12th International Workshop on the Application of FPGAs in Nuclear Power Plants

Licensing History and Common Cause Failure Mitigation for FPGA Based Systems in the US Market

Sean Kelley
Chief Operating Officer

October 8-11, 2019
Budapest, Hungary

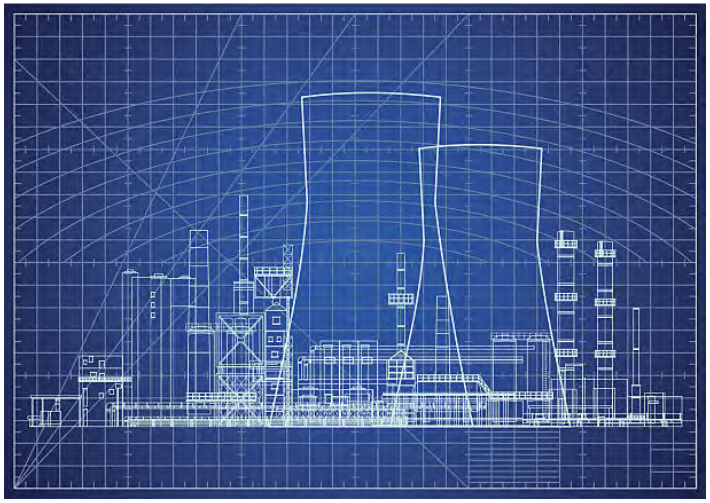
Sunport
Connecting Forward

Sunport

Purpose

Discuss various innovative FPGA-based platforms and devices approved for use in U.S.

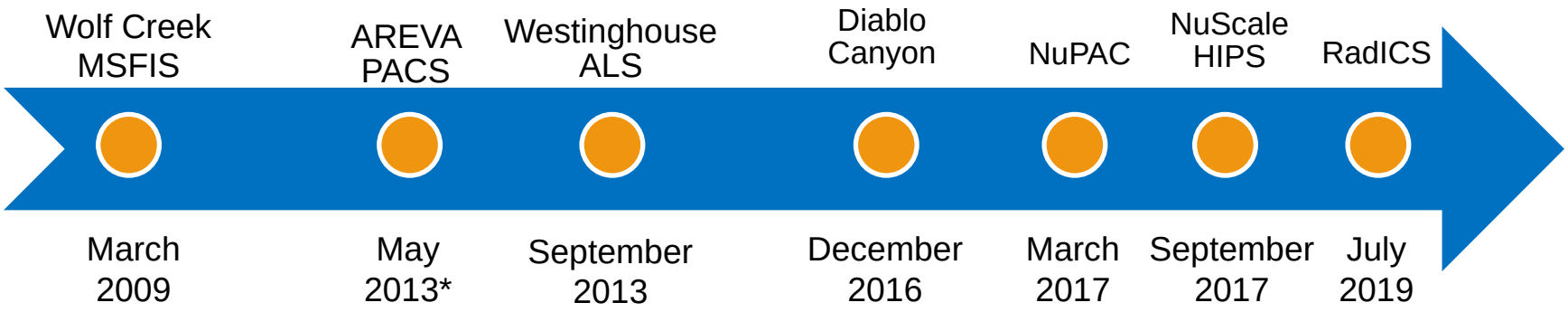
- **Background**
- **Approach to Common Cause Failure (CCF) Mitigation**



Sunport

The Journey

Path blazed by innovators, with the support and guidance from the regulator



* Date of Submittal – Never Approved

Sunport

Wolf Creek MSFIS 1/3

- **Background**
  - First US Safety Related FPGA based application (Approval March 2009)
  - Application specific Wolf Creek Generating Station MSFIS
  - Originally proposed as a hardware only digital solution (i.e., not a software based digital solution) in 2008
  - NRC requested additional review including verification and validation documents
  - Precedent set - FPGA based systems reviewed against SW development standards

