Canadian Nuclear Safety Commission
Commission canadienne de sûreté nucléaire

Failure Mode and Effects Analysis of FPGA-Based Nuclear Power Plant Safety Systems

Phillip McNelles, Zhao Chang Zeng, and Guna Renganathan

8th International Workshop on the Applications of FPGAs in NPPs

Shanghai, China
October 13-16, 2015

Canada

Presentation Outline

- Introduction
  - Potential use of FPGAs in Canadian NPPs
- FMEA
  - Purpose of performing FPGA FMEA (Research Program)
  - FMEA Background
  - FMEA Results
  - Failure Mode Categorization
    - Failure Categories
    - “When and Why” Matrix
    - Failure Types and Parameters
  - Design Suggestions
- Conclusions

Introduction

- Nuclear Power Plants (NPPs) in Canada constructed 1971-1992
  - FPGAs not implemented in NPPs at that time
  - 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)

- If FPGA-based systems are implemented in safety systems:
  - Must be functionally safe and reliable
  - Potential faults and failures must be known

- 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

Failure Mode and Effects Analysis

- Failure Mode and Effects Analysis (FMEA)
  - Common Method in Reliability and Safety Analysis
  - Start of Reliability Program (Study)
  - Reviewed available data from international community (Extensive Literature Review)

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

Failure Mode and Effects Analysis

- Failure Mode and Effects Analysis (FMEA)
  - Performed on FPGAs to identify Failure Mode data
    - Potential Failure Modes
    - Cause(s)
    - Potential Effects on FPGA-based system
    - Effects of Latent Design Errors
    - Eliminate or Mitigate/Control Failure Modes
- Produced a list of failure modes and information
  - Identify most common/most severe failures

FMEA Results

- Identified potential issues
  - Failure modes, faults, logic errors, human factors…
- Failures divided into categories
  - 1st : Lifecycle: “Design (Fabrication)”, “Operation”
  - 2nd : Cause: “Design Defect”, “Manufacturer Defect”, “Environmental”, “Stress/Aging”, “Maintenance (Human Factors)”
- Causes, potential effects, and methods to eliminate/mitigate those failures for each set

FMEA Results

- Design Defect:
  - Logic (“Programming”), Hardware Faults
- Manufacturer Defects:
  - Failures due to issues with the physical chip/board
- Environment:
  - Radiation induced failures (SEE)
- Stress/Aging:
  - Aging Effects
- Maintenance/Human Factors:
  - Personnel/Security

