Failure Modes Taxonomy: Assessing the Reliability of FPGA-Based I&C Systems

9th International Workshop on the Application of FPGA's in NPP's

October 3-6, 2016

Lyon, France

P. McNelles, Z.C. Zeng,
G. Renganathan, M. Chirila and L. Lu

e-Doc #5081398

Presentation Outline

- Introduction
  - Potential use of FPGAs in Canadian NPPs
- FMEA
  - Purpose of FPGA FMEA (Research Program)
  - FMEA Results and Failure Mode Categorization
- OECD-NEA Taxonomy
  - Taxonomy Basis
- FPGA Taxonomy
  - Taxonomy Extension
  - Taxonomy Demonstration
- Conclusions

Introduction

- Nuclear Power Plants (NPPs) in Canada constructed 1971-1992:
  - FPGAs not implemented in NPPs at that time
  - FPGAs later implemented in non-safety systems
- FPGAs have seen more use in NPP I&C:
  - International implementations
  - New builds
  - Replacement of older systems
- Potential for future use in operating plants in Canada

Purpose of FMEA (Research Project)

- FMEA Research Program:
  - Identify potential failure modes and causes
  - Identify methods to avoid or mitigate those failures
  - Ensure FPGA-based systems are safe to use

- Extensive Literature Review:
  - USNRC and ORNL, VTT, EPRI, OECD-NEA
  - Standards from IEC, IEEE and CSA
  - White papers from FPGA suppliers
  - Scientific/technical literature

FMEA Results (General)

- Identified potential issues:
  - Failure modes, faults, logic errors, human factors…
- Failures divided into categories:
  - 1st : Lifecycle: design (fabrication), operation
  - 2nd : Causes: design defect, manufacturer defect, environmental, stress/aging, human factors.
- Causes, potential effects, and methods to eliminate/mitigate those failures for each set

FMEA Results (Failure Sets)

- Failure “causes” divided into “failure sets” based on “failure effects”
  - Failure effect:
    - *“Consequence of a failure mode in terms of the operation, function or status of the item”*
    - IEC 60812 standard (FMEA)[1]
  - Each set includes a description and mitigation
  - Grouped for easier identification and mitigation

FMEA Results (Failure Sets)

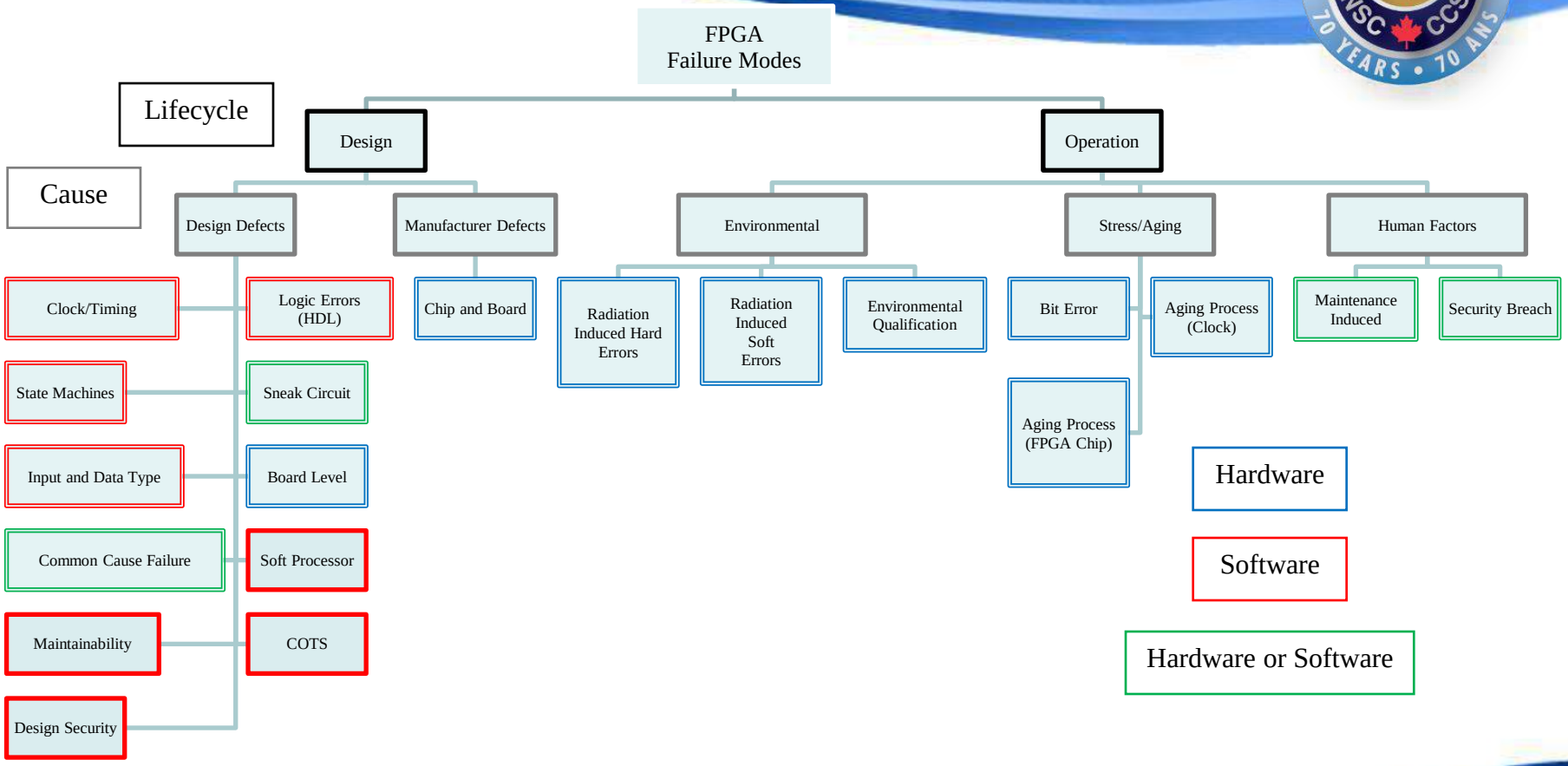


Figure 1: FPGA Failure Mode Categories (Failure Sets)[2]

Elementary Fault Classes

- Elementary fault classes:
  - High-level classification (IEEE)[3]
  - Generic digital fault information
  - 31 potential fault combinations
- Three major groupings (5 total):
  - Development (dev.) faults
  - Interaction (int.) faults
  - Physical faults
- Mapping of FPGA faults to elementary fault classes:
  - Useful for identifying failures
  - Utilize mitigation methods

FMEA Category	Elementary Fault Example
All Software/HDL Failures (Except "Design Security")	Software Faults
Manufacturer Defects Board Level (Design)	Production Defects and/or Hardware Errata
Environmental (Environmental Qualification)	Physical Interference (Natural, Hardware (HW))
Environmental (Radiation Induced Hard Errors) (Radiation Induced Soft Errors)	Physical Interference (Nat., HW., Perm) ((Nat., HW., Trans.)
Stress/Aging	Physical Deterioration
Human Factors (Maintenance Induced)	Physical Interference (Hardware, Non-Mal) Input Mistakes (Software, Non-Mal)
Human Factors (Security Breach)	Intrusion Attempts (Hardware, Mal) Virus/Worms (Software, Mal, Int)
Design Security	Logic/Timing Bombs (Software, Mal, Dev)

Table 1: FMEA Fault Mapping[3]

FPGA Failure Mode Interface

- FPGA FMEA compiled and categorized a large amount of FPGA failure mode data
- Need to create interface for FPGA FMEA data and results from international working groups
  - Working Group on Risk Assessment (WGRISK)
- FPGA FMEA failure data is restructured based on international research and practices
  - FPGA Failure Modes Taxonomy
- FPGA taxonomy framework based on digital failure mode work performed by the OECD-NEA

OECD-NEA Digital Instrumentation and Control Failure Mode Taxonomy

- OECD-NEA published "*Failure Modes Taxonomy for Reliability Assessment of Digital I&C Systems for PRA*"[4,5]
  - Considered failure modes/effects, uncovering situations
- Specific to software-based systems, with FPGAs left as a topic for future work
  - Mitigation methods also not covered in detail
- FPGA taxonomy creates a "plug-in" to interface with OECD-NEA taxonomy
- FPGA taxonomy represents the culmination of a CNSC research project into FPGA-based system reliability