Sunport

Wolf Creek MSFIS 2/3

- **Approach to CCF Mitigation**
  - FPGAs with diverse logic core - independently computes parallel application specific logic
  - Differing Synthesis directives implement diverse logic paths
  - Diverse logic for platform functions and self testing
  - Parallel computing logics mismatch deemed a failure and sets outputs to safe state

Sunport

Wolf Creek MSFIS 3/3

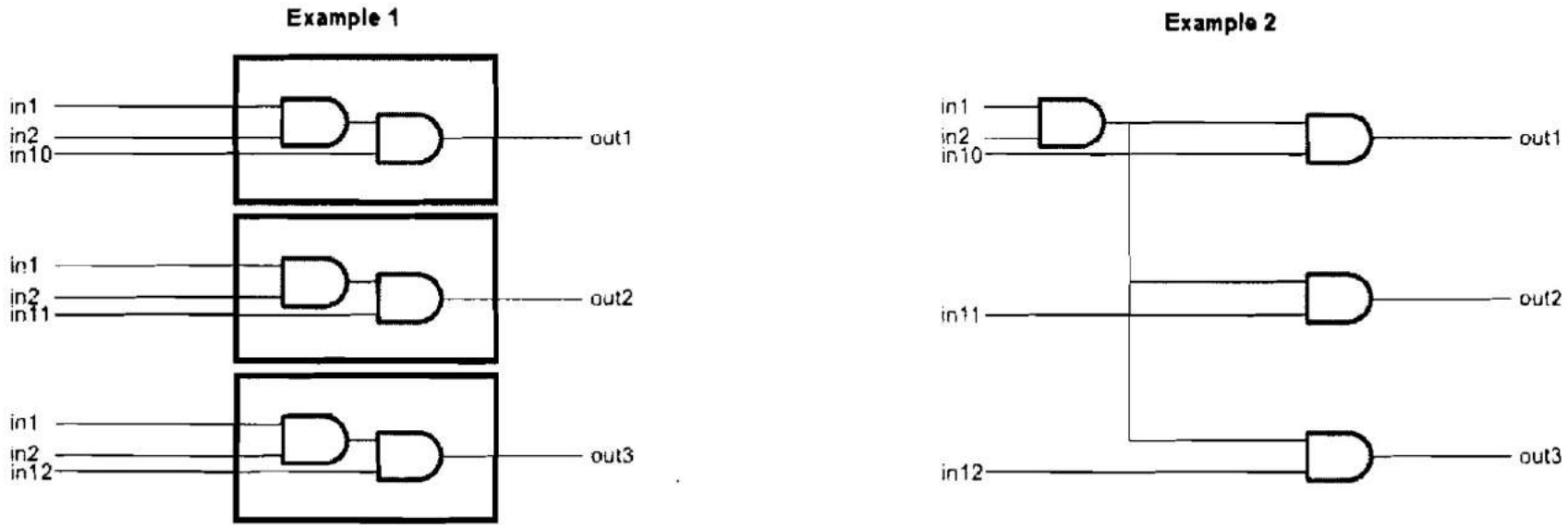


Figure 9 - Example of Diverse Logic Implementation

NRC determined sufficient diversity, due to low level of complexity and IV&V detailed review of core logics

Sunport

AREVA PACS 1/3

- **Background**
  - Priority Actuation modules integrate Safety/Non-Safety for actuator control and monitoring
  - Intended for U.S. EPR new build (Submittal in May 2013)
  - Utilized two separate modules: a safety-related priority module and non-safety-related communication module (micro-processor based)
  - Both modules qualified to same safety-related requirements

