11th International Workshop on the Application of FPGAs in Nuclear Power Plants

Using NUREG/CR-7007 to Assess the Internal Diversity of an FPGA - Based Platform

Sean Kelley
Chief Operating Officer

October 8-11, 2018
Dallas, Texas, USA

Sunport
Connecting Forward

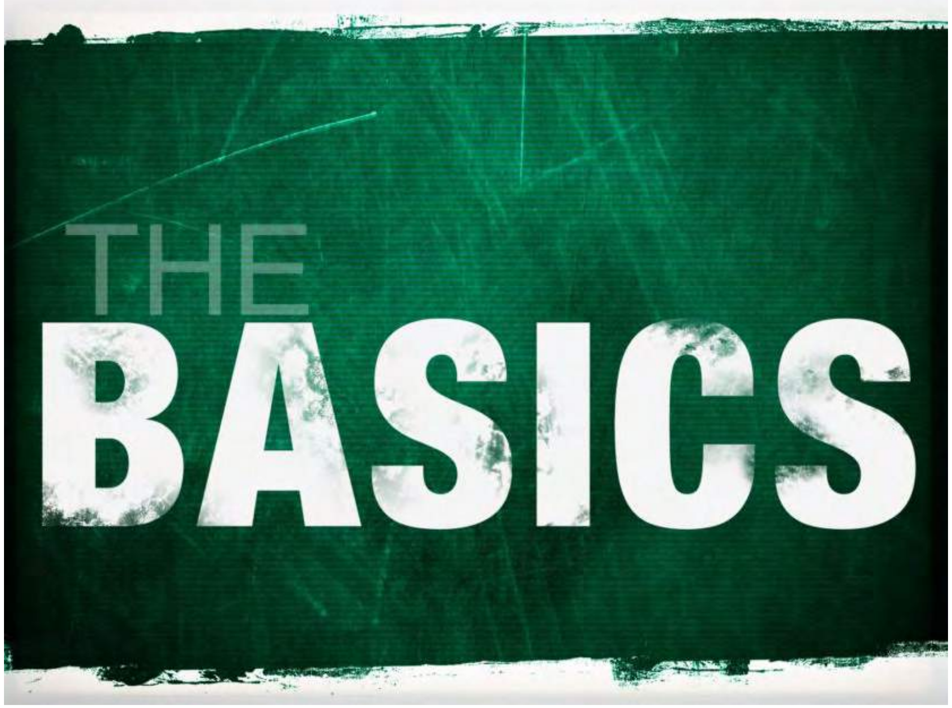
The Age Old Question

…..or at least 25+ years old

- Current NRC activities related to action plan for Common Cause Failures (CCFs) stem from SECY-93-087 – “Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor Designs”
- If diversity is required in a safety system to mitigate the consequences of potential CCFs……

How much diversity is enough?

NUREG/CR-7007



Three Baseline Diversity Strategies

- Strategy A – Different Technologies
  - Ex: Analog vs. Digital
- Strategy B – Different Approaches within Same Technology
  - Ex: FPGA vs. Microprocessor
- Strategy C – Different Technology Architectures within Same Technology
  - Ex: Diverse microprocessors as the basis for primary safety systems and diverse backup system (DAS)
  - Ex: FPGA vs. CPLD

Decide which strategy is closest

Diversity Attributes

- Design – Strategy A, B, or C
- Equipment Manufacturer – manufacturer and equipment Type
- Logic Processing Equipment – architecture, versions, data-flow, and/or component integration
- Functional – underlying mechanisms, different purpose, function, control logic, actuation means, time response
- Life-cycle – organizations/companies, management, teams
- Logic – algorithms, timing, run-time environment
- Signal – sensed parameters, physical effects, sensor types

Inherent vs. Intentional

Implementation

1. Classify the diversity strategy — Identification of specific diversity strategy selected
2. Confirm inherent diversity credit — Impact of technology difference
3. Identify intentional diversity usage — Diversity criteria intentionally applied. Conscious decisions, must be adhered to by effort
4. Categorize diversity usage in relation to the corresponding strategy classification — Capturing combination of diversity vs. corresponding strategy identified in NUREG/CR-7007 (A, B, C)
5. Assess the diversity strategy — Comparative evaluations against the baseline diversity strategies