OECD-NEA DIC Taxonomy Basis

- Overall, four main elements are considered:
  - Fault location
  - Failure effect
  - Uncovering situation
  - End effect (maximum and most likely)

- Considering the “end effect”, three additional aspects can be included:
  - Failure origin
  - Most likely end effect (Fault Tolerant Design (FTD))
  - Maximum possible end effect (No FTD)

OECD-NEA DIC Levels of Abstraction

- Five levels of abstraction:
  1) System
     - Complete I&C System
  2) Division
     - Physical separation of the I&C System
  3) I&C Unit
     - Elements that execute specific functions
  4) Module
     - Task-specific HW/SW elements
  5) Basic Component
     - Individual hardware components

OECD-NEA DIC Test System

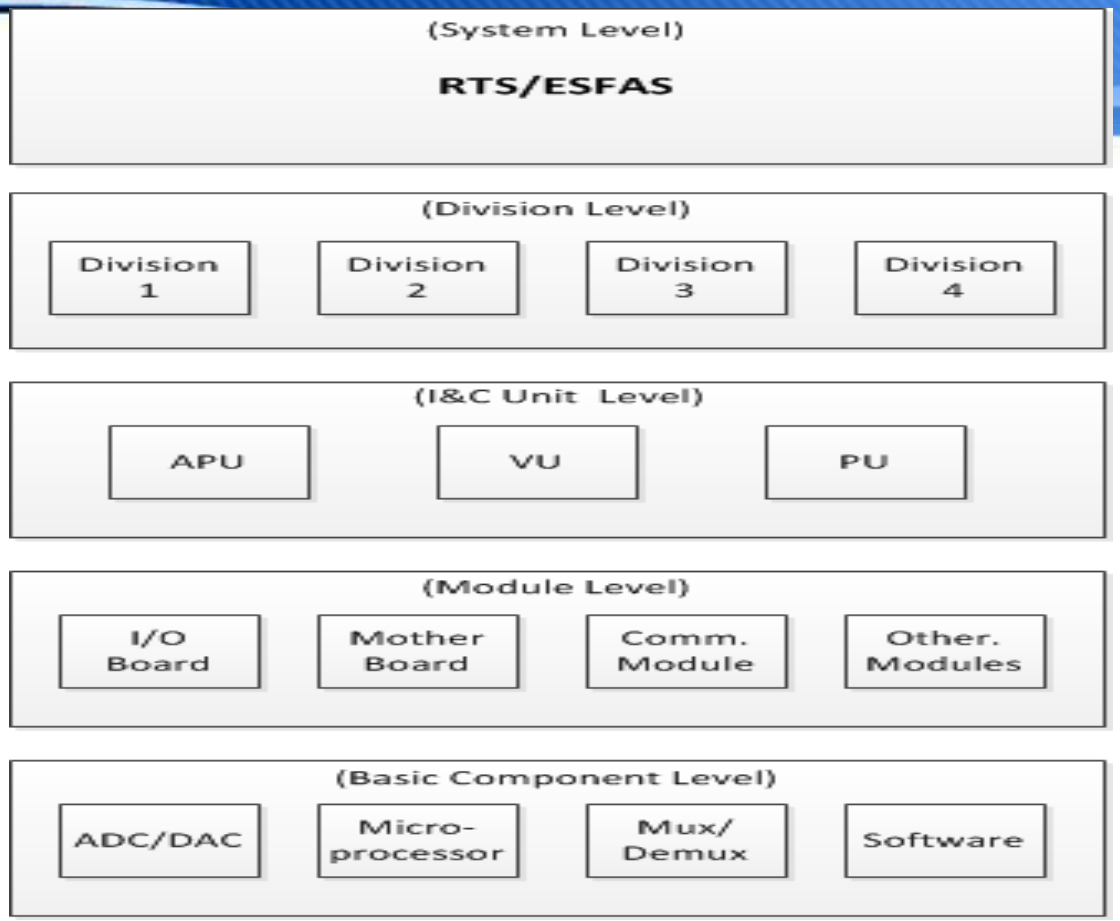


Figure 3: Simplified Reactor Trip System/Engineering Safety Features Actuation System (RTS/ESFAS) Test System[4]

OECD-NEA DIC Failure Modes and Effects (1)

- Failure effects at lower level become failure modes at next level
- Failure at the basic component level causes failure at the module level
- "Cascading failure"
  - Separate from Common Cause Failure (CCF)

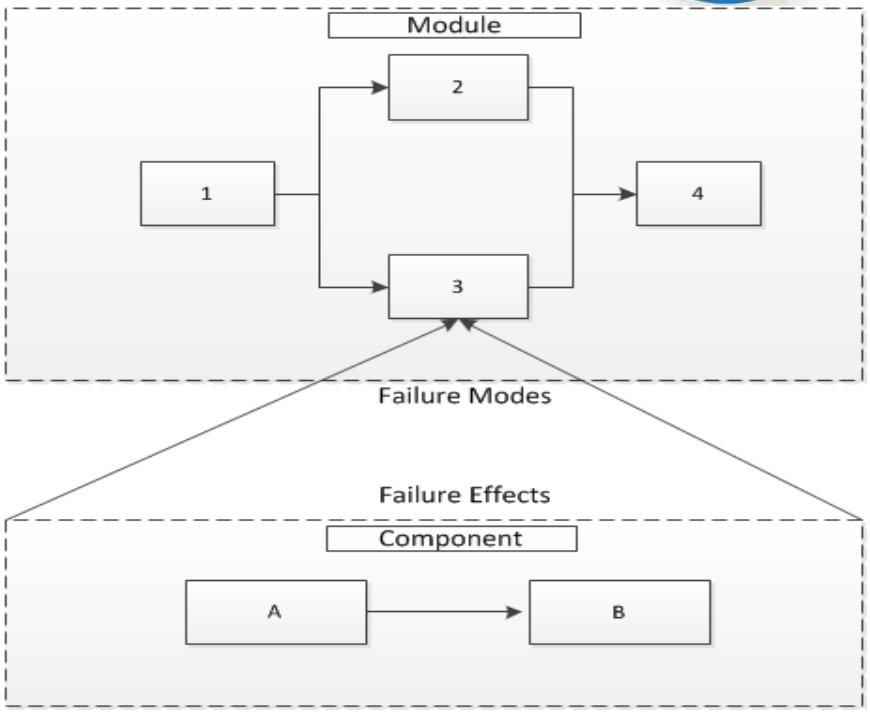


Figure 4: Failure Effect and Failure Mode Relation[4]

OECD-NEA DIC Failure Modes and Effects (2)

- **Fatal:** Unit stops functioning completely, and no longer provides an output:
  - **Ordered fatal:** Unit outputs forced into pre-set values
  - **Haphazard fatal:** Unit is in an unpredictable state

- **Non-Fatal:** Unit fails, but still performs computations, passing along incorrect data:
  - **Plausible Behavior:** Incorrect outputs are not easily identified
  - **Implausible Behavior**: Unit outputs are obviously incorrect

OECD-NEA DIC Uncovering Situations

- Four possible uncovering situations:
  - Demand
    - Latent
    - Triggered
  - Spurious action
  - Online detection
  - Offline detection

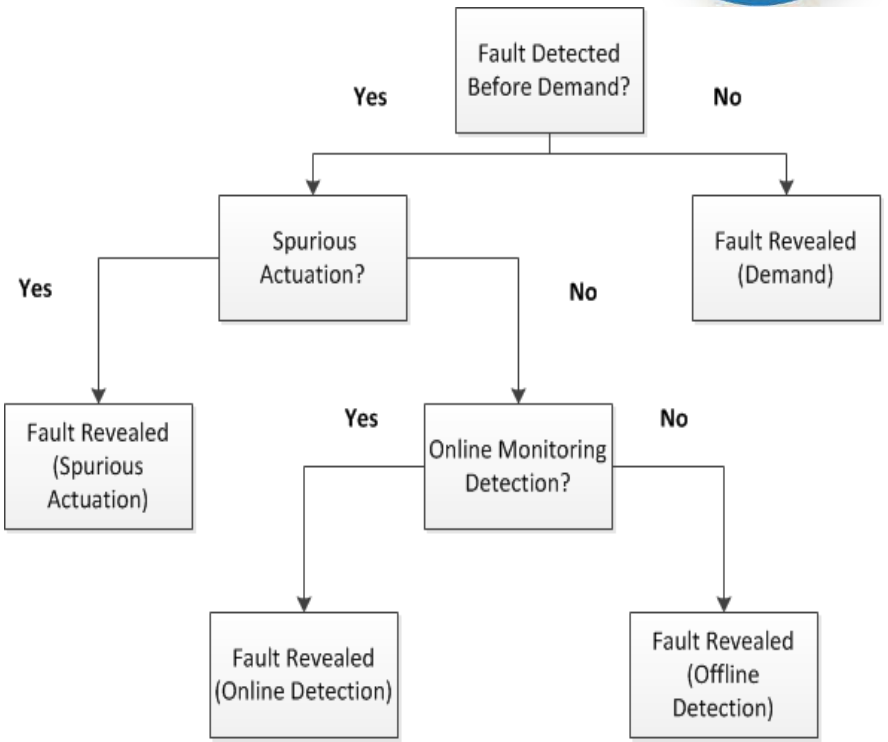


Figure 4: Fault Uncovering Situations[4]