Sunport

AREVA PACS 2/3

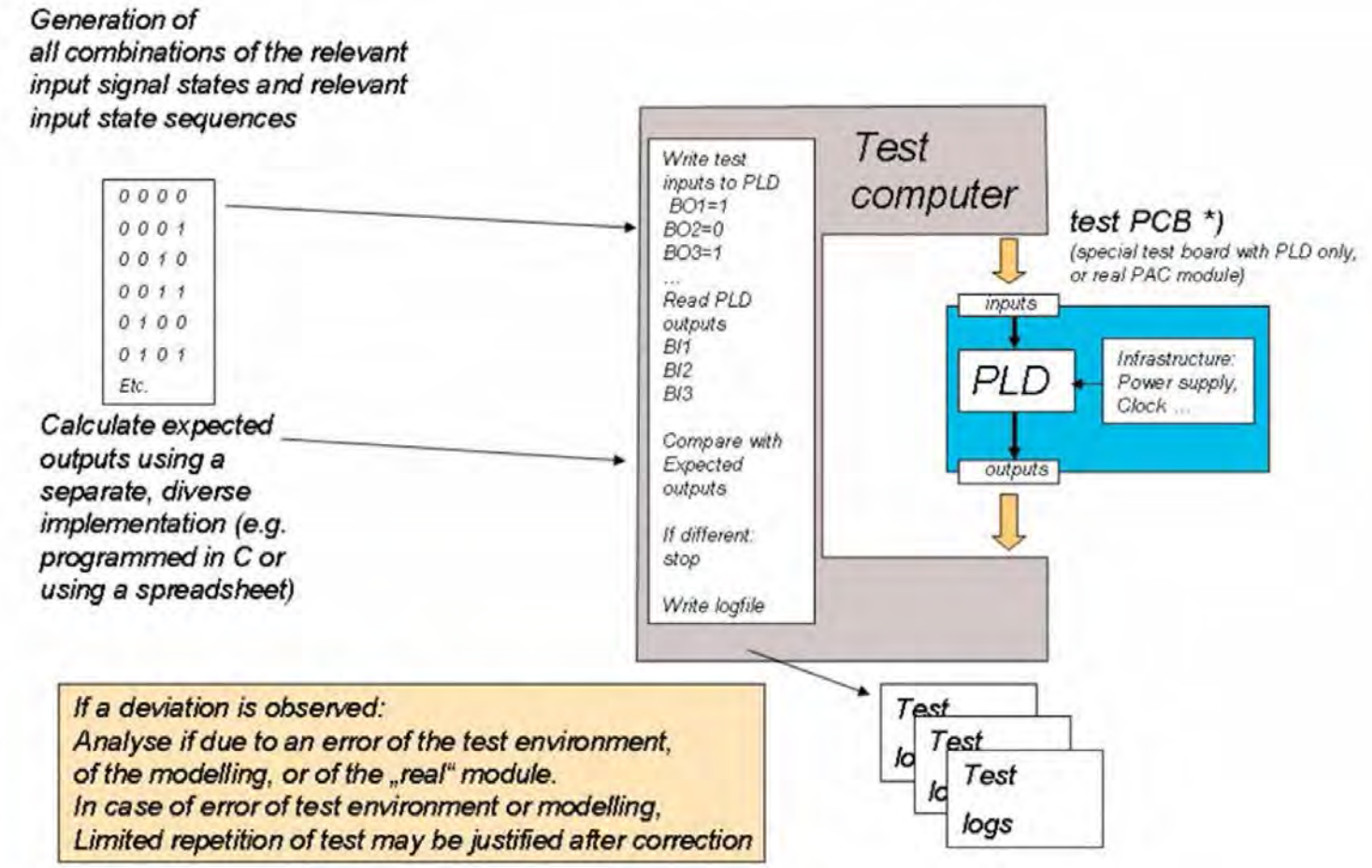
- **Approach to CCF Mitigation**
  - 100% combinatorial testing
  - IEEE 7-4.3.2-2003 and D&IC-ISG-04 supports 100% testing methodology for CCF mitigation
  - Achievable only for simple devices/applications
  - NRC review not completed due to ending of U.S. EPR licensing efforts

Although licensing process not completed, NRC appeared to be on a path for approval

Sunport

AREVA PACS 3/3

Overall Test Concept



Sunport

Westinghouse ALS 1/5

- **Background**
  - Westinghouse ALS CS Innovations technology advancement to a generic platform approval (September 2013)
  - Evolution of development method, architecture, board suite, and communication interfaces used in the Wolf Creek MSFIS ALS application
  - Diablo Canyon utilized in hybrid system replacing Eagle 21 digital PPS with a new digital PPS based on two platform, a PLC and Westinghouse ALS FPGA system

