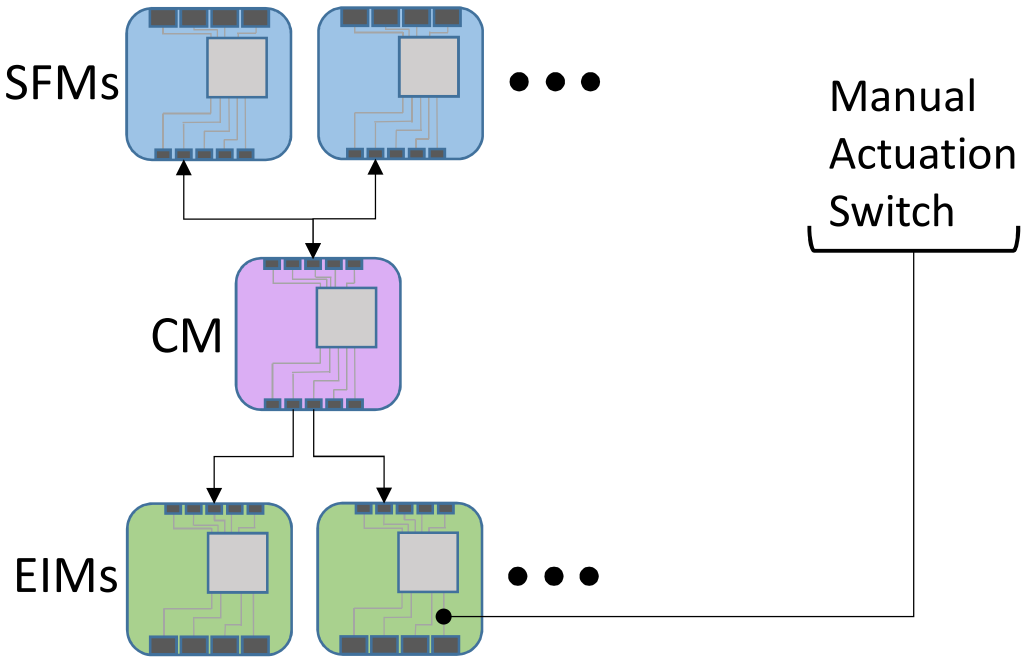
# Functional Diversity (Logic)

- The HIPS platform architecture supports functional diversity by requiring segregation of safety functions by their inputs
- The logic implemented within an SFM is unique to its input(s)
- The safety functions of the different HIPS modules are also functionally unique/diverse.