Relation of OECD-NEA DIC Taxonomy and FPGA FMEA

- OECD-NEA taxonomy categorizes the failure modes based on end effects, uncovering situation, and the level of abstraction (failure location)
- Does not provide categorization for the cause or mitigation methods of those failure modes
- FPGA FMEA failure sets interfaces with the OECD-NEA taxonomy framework by creating a taxonomy extension
  - Failure effects and uncovering situations
  - Hardware and software (HDL code) failure modes
  - Potential effects on module and system level

Taxonomy Extension

- "Logic Process" represents digital hardware and software/HDL components
- Extends OECD-NEA taxonomy to include FPGAs for all levels of abstraction
- Creates plug-in for modelling FPGA failure modes using OECD-NEA framework

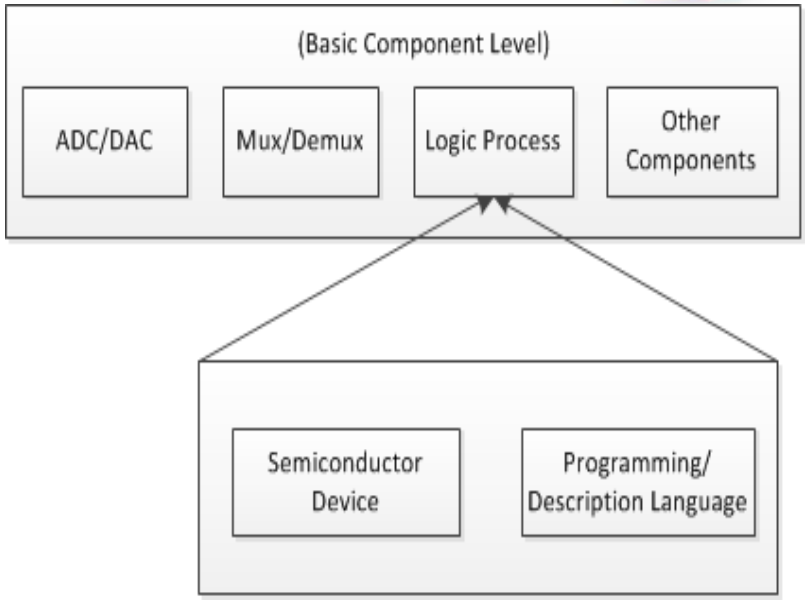


Figure 5: Extended Taxonomy Using "Logic Process"

FPGA Taxonomy

- FPGA FMEA failure mode data focused on FPGA/chip board
- OECD-NEA taxonomy stopped at basic component level
- FPGA taxonomy added a Sub-Component (SC) level of abstraction
- Sub-component level accounts for failures of FPGA chip (Basic Component (BC))
- HW and SW (HDL code) failure set data

FPGA Taxonomy (Sub-Component) (1)

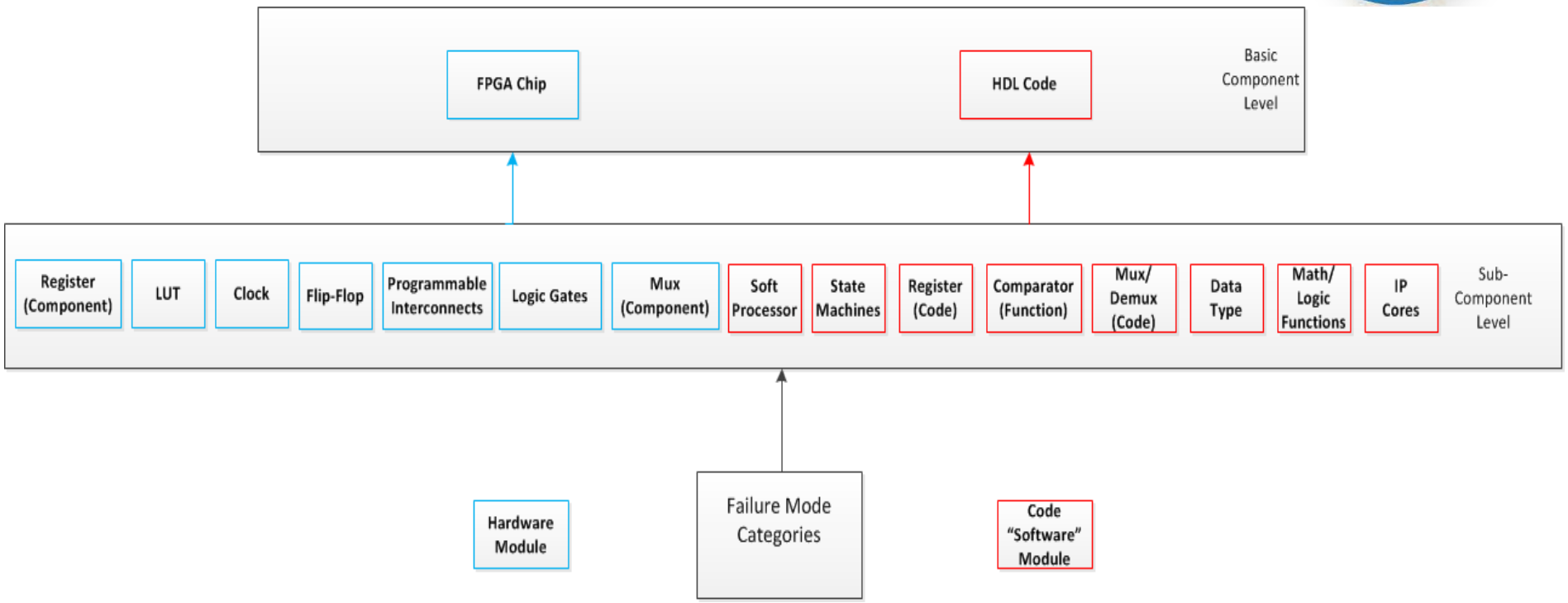


Figure 6: Relationship between "Basic Component", "Sub-Component", and "Failure Categories"

FPGA Taxonomy (Sub-Component) (2)

- Sub-component level considers hardware and software (HDL code) failures
- Hardware Sub-component example:
  - FPGA chip/board
  - Hardware FMEA (single event upset)
- Software (HDL code) Sub-component example:
  - Parameter trip
  - Software FMEA (state machine endless loop)
- Uncovering situations for both cases

