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

Digital Design Decisions to Optimize Safety System Operation and Maintenance

Mark Burzynski
Chief Executive Officer

October 14-16, 2019
Budapest, Hungary

Sunport
Connecting Forward

Sunport

Purpose

Describe insights from digital design decisions to optimize safety system operation and maintenance at two U.S. protection system modernization projects

- **Oconee Experience**
- **Diablo Canyon Experience**
- **Topics Evaluated**
  - Clear Vision for Project
  - Platform Selection
  - System Architecture
  - Licensing Hurdles
  - Results Achieved

Sunport

Oconee Experience

Clear vision on maintenance and reliability improvements for protection system modernization

- Use of interchannel communication features to improve reliability
- Addition of parallel ESFAS to improve maintainability and availability
- Elimination of manual online surveillance testing
- Goal to use of best estimate analyses to address D3 without need for diverse actuation system

Oconee
Platform Selection Decisions [1]

Selected digital to address obsolescence of original analog system and with necessary features to achieve targeted benefits

- Reduced hardware board count and inventory requirements and improved protection system reliability with higher functionality digital modules
- Improved plant safety with higher availability for new system and use of graceful degradation response to faults detected by self-testing

Oconee
Platform Selection Decisions [2]

Platform Selection Decisions (cont.)

- Used self-testing features to eliminate manual channel functional tests required each calendar quarter
- Used self-monitoring features and alarms to automate manual channel checks each shift
- Digital diagnostic messaging and module HMI design to simplify troubleshooting and corrective maintenance
- Added automated test cart and HMI for end-to-end testing to reduce time and resources required to perform testing during refueling outages

Sunport

Oconee System Architecture Decisions [1]

Modified architecture to improve safety, reliability, and maintainability

- Optimized architecture within cabinet footprint constraints
- Added redundant voters to improve availability
- Used interchannel communication with 2.MIN/2.MAX logic to improve sensor fault management
- Added redundancy (i.e., master/checker voting processing modules) and 2-out-of-2 logic in each voter output to eliminate spurious actuation failure modes

Oconee
System Architecture Decisions [2]

System Architecture Decisions (cont.)

- Permanently connected maintenance workstation to improve performance monitoring and troubleshooting
- Added small scope 2-out-of-3 analog diverse actuation system for Small and Large LOCA to address common cause failure (CCF) vulnerabilities

Sunport

Oconee
Licensing Hurdles [1]

Modified architecture features that challenged NRC review

- Use of interchannel communication to improve reliability with graceful fault management features
- Combined RPS and ESFAS functions on single processor
- Added redundant 2-out-of-3 ESFAS to improve maintainability and availability

Oconee
Licensing Hurdles [2]

Licensing Hurdles (cont.)

- Exported data to plant process computer through single Monitoring & Service Interface and one-way data diode
- Service Unit permanently connected via Monitoring & Service Interface with two-way communication capability
- Best-estimate coping analyses accepted to bound all CCF events except for Small and Large LOCA

Sunport

Oconee Results Achieved

	Cost Savings	Maintainability	Reliability	Availability	Safety
Self-Testing	✓			✓	
Self-Monitoring	✓			✓	
Diagnostic and HMI	✓	✓			
Modified Architecture		✓	✓	✓	✓
Interchannel Communication					✓
Reduced Hardware	✓		✓		
No DAS	X	X			X

Sunport

Diablo Canyon Experience

Clear vision on simplification of licensing and no diverse actuation system for protection system modernization

- Decided not to use interchannel communication
- Elimination of operator actions credited for digital CCF mitigation
- No elimination of surveillance requirements
- Avoiding the need for a diverse actuation system is an important plant goal
- Original design had a single nonsafety maintenance workstation

Sunport

Diablo Canyon Platform Selection Decisions [1]

Selected two digital platforms to address obsolescence of existing digital system and with necessary features to achieve targeted benefits

- Chose two platforms with sufficient diversity (i.e., one with microprocessor and one with FPGA) to implement D3 strategy
- Digital to digital replacement of the acquisition and processing layer but not the voting layer

Diablo Canyon
Platform Selection Decisions [2]

Platform Selection Decisions (cont.)

- ALS platform utilizes a minimal set of hardware to implement the system with high reliability and integrity with internal diversity strategy to eliminate CCF concerns for that platform
- Triconex platform uses triple modular redundant communication buses which adds equipment to the basic design but was familiar to the plant personnel

Sunport

Diablo Canyon System Architecture Decisions [1]

Modified architecture to eliminate operator actions credited for digital CCF without addition of a diverse actuation system

- Optimized architecture based on careful allocation of trip functions between the two platforms
- Complicated D3 analyses required to demonstrate acceptability of architecture where ALS provides diverse trips for Triconex failure and internal diversity of ALS ensures no CCF prevents required trips from ALS

Diablo Canyon
System Architecture Decisions [2]

System Architecture Decisions (cont.)