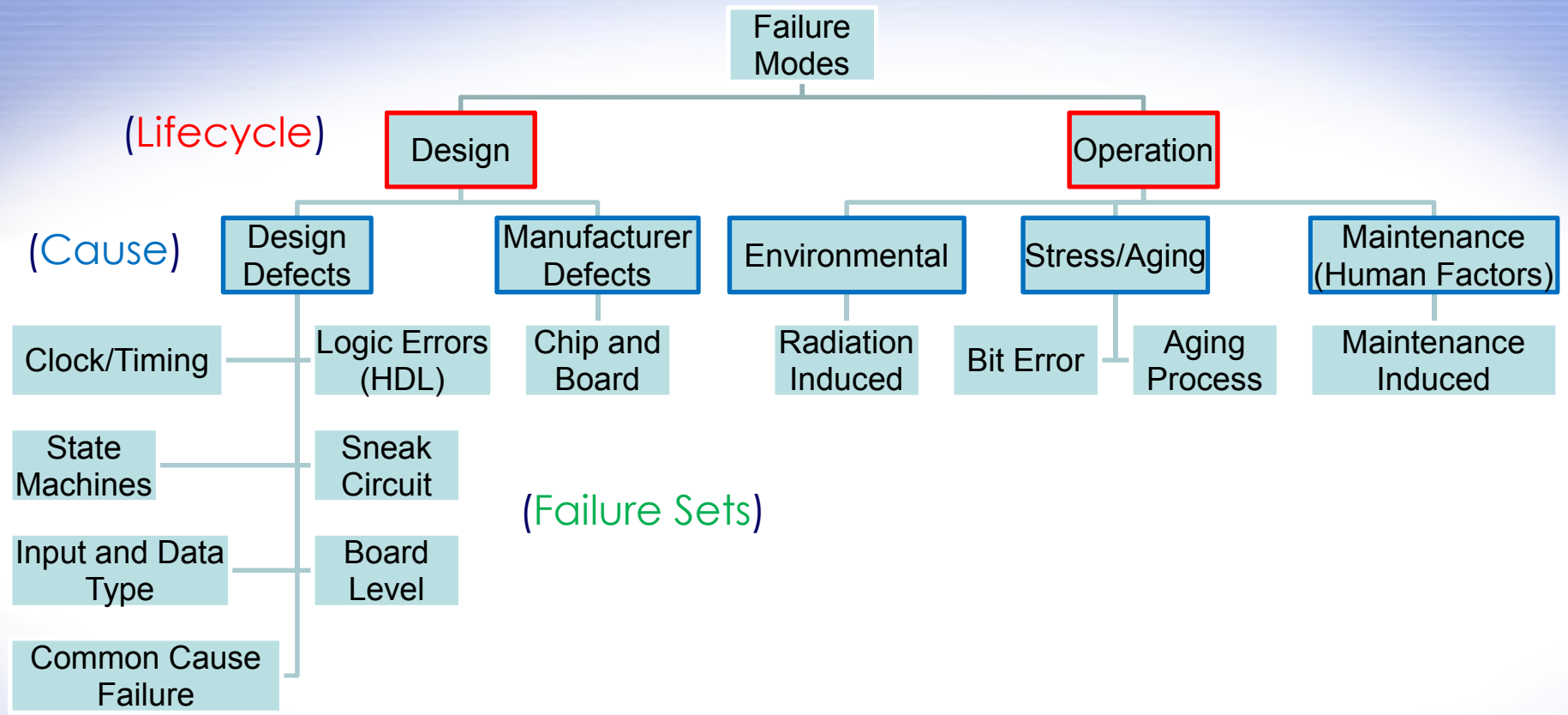
FMEA Results

- Certain failure modes specific to FPGA
  - Clock/timing failures
    - Significance of proper clock/timing behavior
    - Optimization by synthesis software may alter intended behavior
- Certain failure modes common to digital technology
  - Single Event Effects (SEE)
    - Importance of SEE mitigation
  - Programming Errors (HDL code)
    - FPGA design has some similarities with software-based design
    - Non-standard language additions may introduce failures
  - Aging Failures

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)
  - Each set includes a description and mitigation
  - Grouped for easier identification and mitigation

FMEA Results (Failure Sets)



Failure Category Diagram

FMEA Results (Failure Sets)

- Sample of Failure Sets
- Design
  - Clock/Timing
  - State Machines
  - Common Cause Failure
  - Logic Errors (HDL)
- Operation
  - Aging Process Failures
  - Radiation-Induced Failures

FMEA Results (When and Why Matrix)