Sub-Component Hardware Taxonomy

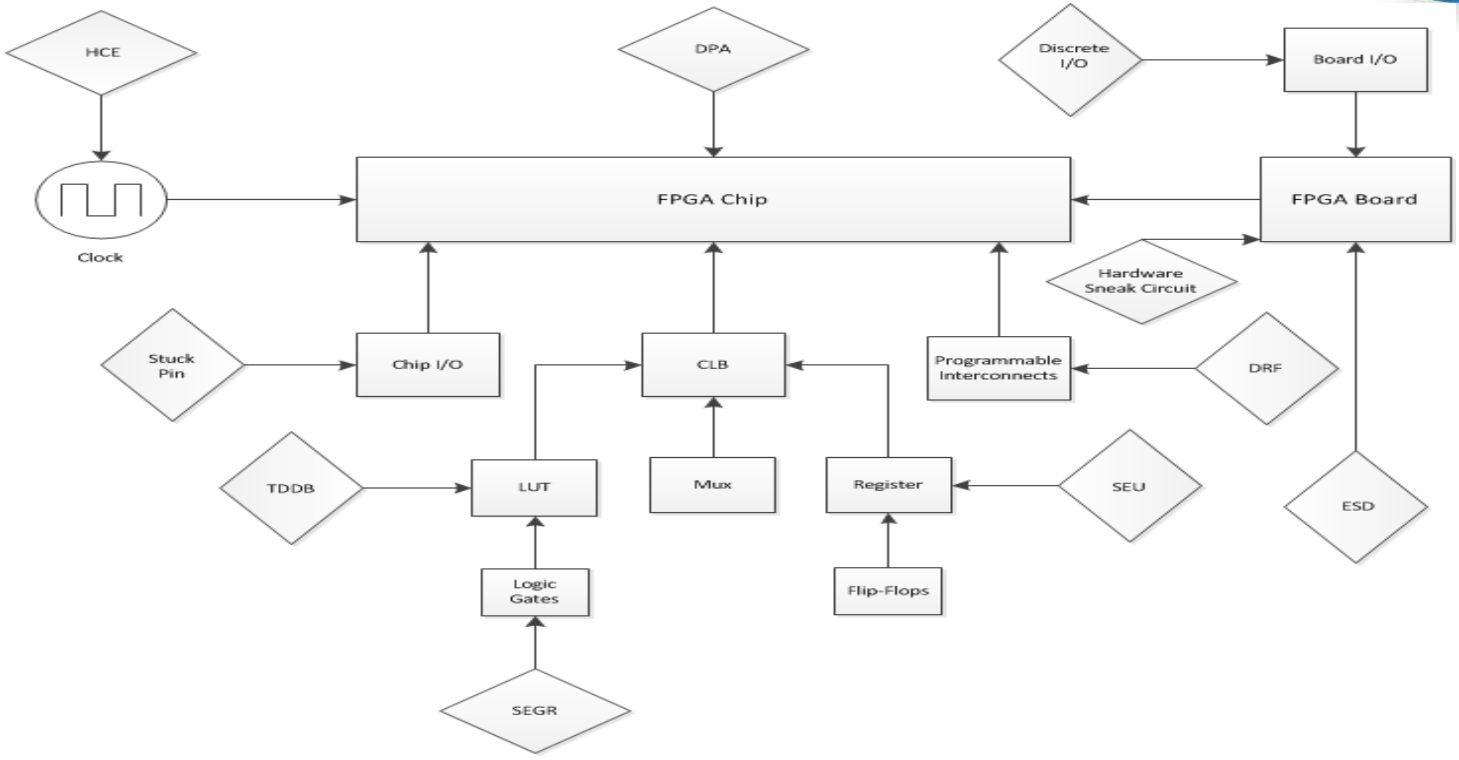


Figure 7: FPGA Chip/Board Hardware Failures

Sub-Component Hardware FMEA

FMEA Heading	FMEA Data
Failure:	Single Event Upset (SEU)
Fault Location:	Register/flip-flop (storage element)
Sub-Component Level Effect:	Temporary bit upset in storage element
Basic Component Level Effect:	Incorrect output
Failure Type:	Non-fatal
Failure Set (FPGA FMEA):	Radiation induced soft error
Failure Set (Elementary Fault Class):	Physical interference
Cause (FPGA FMEA):	Environmental
Cause (Elementary Fault Class):	Physical/interaction
Lifecycle:	Operation (operational)
Mitigation Method(s):	Error Detection and Correction (EDAC) Triple Modular Redundancy (TMR)

Table 2: Hardware Sub-Component Level Failure Modes/Failure Effects (SEU Example)

Sub-Component Software Taxonomy

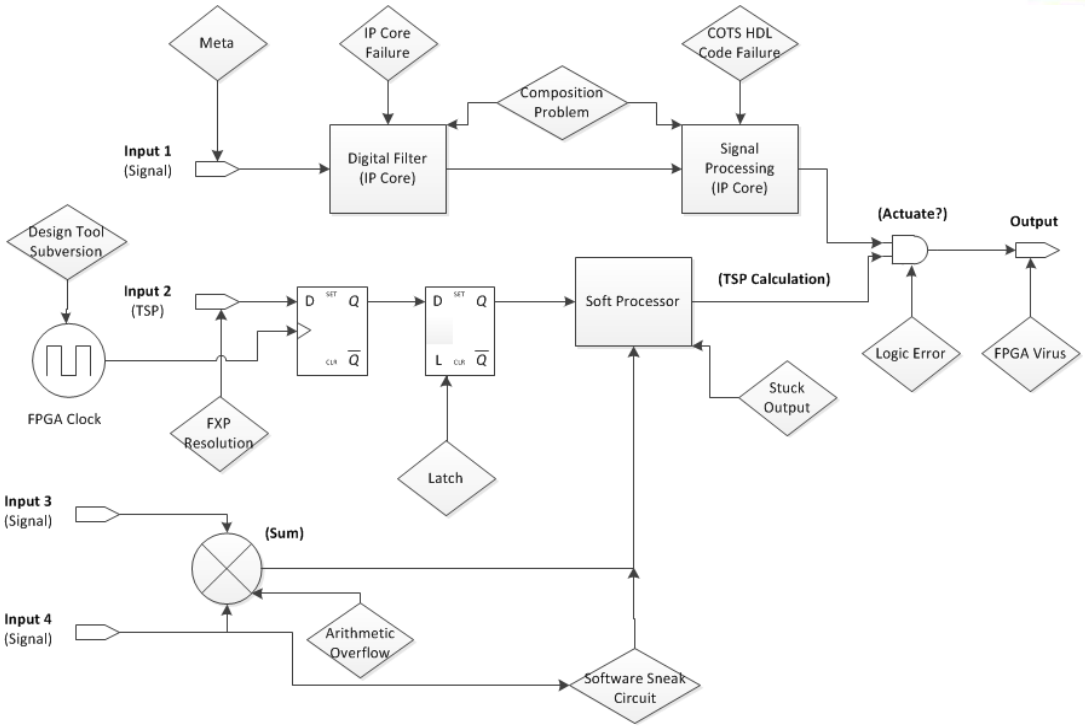


Figure 8: FPGA Software Failures (Parameter Trip)[6,7]

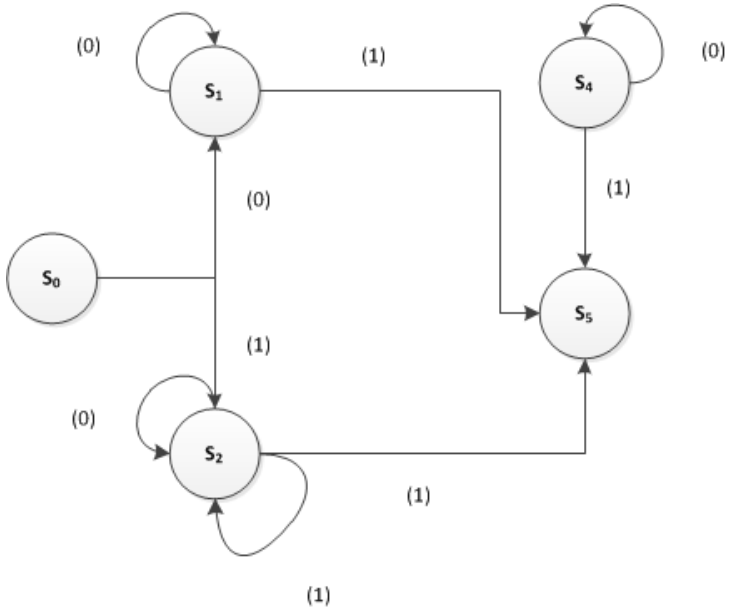


Figure 9: FPGA Software Failures (State Machine)

Sub-Component Software FMEA

FMEA Heading	FMEA Data
Failure:	Endless loop
Fault Location:	State machine (FPGA Logic)
Sub-Component Level Effect:	State machine caught in endless loop
Basic Component Level Effect;	No output or stuck output
Failure Type:	Fatal
Failure Set (FPGA FMEA):	State machine
Failure Set (Elementary Fault Class):	Software fault
Cause (FPGA FMEA):	Design defect
Cause (Elementary Fault Class):	Development
Lifecycle:	Design (development)
Mitigation Method(s):	State Machine Hazard Analysis (SMHA) Watchdog Timer (WDT)

Table 3: Software Sub-Component Level Failure Modes and Failure Effects (State Machine Endless Loop Example)

FPGA Taxonomy Uncovering Situations

Uncovering Situation	Fault Tolerance Feature
Online detection mechanisms	Revealed by EDAC methods
Spurious actuation	SEU: Memory upset causes values to read above a setpoint; causing a spurious trip.