Sunport

Westinghouse ALS 2/5

- **Approach to CCF Mitigation**
  - Added built-in design diversity beyond CS Innovations technology
  - “Core Diversity Design” - two redundant logic implementations within each FPGA (Core 1 and Core 2)
  - Different synthesis directives for each logic implementation
  - Core outputs combined in a hardwired “OR” ensuring protective action if either path commands actuation

NRC determined platform level diversity alone was not enough and required application-specific diversity reviews

Sunport

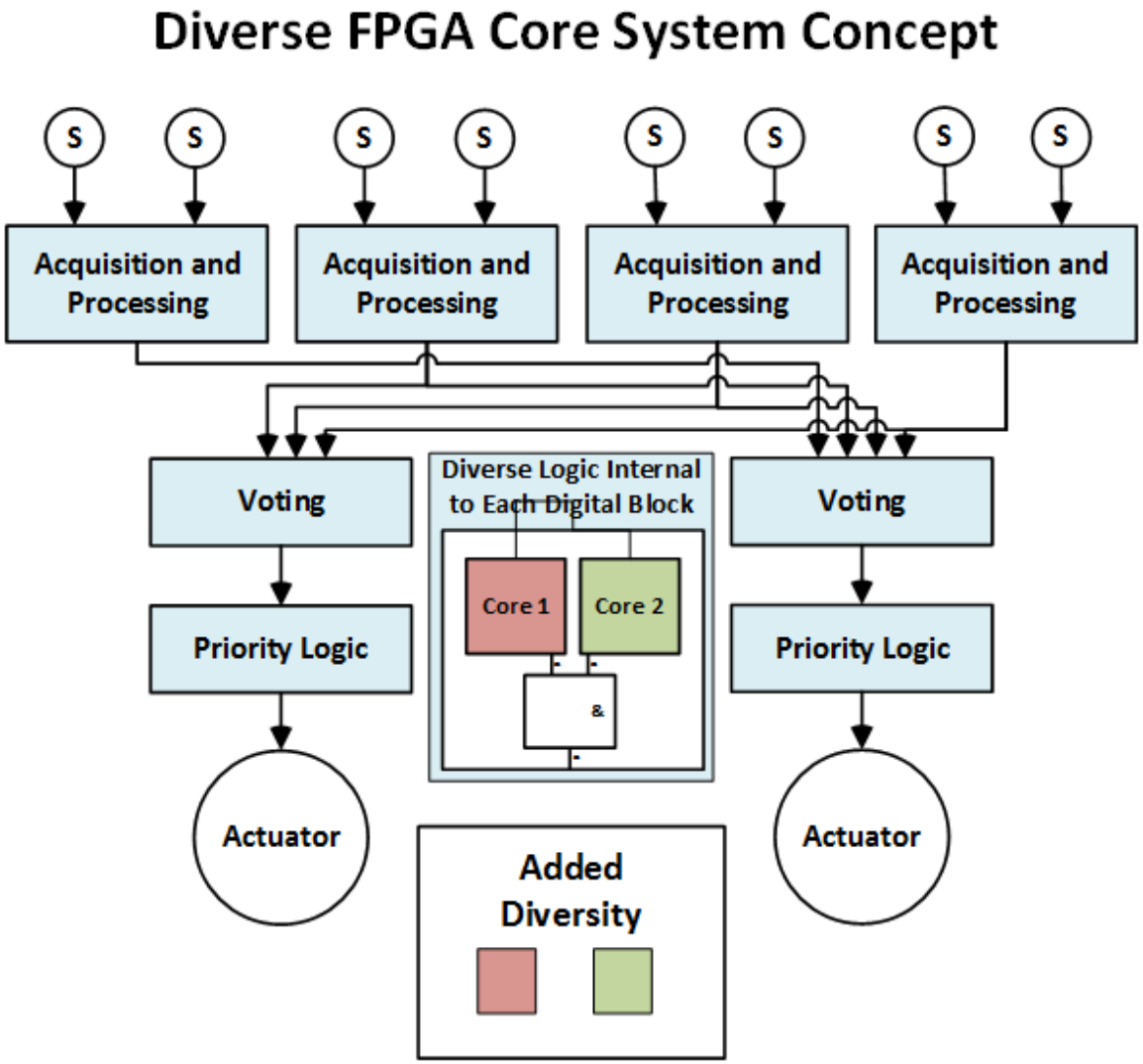
Westinghouse ALS 3/5

- **Approach to CCF Mitigation (cont.)**
  - "Embedded Design Diversity" - "Option" for additional diversity
  - Requires two versions of hardware descriptive language files
  - Independent design teams utilized to implement
  - Implementing and maintaining independent design teams can prove costly and add organizational complexity

"Embedded Design Diversity" is an application level decision NRC determined project specific reviews are needed