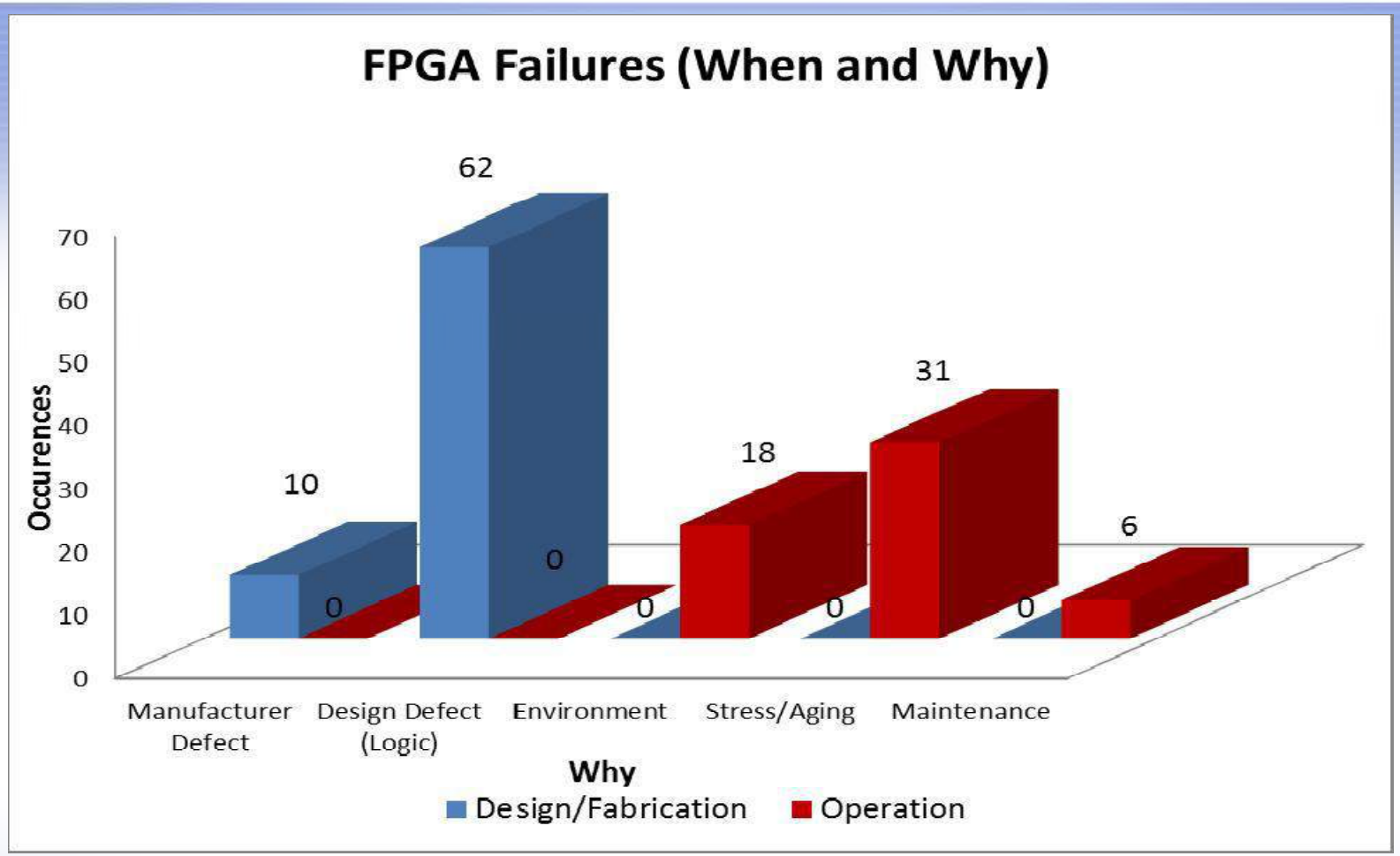
- Additional way to categorize failure modes
  - Presented in “When and Why” Figure
- When:
  - Stage in system lifecycle that the failure occurs
- Why:
  - Failure Category (Failure Modes)

FMEA Results (When and Why Matrix)

- Lifecycle Categories (“When”):
  - Design (Fabrication)
  - Operation

- Cause Categories (“Why”):
  - Design Defects
  - Manufacturer Defects
  - Environmental
  - Stress/Aging
  - Maintenance (Human Factors)

FMEA Results (When and Why Graph)



FPGA FMEA "When and Why" Results

FMEA Results (When and Why Results)