Table 4: Uncovering Situations for Hardware Sub-Component Level (SEU Example)

Uncovering Situation	Fault Tolerance Feature
Online detection mechanisms	State machine endless loop caught by WDT. State machine returned to pre-defined state.
Offline detection mechanisms	Endless loop found and corrected by using state machine hazard analysis.

Table 5: Uncovering Situations for Software Sub-Component Level (State Machine Endless Loop Example)

FPGA Taxonomy Demonstration (1)

- Four step process[4]:
  1. Failure effects are assigned to the failure modes based on the FPGA taxonomy to allow for functional impacts and uncovering situations to be described
  2. Failure mode categories are defined based on failure effect(s), uncovering situation(s) and fault locations
  3. Fault end effects are described based on fault tolerance, fault location/detection, and functional impact
  4. Failure modes are grouped based on similar attributes, detection methods, and end effects

FPGA Taxonomy Demonstration (2)

- FPGA Taxonomy is demonstrated using digital RTS/ESFAS (Figure 3)
  - Specifically considers “Analog Input Module” (AIM)
- Taxonomy process is applied to hardware and software (HDL code) failure modes
- Demonstrated by:
  - FMEA tables
  - Fault trees (modelling)
- FPGA failure mode data applicable to wide variety of reliability analysis methods

Test System (Module Level)

Legend

AIM: Analog Input Module

DIM: Digital Input Module

PS: Power Supply

SCM: Signal Conditioning Module

AOM: Analog Output Module

DOM: Digital Output Module

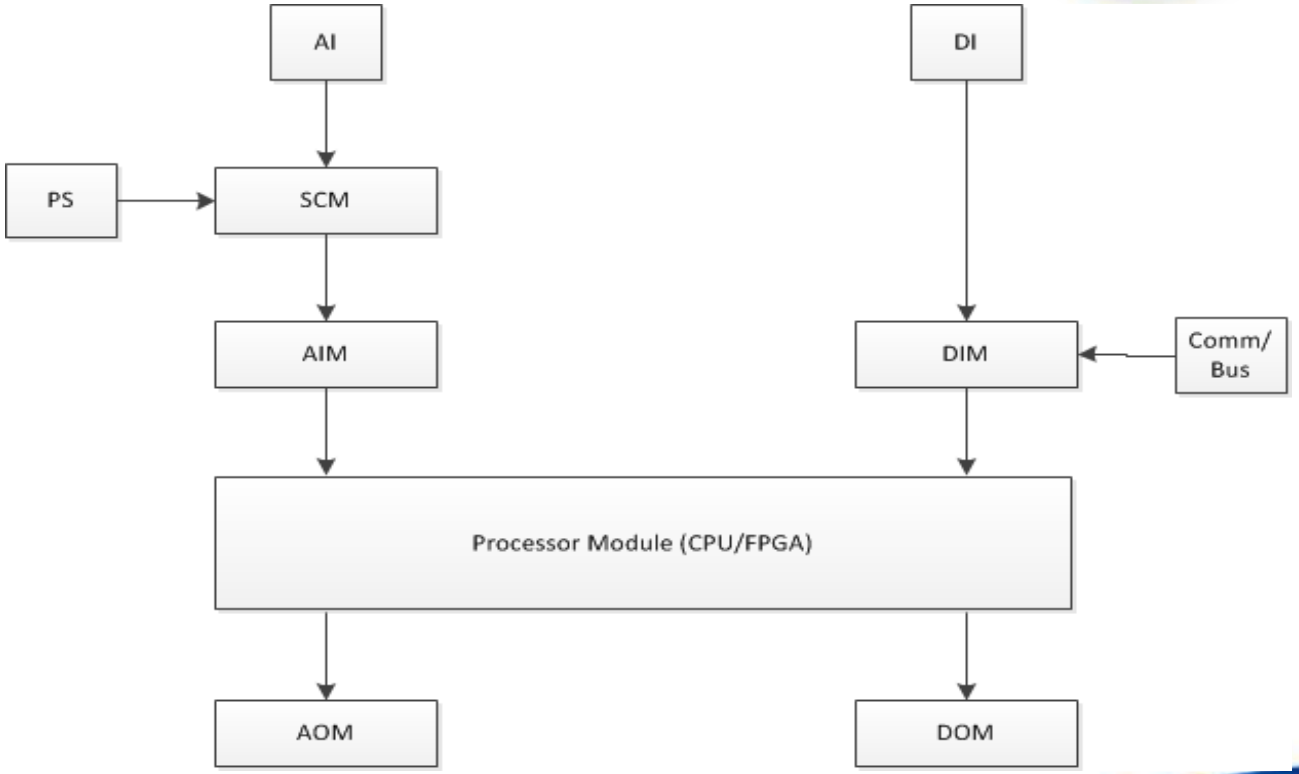


Figure 10: Test System (Module Level)[4]

FPGA Taxonomy Hardware Demonstration FMEA Tables (Step 1)

Demonstration Heading	FMEA Data
Failure Mode:	Single Event Upset (SEU)
Hardware Module:	Register/flip-flop (storage element)
Failure Set (FPGA FMEA):	Radiation induced soft error
Failure Set (Elementary Fault Class):	Physical interference
Failure Effect:	Non-fatal (plausible or implausible)
Uncovering Situation:	Online detection
Functional Impact on “BC”:	Incorrect output (FPGA)
Functional Impact on “AIM”:	Incorrect output (AIM)
Mitigation Method(s):	Error Detection/Correction Codes (EDAC) Triple Modular Redundancy (TMR)

Table 6: Step 1 for the Hardware Sub-Component Level Taxonomy Demonstration (SEU Example)

FPGA Taxonomy Hardware Demonstration FMEA Tables (Steps 2-3)

Demonstration Heading	FMEA Data
Failure Mode:	Single Event Upset (SEU)
Hardware Module:	Register/flip-flop (storage element)
Failure Set (FPGA FMEA):	Radiation induced soft error
Failure Set (Elementary Fault Class):	Physical Interference
Compressed Failure Mode:	Loss of function or spurious function
Uncovering Situation:	Online detection
Failure Detection:	Self-monitoring or self-revealing
Functional Impact on “BC”:	Incorrect FPGA output
Failure End Effect (“AIM”):	Incorrect AIM output
Mitigation Method(s):	Error detection/correction, TMR

Table 7: Steps 2-3 for the Hardware Sub-Component Level Taxonomy Demonstration (SEU Example)

FPGA Taxonomy Hardware Demonstration FMEA Tables (Step 4)

Demonstration Heading	FMEA Data
Failure Mode:	Single Event Upset (SEU)
Hardware Module:	Register/flip-flop (Storage Element)
Failure Set (FPGA FMEA):	Radiation induced soft error
Failure Set (Elementary Fault Class):	Physical interference
Compressed Failure Mode:	Loss of function or spurious function
Failure Detection:	Monitoring or self-revealing
Failure End Effect (“AIM”):	Incorrect AIM Output (Loss of function or spurious function)
Failure End Effect (“RTS/ESFAS”):	1oo4 conditions of specific APU/VU according to Fault Tolerant Design (FTD)
Mitigation Method(s):	Error detection/correction, TMR

Table 8: Step 4 for the Hardware Sub-Component Level Taxonomy Demonstration (SEU Example)

FPGA Taxonomy Software Demonstration FMEA Tables (Step 1)

Demonstration Heading	FMEA Data
Failure Mode:	Endless loop
Hardware Module:	State machine (FPGA Logic)
Failure Set (FPGA FMEA):	State machine
Failure Set (Elementary Fault Class):	Software fault
Failure Effect:	Fatal (Haphazard)
Uncovering Situation:	Online detection
Functional Impact on “BC”:	No output or stuck output (FPGA)
Functional Impact on “AIM”:	No output or stuck output (AIM)
Mitigation Method(s):	State machine hazard analysis watchdog timer

Table 9: Step 1 for the Software Sub-Component Level Taxonomy Demonstration (State Machine Endless Loop Example)