Use spreadsheet in NUREG/CR-7007

Determine Adequacy of Diversity Strategy

- Proposed diversity strategy can be shown to adequately addresses CCF mitigation needs, as identified via a D3 assessment, based upon:

  1. Conformance to one of three baseline strategies (or an accepted variant), or
  2. Determination strategy reasonably ensures CCF mitigation comparable to baseline strategy (i.e., acceptable rationale provided to support mitigation claims)

Similar scores to baseline should be acceptable

CASE STUDY

Sunport

Case Study of a Sample FPGA System

- Hypothetical PLD based protection platform
  - Segregated self-diagnostics and finite state machine for execution of application
  - Uses multiple types of PLD devices throughout system
  - Use of multiple and separate timing domains
  - Multiple vectors for accomplishing safety functions (i.e., functional diversity for accomplishing safety functions)
- Separate and independent Design and IV&V personnel
  - Including separation of management teams
- Nuclear processes and design elements a focus at conception

Achieves Diversity by combining Technology, Design Elements, and Processes

Design Attributes

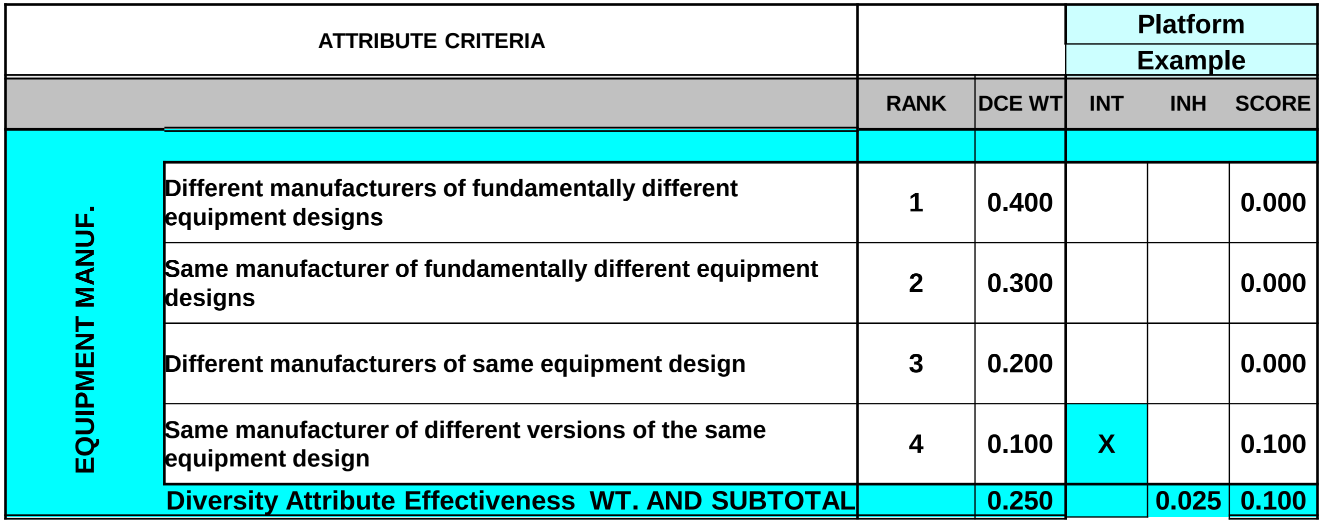
- Use of 2 types of PLDs (i.e., Different architectures within same technology family, Strategy C)

ATTRIBUTE CRITERIA				Platform Example		
		RANK	DCE WT	INT	INH	SCORE
DESIGN	Different technologies (A)	1	0.500			0.000
	Different approaches within a technology (B)	2	0.333			0.000
	Different architectures (C)	3	0.167	X		0.167
	Diversity Attribute Effectiveness WT. AND SUBTOTAL		1.000		0.167	0.167

Determines Baseline Strategy

Equipment Manufacturer

- Same manufacturer for the different PLDs
  - Conservative credit given to design by treating different chip families as different versions of the same product rather than different products