- Two important results from the graph
- "Design Stage" had most results (73)
  - Includes Logic, Timing and general Hardware faults
  - "Design Defect" most populous category
  - Most failures eliminated before implementation
- Stress/Aging Failure Mitigation
  - Aging process failures cannot be avoided
  - Revealed using self-tests and periodic testing

Failure Types and Parameters

- Failure Causes divided into “Types” and “Parameters”

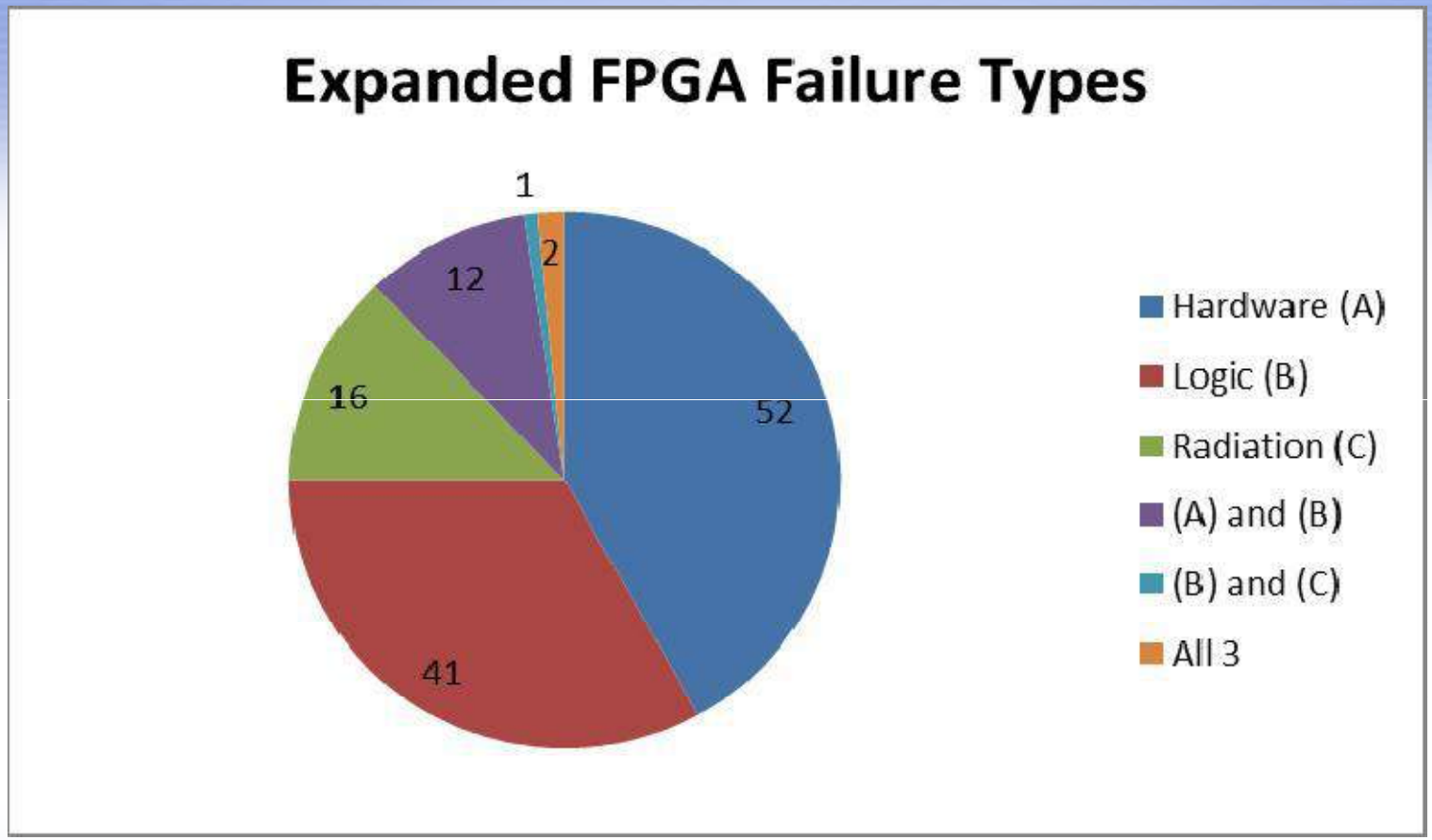
Failure Type	Definition
A	Hardware Failure
B	Logic Failure
C	Radiation Failures