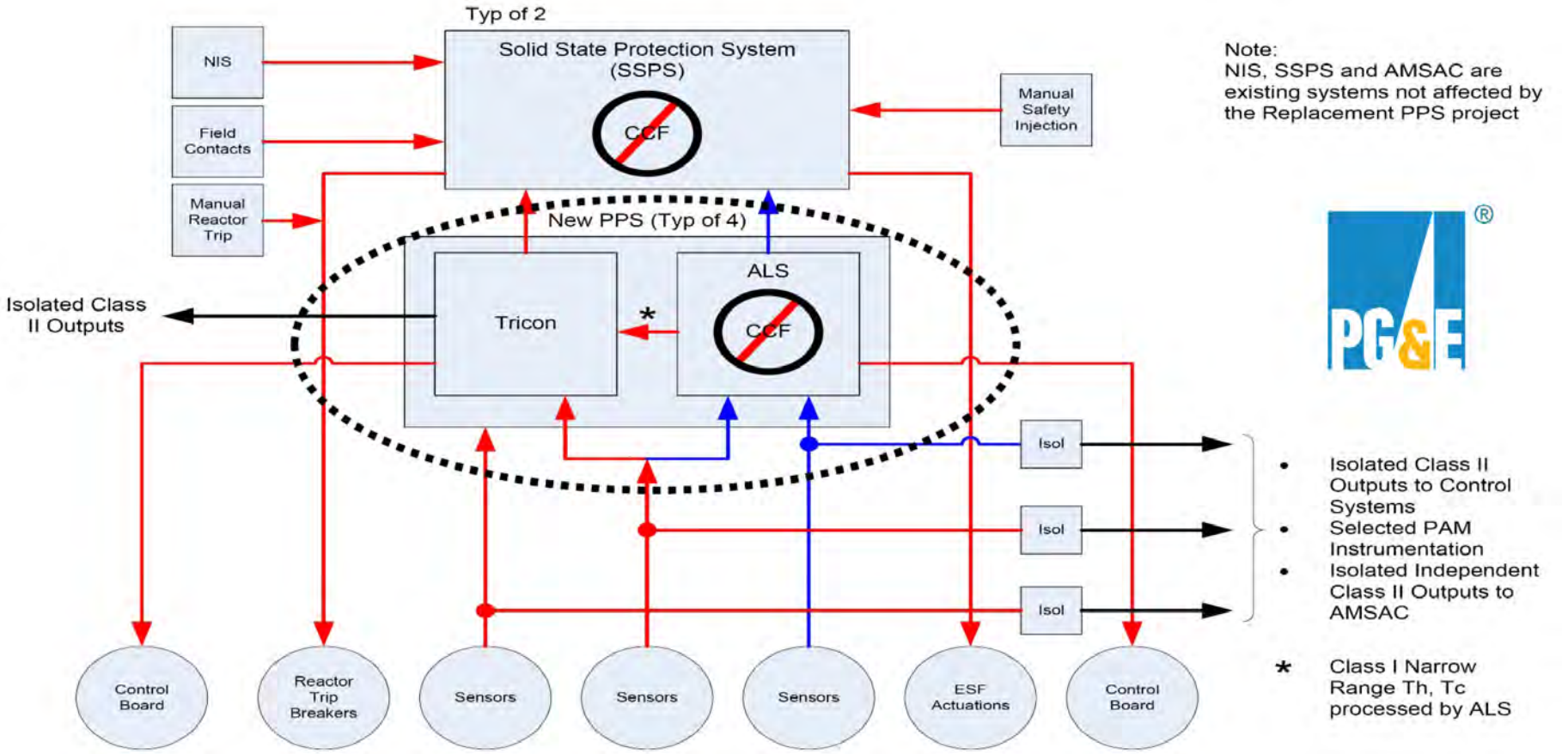
Sunport

Westinghouse ALS 4/5



Sunport

Westinghouse ALS 5/5



Sunport

Lockheed Martin NuPAC 1/2

- **Background**
  - Lockheed Martin Global, Inc. and State Nuclear Power Automation System (SNPAS) Engineering Company collaboration (Approval March 2017)
  - Two FPGAs: non-configurable, configurable
    - Non-Configurable - Platform level logics
    - Configurable - Application level logics

Sunport

NuPAC 2/2

- **Approach to CCF Mitigation**
  - Topical report specifies NuPAC platform utilizes hardware diversity and software program diversity
  - Specifics not given

Solutions and Acceptance are left open to be resolved by future submittals

Sunport

NuScale HIPS 1/3

- **Background**
  - Rock Creek Innovations LLC and NuScale Power LLC
  - Two FPGA types :
    - SRAM based
    - either a one-time programmable or flash based
  - FPGA types alternated throughout redundant architecture channels