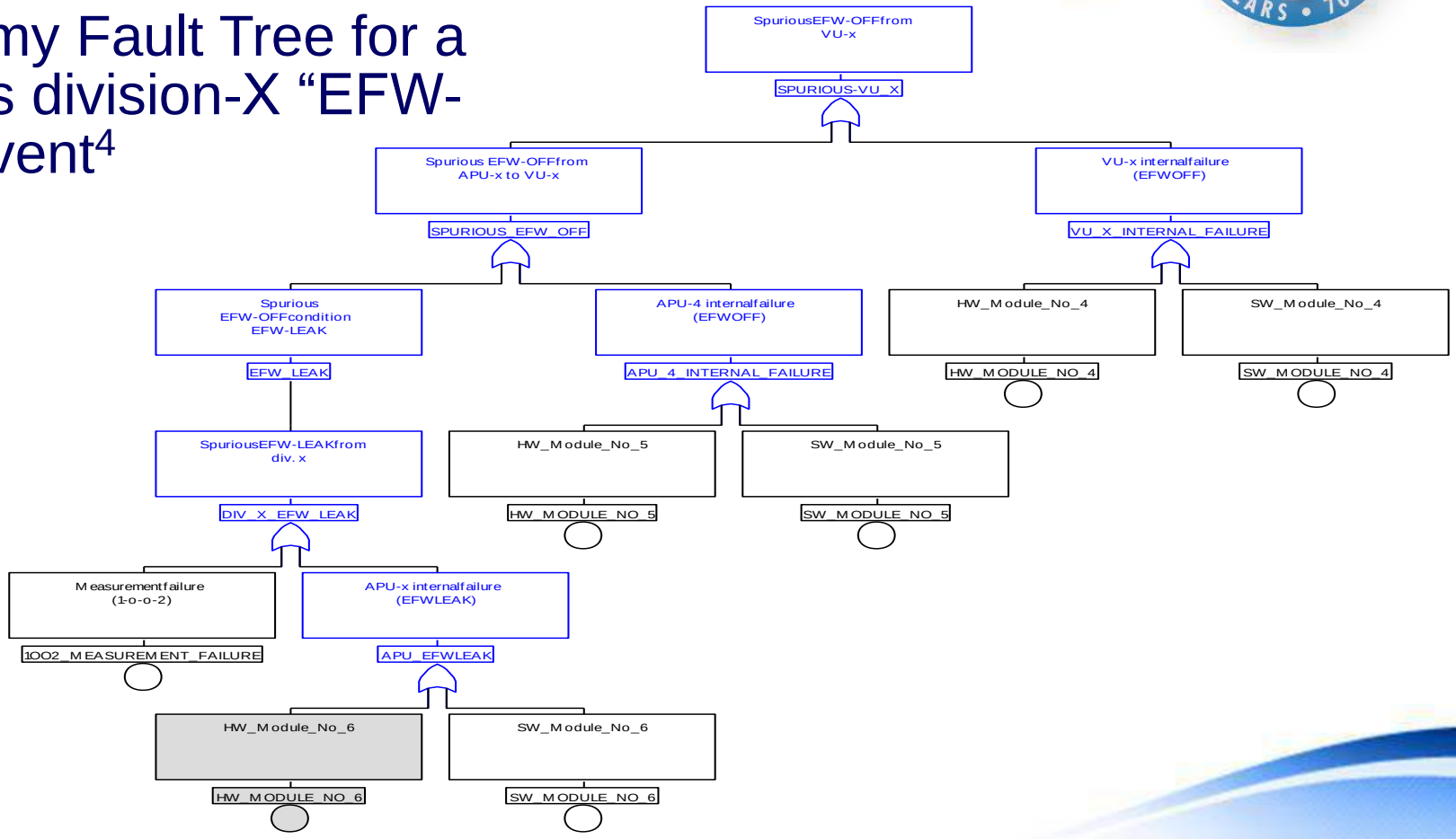
FPGA Taxonomy Software Demonstration FMEA Tables (Step 4)

Demonstration Heading	FMEA Data
Failure Mode:	Endless Loop
Hardware Module:	State machine (FPGA Logic)
Failure Set (FPGA FMEA):	State machine
Failure Set (Elementary Fault Class):	Software fault
Compressed Failure Mode:	Latent loss of function
Failure Detection:	Monitoring
Failure End Effect (“AIM”):	No output or stuck output (AIM)
Failure End Effect (“RTS/ESFAS”):	Loss of 1oo4 conditions of specific APU/VU outputs
Mitigation Method(s):	State machine hazard analysis watchdog timer

Table 10: Step 4 for the Software Sub-Component Level Taxonomy Demonstration (State Machine Endless Loop Example)

FPGA Taxonomy Demonstration: Fault Tree Modelling (1)

Figure 11: OECD-NEA Taxonomy Fault Tree for a spurious division-X "EFW-OFF" Event[4]



FPGA Taxonomy Demonstration: Fault Tree Modelling (2)

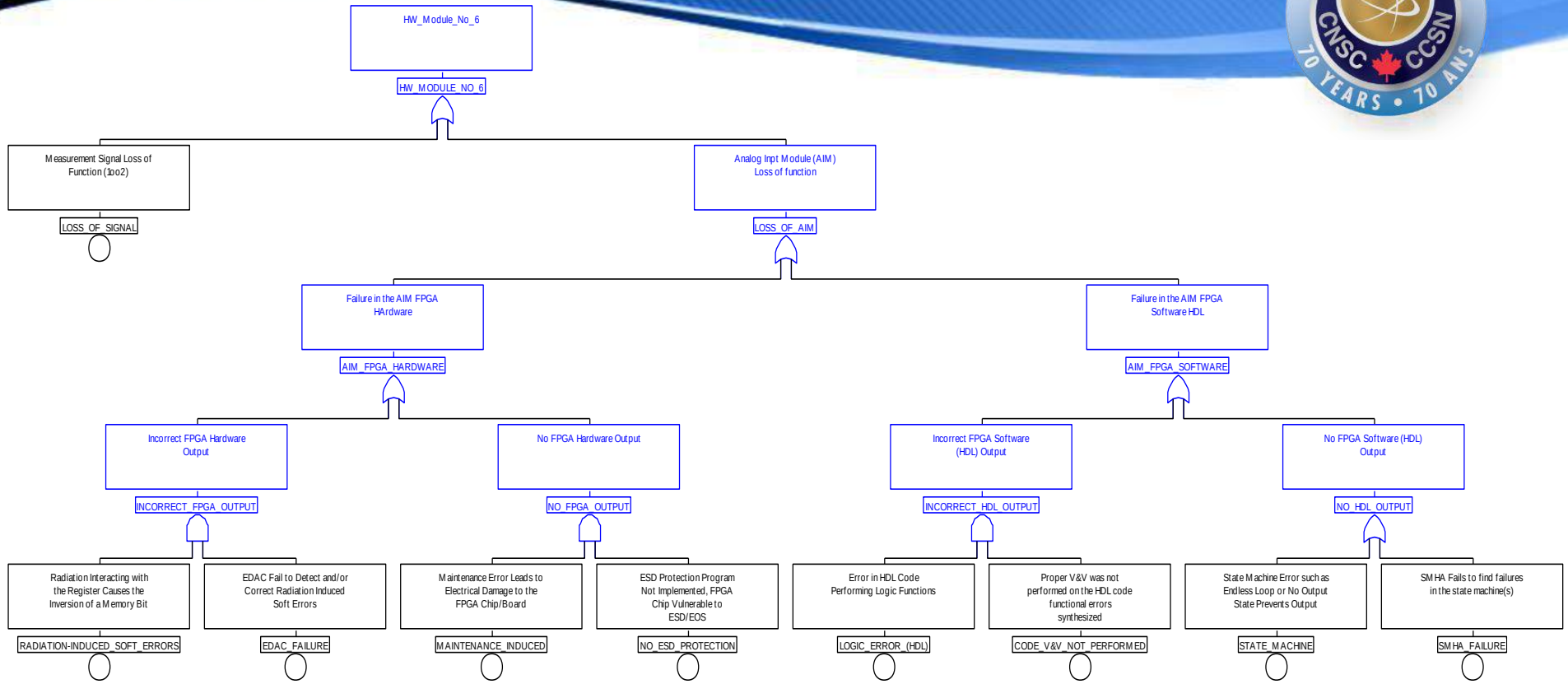


Figure 12: Fault Tree for HW Module #6 (Sub-Component Level) using Failure Categories

Conclusion

- FPGAs are expected to see increased use in NPPs
- Extensive FMEA performed to categorize failure modes
- Created FPGA taxonomy to interface with OECD-NEA digital failure modes taxonomy
  - Completes important aspects of future work
  - FPGA taxonomy useful to working groups
- Taxonomy demonstration using FMEAs and fault trees
- Further work performed using FMEA data on the comparison of reliability analysis methods[8]

References

[1] International Electrotechnical Commission (IEC), 60812, *Analysis Techniques for System Reliability- Procedures for Failure Mode and Effects Analysis (FMEA),* Geneva, 2006.