	ATTRIBUTE CRITERIA			Platform Example		
		RANK	DCE WT	INT	INH	SCORE
EQUIPMENT MANUF.	Different manufacturers of fundamentally different equipment designs	1	0.400			0.000
	Same manufacturer of fundamentally different equipment designs	2	0.300			0.000
	Different manufacturers of same equipment design	3	0.200			0.000
	Same manufacturer of different versions of the same equipment design	4	0.100	X		0.100
	Diversity Attribute Effectiveness WT. AND SUBTOTAL		0.250		0.025	0.100

Be conservative and be able to defend your position

Sun port

Logic Processing Equipment

- Intentional selection of different logic processing approaches in the different PLD devices
- Inherent differences in data flow microarchitectures and structural characteristics

ATTRIBUTE CRITERIA				Platform Example		
		RANK	DCE WT	INT	INH	SCORE
LOGIC PROC. EQUIP.	Different logic processing equipment architectures	1	0.400			0.000
	Different logic processing versions in same equipment architecture	2	0.300	X		0.300
	Different component integration architectures	3	0.200			0.000
	Different data flow architectures	4	0.100		i	0.100
	Diversity Attribute Effectiveness WT. AND SUBTOTAL		0.644		0.258	0.400

Again….. a conservative approach by assuming different versions of the architecture

Function

- Inherent response time scale due to different clock domains
- Intentional use of different underlying mechanisms and actuation means
  - Existing plant system designs (Anticipated Transient w/o SCRAM (ATWS) operating experience and 10 CFR 50.62)
  - Internal diverse actuation mechanisms (logics and actuation paths)

ATTRIBUTE CRITERIA				Platform Example		
		RANK	DCE WT	INT	INH	SCORE
FUNCTION	Different underlying mechanisms to accomplish safety function	1	0.500	X		0.500
	Different purpose, function, control logic, or actuation means of same underlying mechanism	2	0.333	X		0.333
	Different response time scale	3	0.167		i	0.167
	Diversity Attribute Effectiveness WT. AND SUBTOTAL		0.600		0.600	1.000

Since some system design rules must be maintained you can take credit for them

Lifecycle

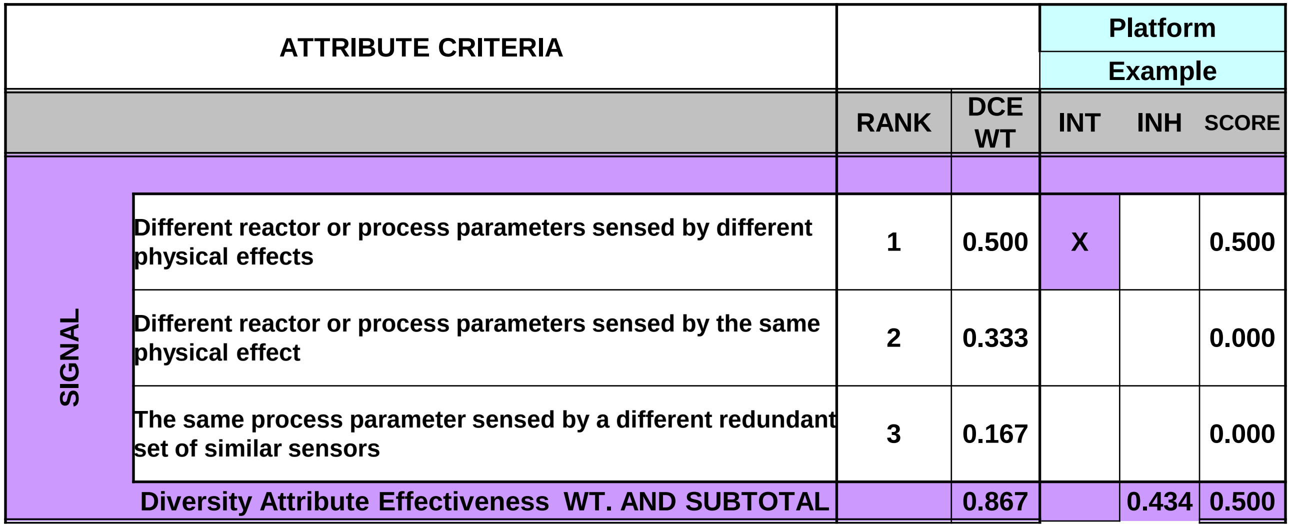
- Intentional use of different management teams and use of nuclear processes leads to
- Inherent diversity of personnel (Design vs. IV&V)