Sunport

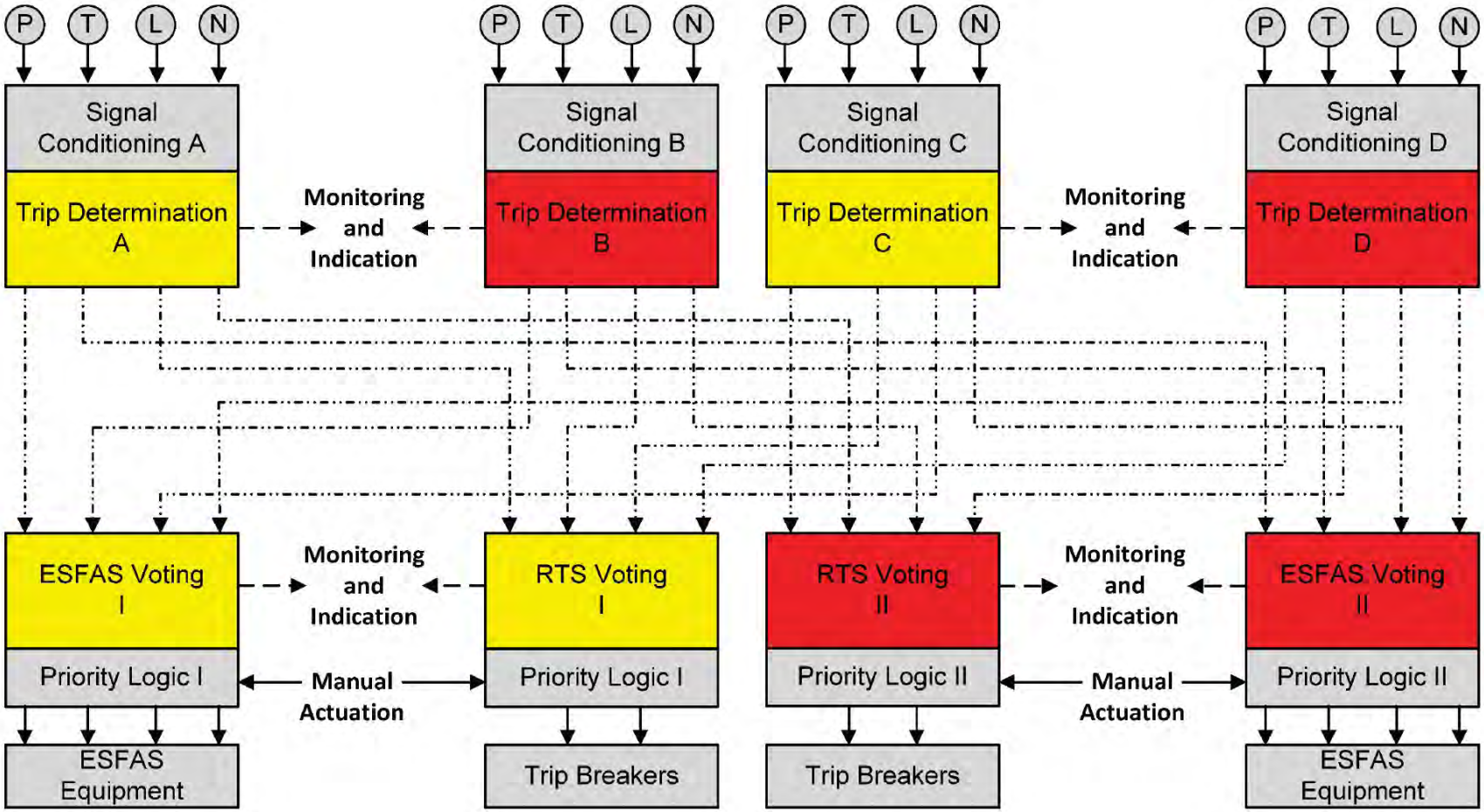
NuScale HIPS 2/3

- **Approach to CCF Mitigation**
  - HIPS Platform CCF Mitigation focused on equipment diversity (Two FPGA types)
  - Low-level architectural aspects inherently create configuration/operational differences
  - Each FPGA type has diverse development tools and programming methods
  - Development and IV&V lifecycles needed for each type (synthesis and simulation level)

Application specific action to verify design conforms to diversity attributed prescribed in Topical Report

Sunport

NuScale HIPS 3/3



Red and Yellow Indicate FPGA Diversity

Sunport

Radiy RadICS 1/3

- **Background**
  - 3rd Generation FPGA-based I&C equipment Nuclear Power Plants by Radiy
  - IEC 61508 SIL 3 certified (single channel configuration)
  - 9 NPP installations (Ukraine and Argentina)
    - 1 Reactor Trip System,
    - 2 Nuclear Island I&C,
    - 1 Conventional Island I&C,
    - 4 ESFAS,
    - 1 MCR and SCA Annunciation System
  - 80+ installations of previous 2nd Generation (Ukraine, Bulgaria, Brazil)