[2] McNelles, P., Zeng, Z.C., Renganathan, G., 2015, “Modelling of Field Programmable Gate Array Based Nuclear Power Plant Safety Systems Part I: Failure Mode and Effects Analysis”, *Proc. Of the 7th International Conference on Modelling and Simulation in Nuclear Science and Engineering*, Ottawa, Canada.

[3] Avizienis, A., Laprie, J. C., Randell B., and Landwehr, C., "Basic Concepts and Taxonomy of Dependable and Secure Computing," in *IEEE Transactions on Dependable and Secure Computing*, vol. 1, no. 1, pp. 11-33, January-March 2004.
doi: 10.1109/TDSC.2004.2.

[4] OECD-NEA, *Failure Modes Taxonomy for Reliability Assessment of Digital I&C Systems for PRA,* France, 2015.

References continued

[5] OECD-NEA, Recommendations on Assessing Digital System Reliability in Probabilistic Risk Assessment of Nuclear Power Plants, France, 2009.

[6] AP1000 Design Control Document (Revision 15), Chapter 7: Instrumentation and Controls, Westinghouse, http://pbadupws.nrc.gov/docs/ML1117/ML11171A500.html>

[7] Electric Power Research Institute, Design Description of a Prototype I implementation of Three Reactor Protection System Channels Using Field-Programmable Gate Arrays, Oak Ridge Tennessee, 1997.

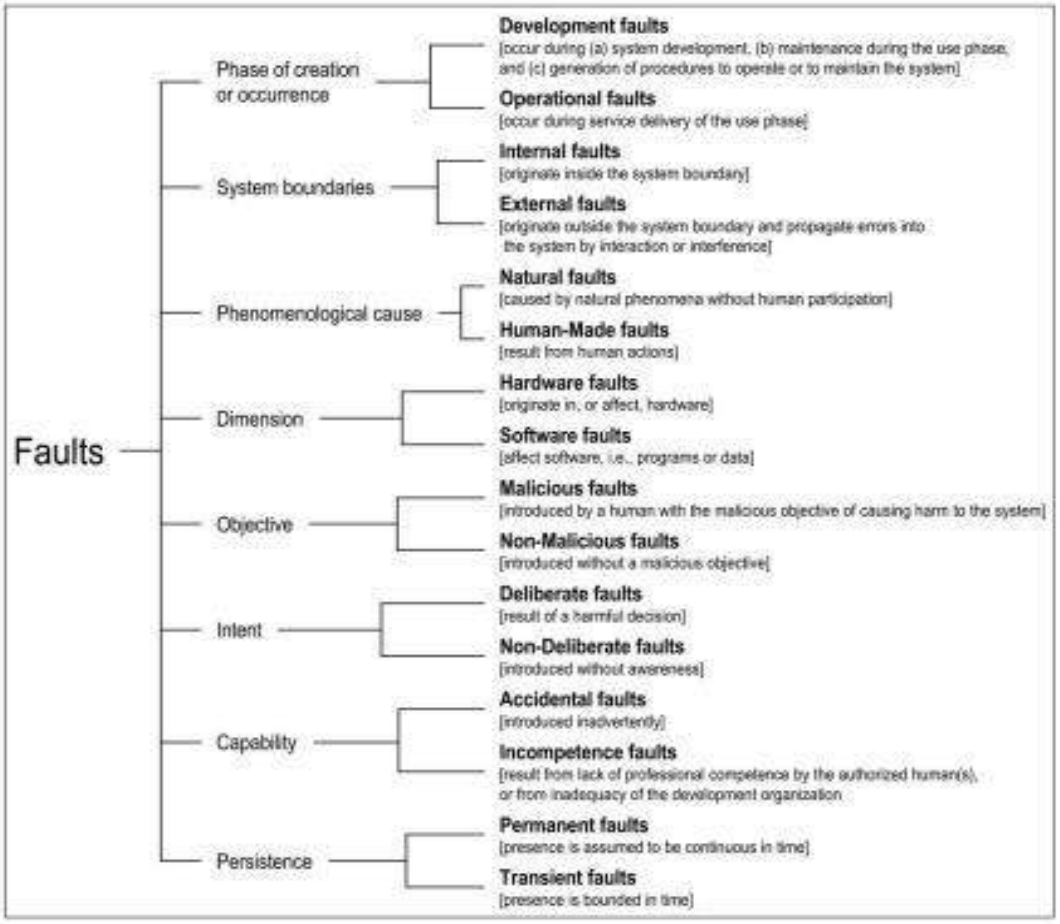
[8] P. McNelles et al., 2016, A Comparison of Fault Trees and the Dynamic Flowgraph Methodology for the Analysis of FPGA-based Safety Systems Part 1: Reactor Trip Logic Loop Reliability Analysis, Reliability Engineering and System Safety. DOI: doi:10.1016/j.ress.2016.04.014

Thank you for your time.

Questions?