- Temperature sensor inputs necessary for the safety functions in Triconex routed through ALS because ALS input boards readily accept temperature signals without any additional hardware
- No diverse actuation system necessary that would complicate the protection system, increase the possibility of a protection system inadvertent actuation, and result in an additional system that needs to be tested and maintained

Sunport

Diablo Canyon Licensing Hurdles [1]

Design decisions that challenged NRC review

- Assessment of temperature signal routing for potential impacts on D3 strategy
- Safe state arbitration for disagreements between ALS diverse core outputs
- Design change to separate maintenance computer for each subsystem also simplifies factory accepting acceptance testing requirements and eliminates potential software interaction issues

Sunport

Diablo Canyon Licensing Hurdles [2]

Licensing Hurdles (cont.)

- Single functional requirements specification for project applied to both vendors
  - not all functional requirements applicable to each platform
  - contributed to vendors not meeting all applicable requirements during detailed design
  - required redesign that extended vendor schedules and complicated NRC review
- Two-year delay due to functional requirement specification changes, redesign, first-of-a-kind engineering, and integrated factory acceptance test resolution

Sunport

Diablo Canyon Results Achieved

	Results	Comments
Simplification of Licensing	X	Several factors added complexity or duration to licensing review
Elimination of Operator Actions Credited for Digital Common Cause Failure Mitigation	✔	
Avoid Need for Diverse Actuation System	✔	Achieved but with added complexity to architecture and two safety-related platforms to be tested and maintained
Single Nonsafety Maintenance Workstation	X	Design change to separate maintenance computer for each subsystem

Sunport
Connecting Forward

www.sunport.ch

Thank you

SunPort SA

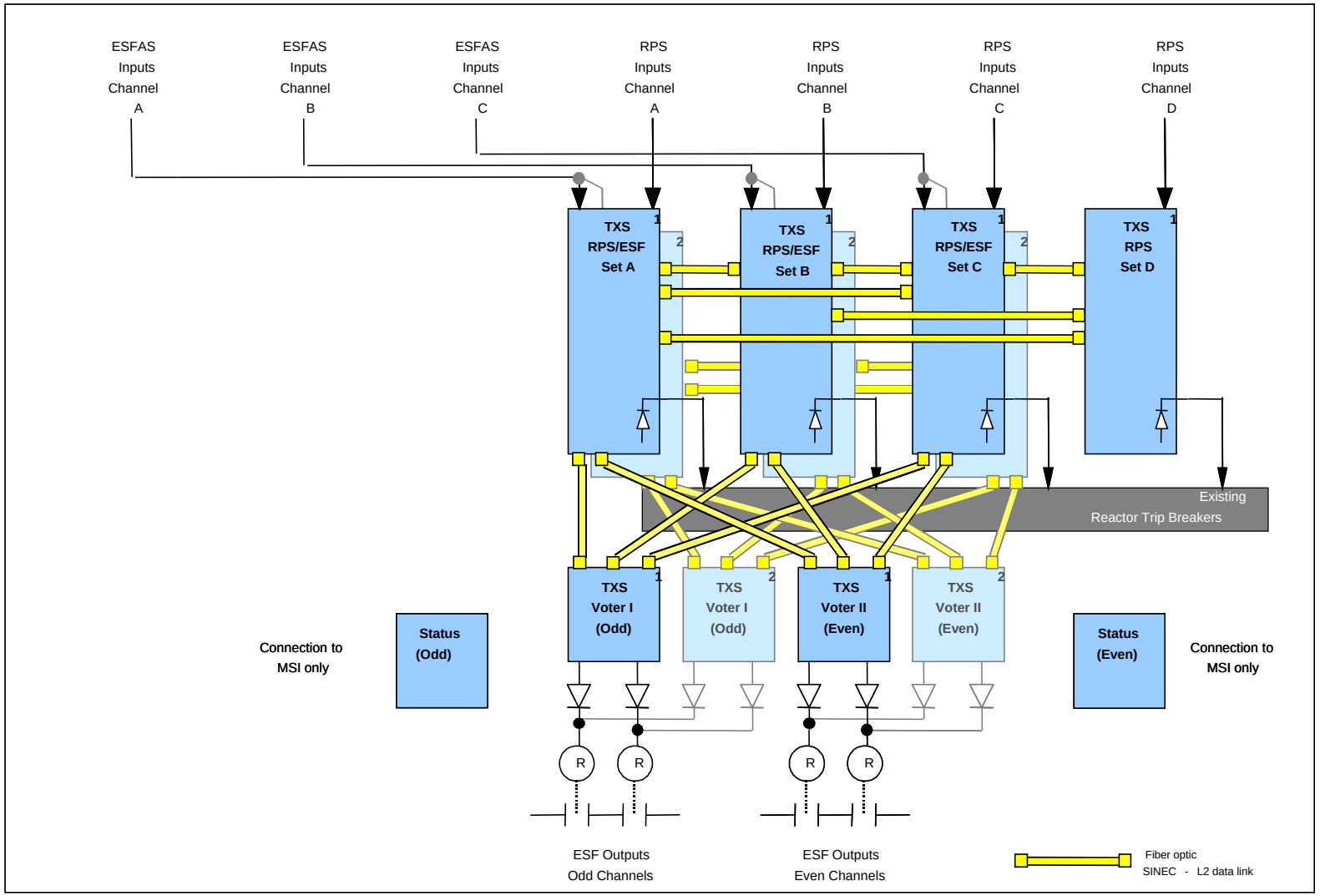
LaCite Business Nucleus Avenue
De l'Universite 24 CH-1005
Lausanne, Switzerland