FPGA Failure Types

Failure Parameter	Definition
V	Electric
T	Temperature
M	Material
S	Chip size
R	Radiation Failures
L	Logic Failure
H	Hardware (General)

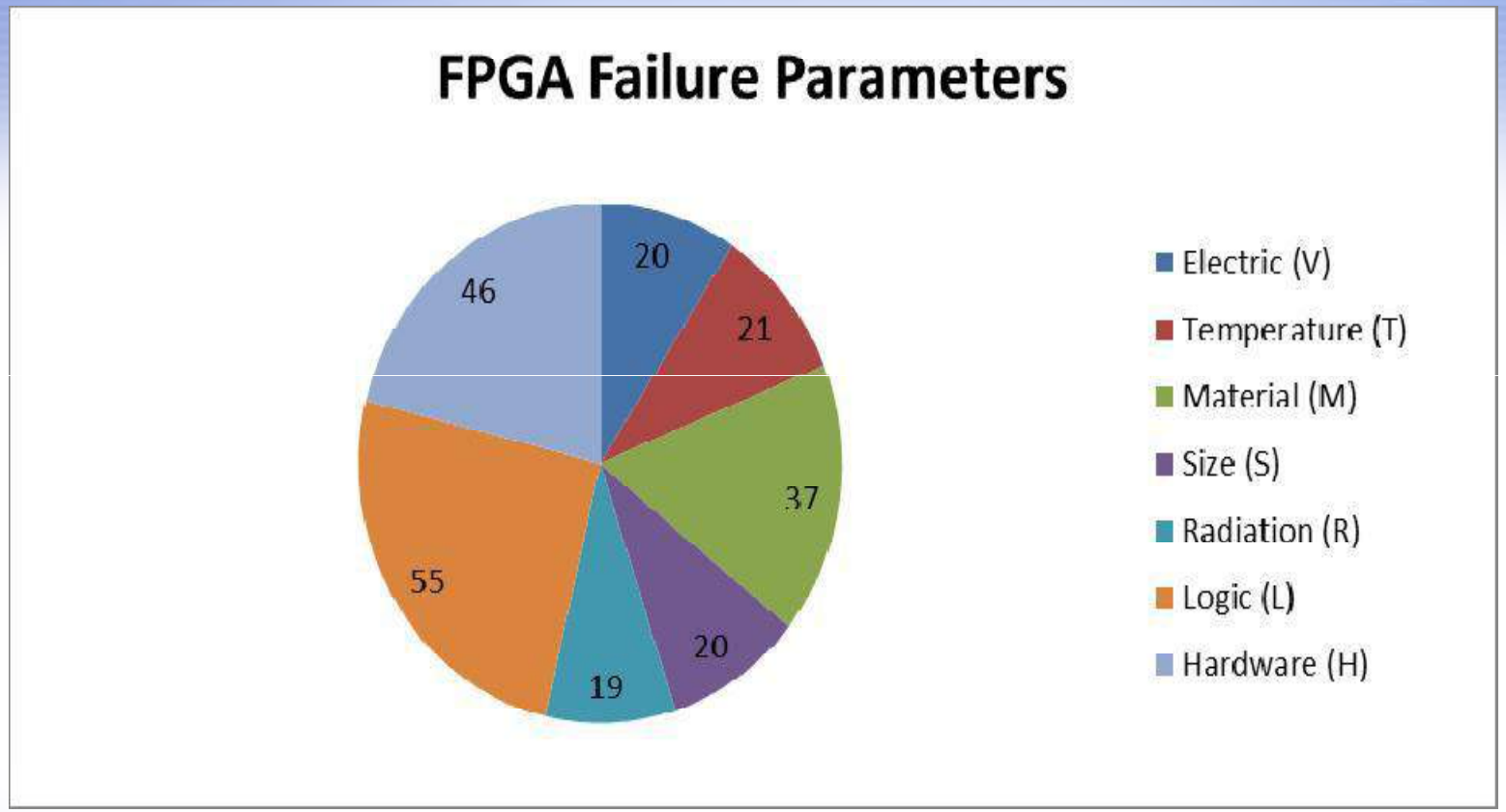
FPGA Failure Parameters

Failure Types and Parameters



FPGA Failure Types

Failure Types and Parameters



FPGA Failure Parameters

Failure Type and Parameter Results

- "Failure Type" Results:
  - Hardware Faults most numerous (52)
  - More Hardware and Logic faults than Radiation
  - Significant overlap (Timing, Common Cause)

- "Failure Parameter" Results:
  - Shows in detail the factors affecting FPGA reliability
  - Hardware (Aging Process) failures show strong environmental dependency
  - FPGA material (technology) affects both Hardware and Radiation failures

Design and Review Suggestions

- Research provided suggestions for design and review of FPGA systems
  - Design Suggestions
    - Use of Antifuse FPGAs for radiation tolerance
    - Use of synchronous designs
    - Use of self-tests to monitor FPGA chip health
    - Use of coding standards/guides to prevent logic errors

Design and Review Suggestions

- Research provided suggestions for design and review of FPGA systems
  - Review Suggestions
    - Review system for tolerance of radiation effects
      - Design should eliminate effects of SEE (where possible)
      - Design should mitigate any effects of residual SEE
    - Review system for mitigation of aging effects
      - Design should incorporate methods to detect aging failures (Self-tests)
      - Design should include mitigations for effects of residual aging failures

Conclusions

- Detailed FMEA was performed to identify:
  - Failure modes, causes, and effects
  - Expanded to include avoidance and mitigation

- FMEA Categorization
  - Categories facilitate detection and avoidance/ mitigation of failure modes