	ATTRIBUTE CRITERIA			Platform Example		
		RANK	DCE WT	INT	INH	SCORE
LIFECYCLE	Different design organizations/companies	1	0.400			0.000
	Different management teams within the same company	2	0.300	X		0.300
	Different designers, engineers, and/or programmers	3	0.200		i	0.200
	Different testers, installers, or certification personnel	4	0.100		i	0.100
	Diversity Attribute Effectiveness WT. AND SUBTOTAL		0.683		0.410	0.600

Regulatory compliance dictates certain decisions

Signal

- Intentional use of different parameters sensed by different physical effects based on the existing signal diversity in the protection systems (Pressures, Levels, Temperatures, NI, etc)
  - Current practice when designing Nuclear I&C Systems



	ATTRIBUTE CRITERIA			Platform Example		
		RANK	DCE WT	INT	INH	SCORE
SIGNAL	Different reactor or process parameters sensed by different physical effects	1	0.500	X		0.500
	Different reactor or process parameters sensed by the same physical effect	2	0.333			0.000
	The same process parameter sensed by a different redundant set of similar sensors	3	0.167			0.000
	Diversity Attribute Effectiveness WT. AND SUBTOTAL		0.867		0.434	0.500

Old Adage - Stick with what works

Logic

- Intentional use of different and separate logics for safety functions/self tests
- Inherent differences in timing, runtime, and functional representations provided by use of different PLDs and separate clock domains

ATTRIBUTE CRITERIA				Platform Example		
		RANK	DCE WT	INT	INH	SCORE
LOGIC	Different algorithms, logic, and logic architecture	1	0.400	X		0.400
	Different timing or order of execution	2	0.300		i	0.300
	Different runtime environments	3	0.200		i	0.200
	Different functional representations	4	0.100		i	0.100
	Diversity Attribute Effectiveness WT. AND SUBTOTAL		0.733		0.733	1.000

FPGAs have strong diversity capabilities in this area!

Sunport

Evaluating Diversity

- Normalize your System Score with Subtotals and Weighting
  - Example:
    - Logic Section Subtotal:

      Score of 1.0 * Weighting of 0.733 *100 = 73.3
- Add up all section normalized scores to calculate your Normalized System Score
- Compare Normalized System Score to the Baseline Score of 271 to compute a comparison ratio

Having a spreadsheet implementing the NUREG worksheet helps with this task.

Strategy Mapping

- Strategy C represents architectural variations within a technology as the basis for diverse systems, redundancies, or subsystems
- Represents composite of acceptable Diversity solutions
- Most comparable to the case study system
- Strategy C yields a comparison ratio of **0.98**