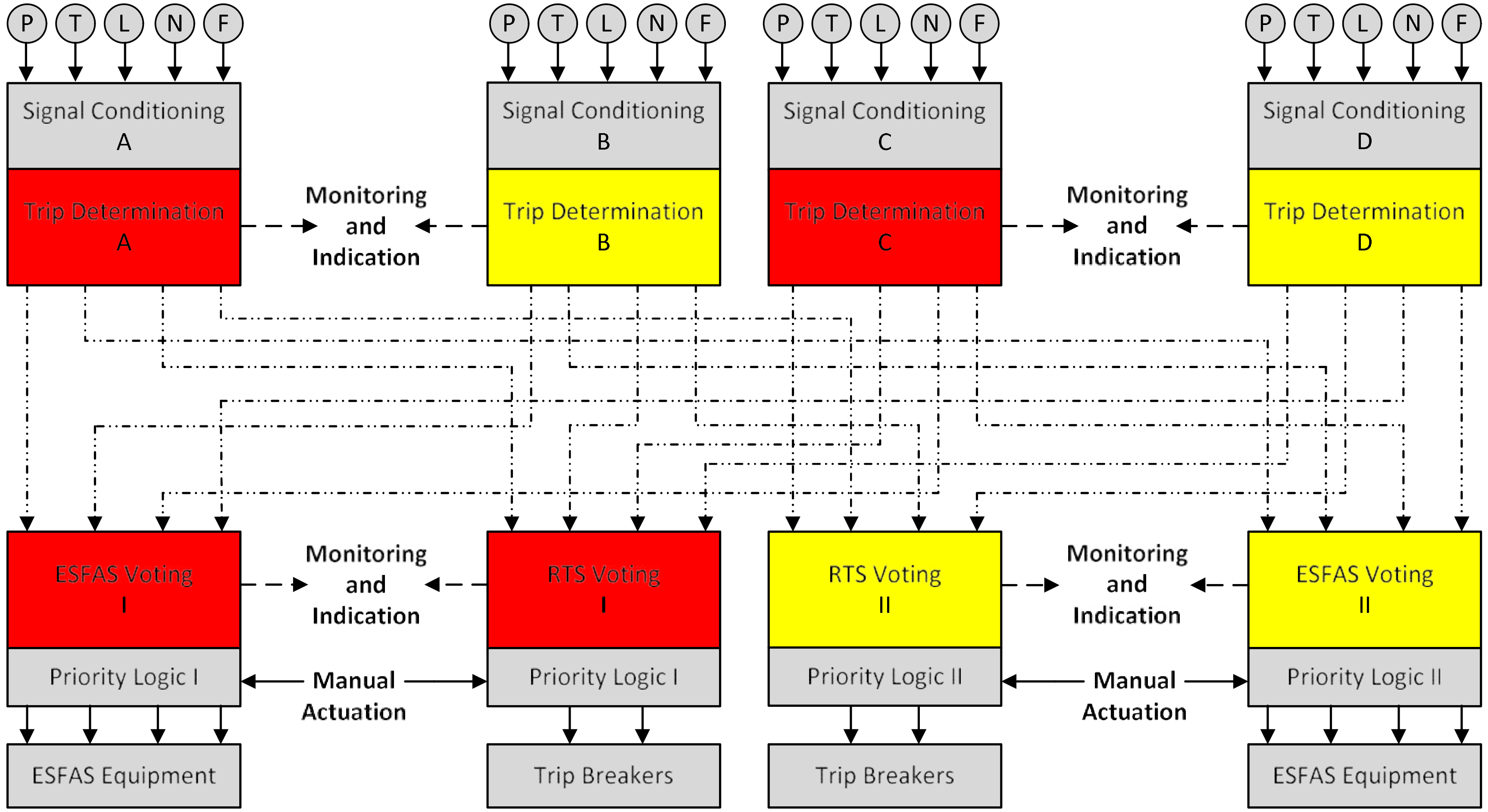

Diverse Trip Determination Logic
SFMs
• • •
Diverse Module Operational Logic
CM
EIMs
• • •

# Functional Diversity (Digital vs Analog)

- Actuation priority logic of the HIPS platform is implemented using discrete components not vulnerable to software CCF
  - Diverse means of actuation that is downstream of the digital portions of the system
  - Different response time scales