Sunport

Backup Slides

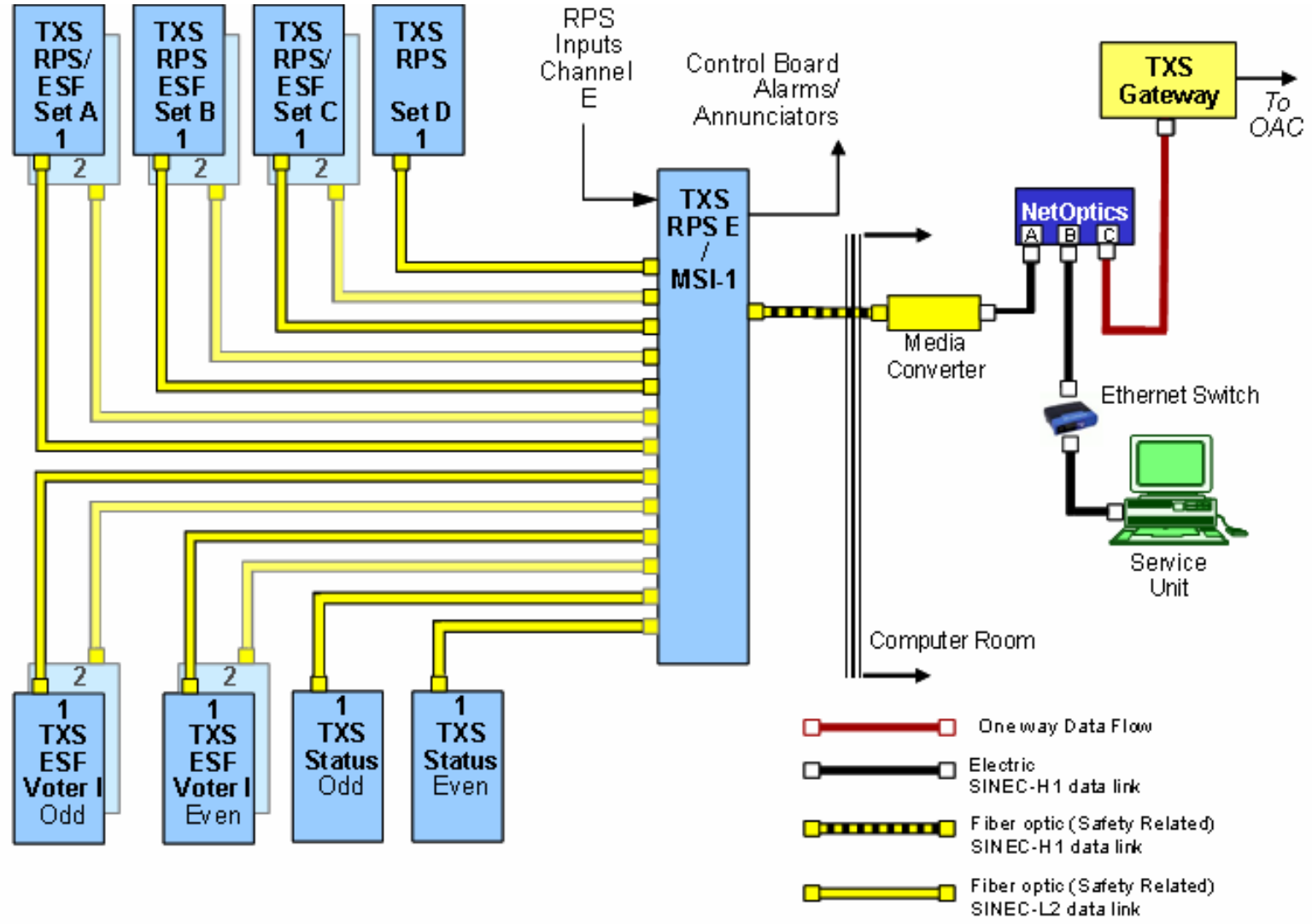
Sunport

Oconee Architecture [1]



Sunport

Oconee Architecture [2]



Sunport

Diablo Canyon Architecture