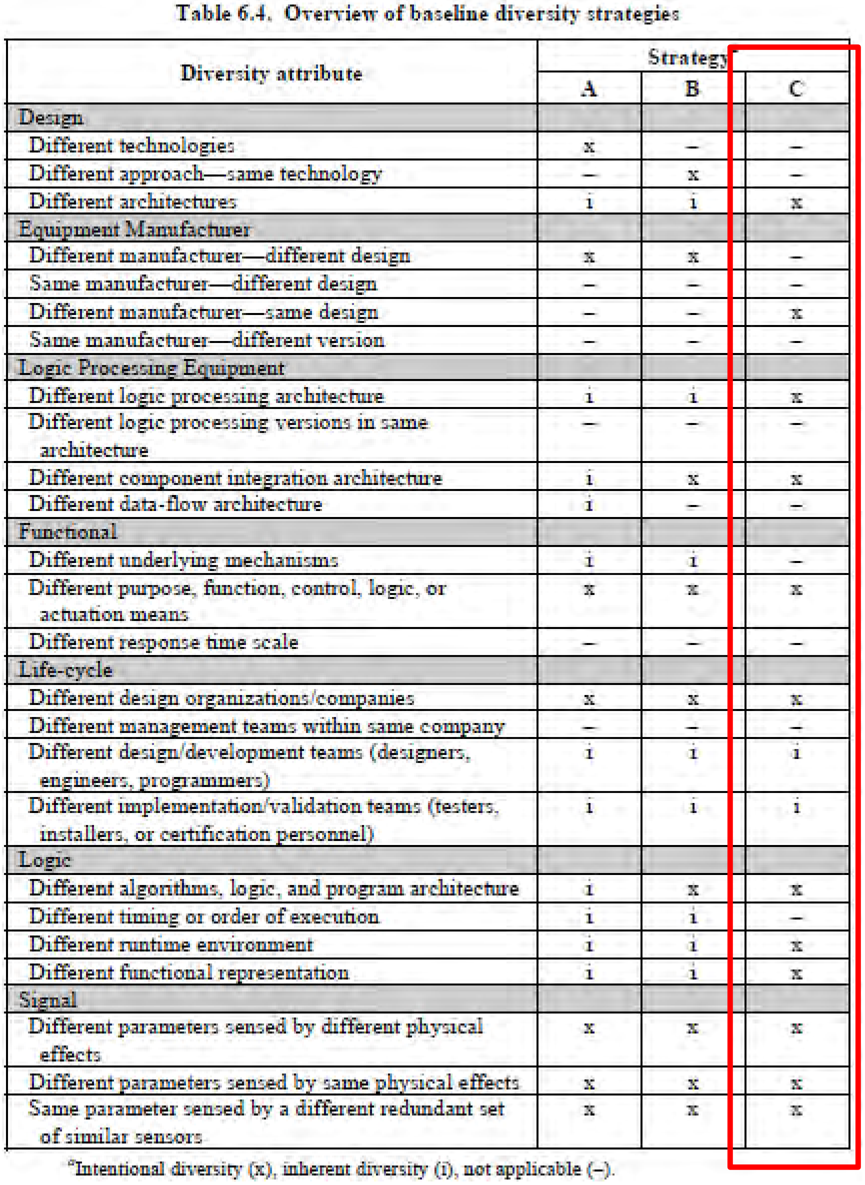


Table 6.4. Overview of baseline diversity strategies

Diversity attribute	Strategy[a]		
	A	B	C
Design			
Different technologies	x	–	–
Different approach—same technology	–	x	–
Different architectures	i	i	x
Equipment Manufacturer			
Different manufacturer—different design	x	x	–
Same manufacturer—different design	–	–	–
Different manufacturer—same design	–	–	x
Same manufacturer—different version	–	–	–
Logic Processing Equipment			
Different logic processing architecture	i	i	x
Different logic processing versions in same architecture	–	–	–
Different component integration architecture	i	x	x
Different data-flow architecture	i	–	–
Functional			
Different underlying mechanisms	i	i	–
Different purpose, function, control, logic, or actuation means	x	x	x
Different response time scale	–	–	–
Life-cycle			
Different design organizations/companies	x	x	x
Different management teams within same company	–	–	–
Different design/development teams (designers, engineers, programmers)	i	i	i
Different implementation/validation teams (testers, installers, or certification personnel)	i	i	i
Logic			
Different algorithms, logic, and program architecture	i	x	x
Different timing or order of execution	i	i	–
Different runtime environment	i	i	x
Different functional representation	i	i	x
Signal			
Different parameters sensed by different physical effects	x	x	x
Different parameters sensed by same physical effects	x	x	x
Same parameter sensed by a different redundant set of similar sensors	x	x	x

[a] Intentional diversity (x), inherent diversity (i), not applicable (–).

Digital Systems combined with DAS deemed acceptable

FPGA System Comparison /w Strategy C

- Normalized System Score – 263
  - (0.167 + 0.025 + 0.258 + 0.600 + 0.410 + 0.434 + 0.733) * 100 = 262.56
- Compare Normalized System Score to the Baseline Score of 271 yields a comparison ratio of **0.97**
- Results for the FPGA System with internal diversity compares favorably (**0.97 vs. 0.98**) to a nominal microprocessor based primary safety system with a microprocessor based diverse backup system (DAS) (principle example for Strategy C) as described in NUREG/CR-7007

Case Study FPGA System with internal diversity does not need a DAS

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