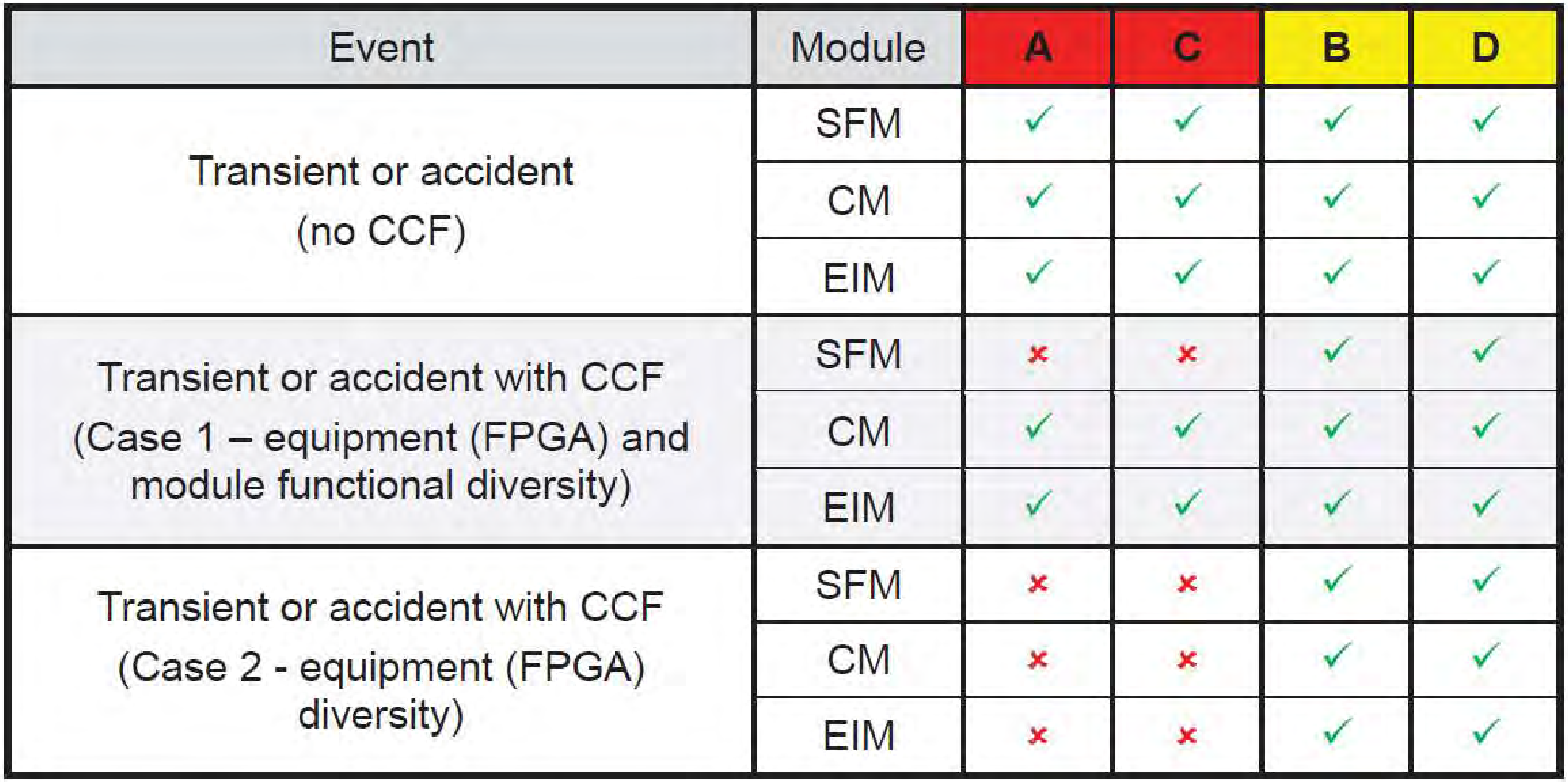


# Diversity Applied



🟥 — FPGA Type #1    🟨 — FPGA Type #2

# Failure Example



| Event | Module | A | C | B | D |
|---|---|---|---|---|---|
| Transient or accident (no CCF) | SFM | ✓ | ✓ | ✓ | ✓ |
| | CM | ✓ | ✓ | ✓ | ✓ |
| | EIM | ✓ | ✓ | ✓ | ✓ |
| Transient or accident with CCF (Case 1 – equipment (FPGA) and module functional diversity) | SFM | ✗ | ✗ | ✓ | ✓ |
| | CM | ✓ | ✓ | ✓ | ✓ |
| | EIM | ✓ | ✓ | ✓ | ✓ |
| Transient or accident with CCF (Case 2 - equipment (FPGA) diversity) | SFM | ✗ | ✗ | ✓ | ✓ |
| | CM | ✗ | ✗ | ✓ | ✓ |
| | EIM | ✗ | ✗ | ✓ | ✓ |

# Summary

- The HIPS platform design includes inherent attributes that are simple and cost effective to address the challenge of software common cause failure.
- Simple approach to diversity supports a more clear path to regulatory approval
- The inherent diversity of the HIPS platform can eliminate the need for extra systems (diverse protection or actuation systems).
- Reduces plant system complexity and associated design and maintenance costs

# Questions???