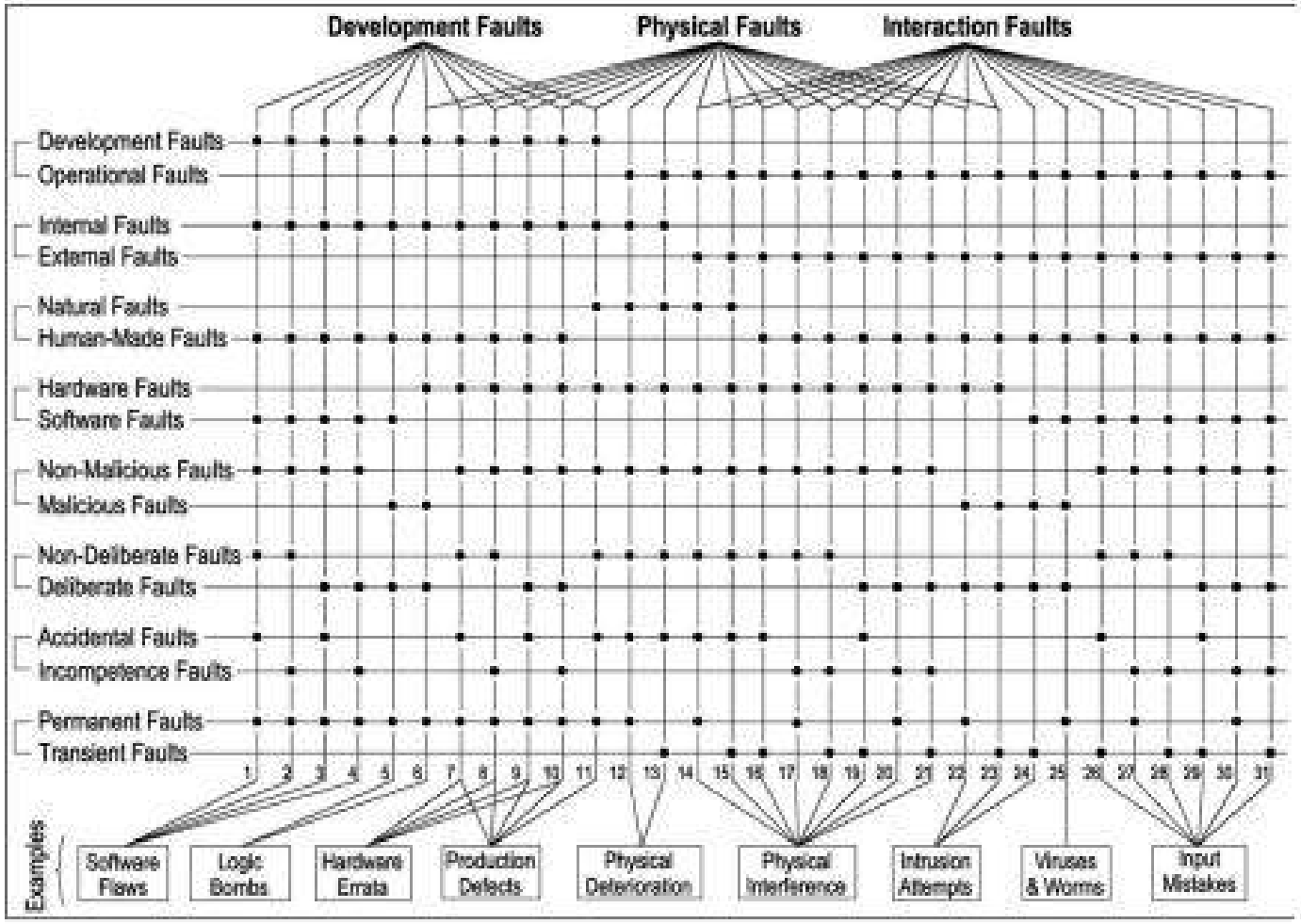
Contact: phillip.mcnelles@canada.ca

Appendix



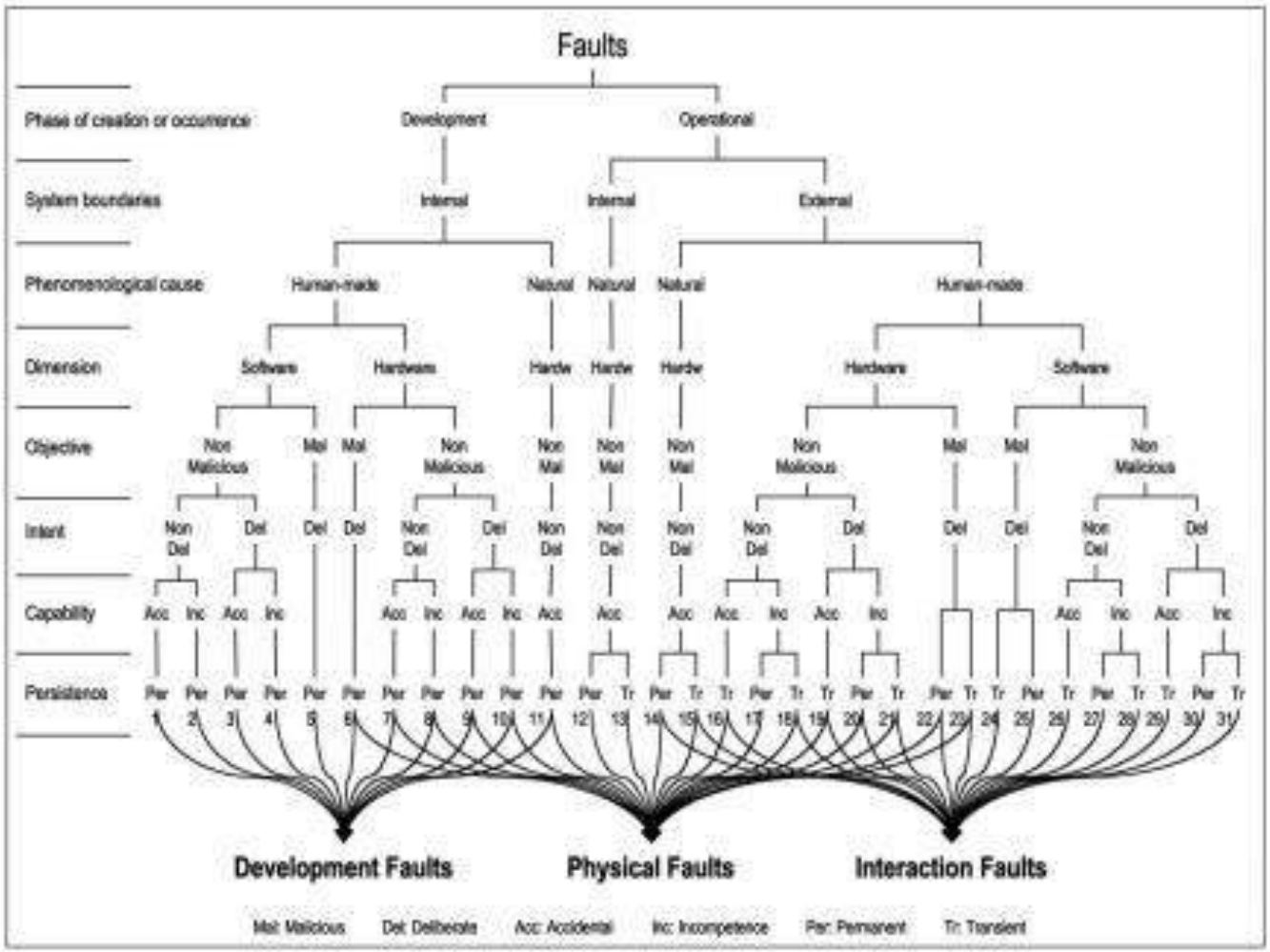
Elementary Fault Classes[3]

Appendix



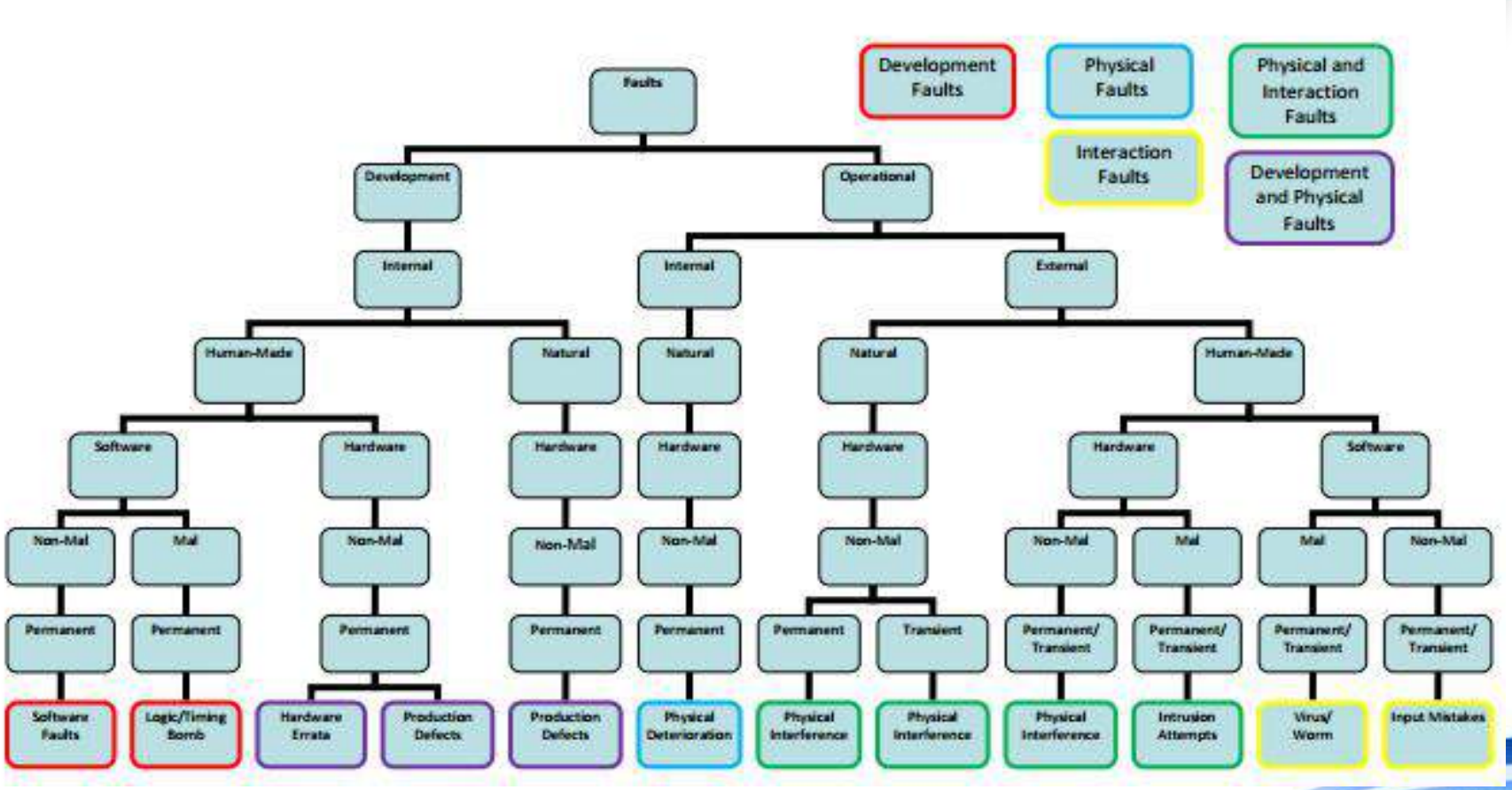
Combined Fault Classes (Matrix Representation)[3]

Appendix



Combined Fault Classes (Tree Representation)[3]

Appendix



Elementary Fault Classes
(FPGA Taxonomy Paper)