Sunport

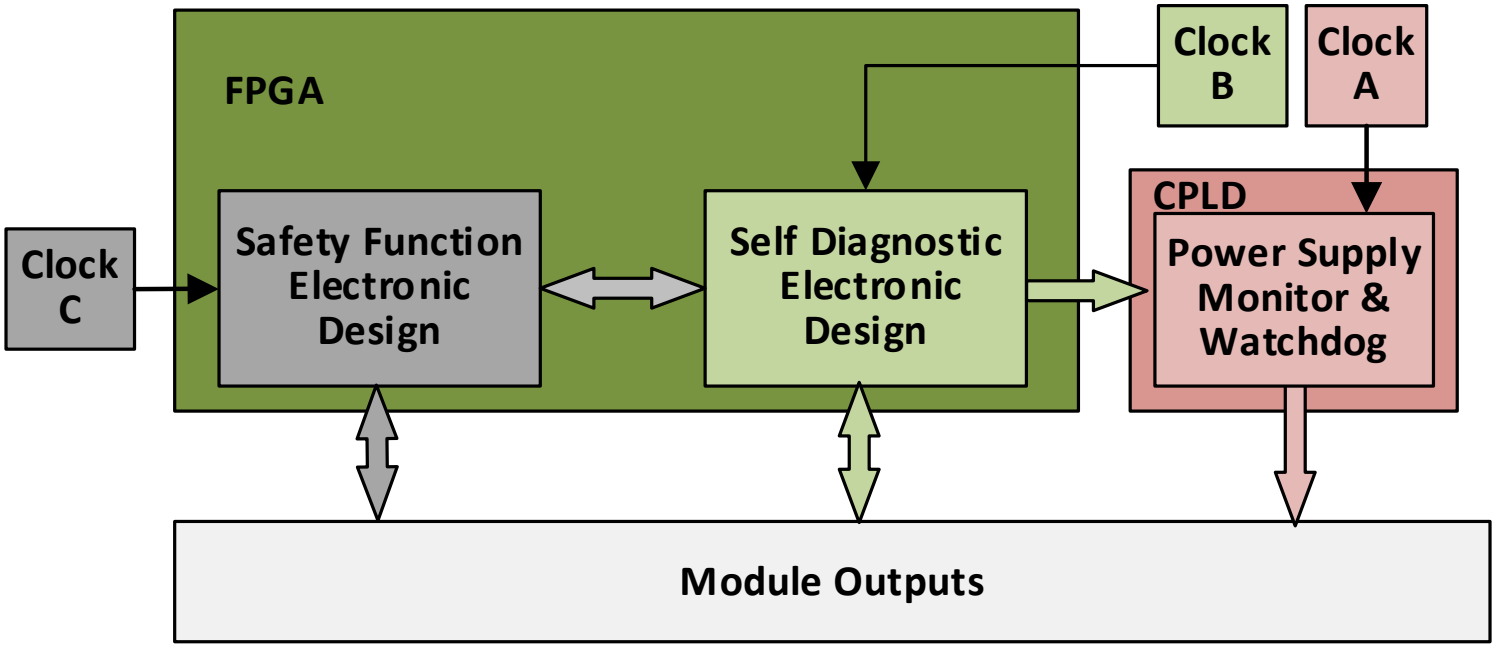
Radiy RadICS 2/3

- **Approach to CCF Mitigation**
  - Diversity strategy uses internal design features applied at platform level addressing CCF vulnerabilities
  - Diverse PLD chips (FPGA vs CPLD):
    - CPLD separate and inherently diverse from FPGA
  - CPLD monitors FPGA – independent/functionally diverse (from FPGA) method ensuing system safe state

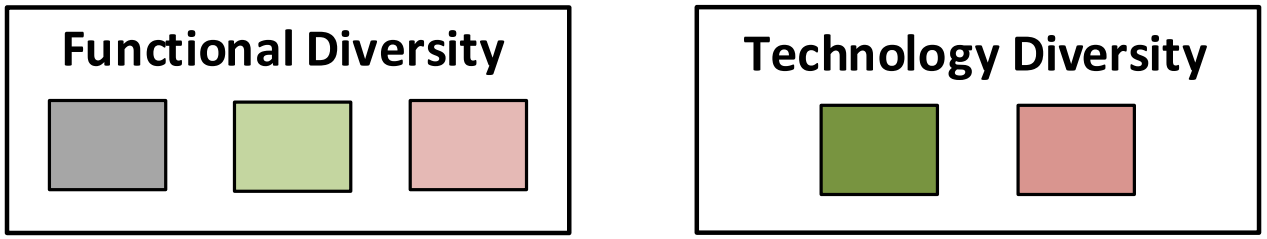
Simplifies overall I&C design: DAS or application specific design tasks NOT needed to address CCF

Sunport

Radiy RadICS 3/3



Single Channel Shown



Sunport

Moving Forward

- Innovators working with receptive regulators has led to great strides in FPGA technologies for nuclear applications
- Collaborative effort must continue as we design and install new systems
- As we do this, Technologies, Designs, and Projects will continue to improve

Sunport
Connecting Forward

www.sunport.ch

Thank you

Contact Information

Sean Kelley
Chief Operating Officer
678.654.9354
s.kelley@sunport.ch

SunPort SA
LaCite Business Nucleus Avenue
De l'Universite 24 CH-1005
Lausanne, Switzerland