    - Failure modes divided by Lifecycle (“Design” and “Operation”)
    - Lifecycle failure modes divided by “Causes”
    - “Failure sets” group failure modes by similar cause/effects
    - Failure “Types” and “Parameters” provide additional information on root cause of failure modes

Conclusions

- Additional Conclusions from FMEA Study
  - Many failure modes not specific to FPGAs
    - Common to digital technology
  - FPGA design shares aspects of software-based design
  - Clock and timing behavior critical to correct operation
  - Non-standard languages can introduce failure modes
  - Synthesizer code optimization features are to be avoided

Conclusions

- Primary Results
  - Methods to avoid or mitigate all identified failure modes
  - Majority of failures during the design stage (eliminated)
  - Several aging failures that must be mitigated (self tests and periodic tests)
  - Hardware (aging) failures have environmental factors
  - Large number of potential logic and timing errors

Future Work

- Future work on FPGA-based systems:
  - Failure mode information utilized for FPGA-based system modelling and analysis
  - Comparison of reliability analysis methods
  - Defenses against SEE failures
    - (Error Correcting Codes, Modular Redundancy, etc.)

The End

- Thank you for your time
  - Questions?

References

[1] 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.

[2] Bobrek, M., & Bouldin, D., *Review Guidelines for FPGAs in NPP Safety Systems,* Oak Ridge, Tennessee, 2010.

[3] United States Nuclear Regulatory Commission (U.S. NRC), NUREG-7006, *Review Guidelines for Field Programmable Gate Arrays in Nuclear Power Plant Safety Systems,* Washington D.C., 2010.

[4] Electric Power Research Institute (EPRI), TR-1019181, *Guidelines on the Use of Field Programmable Gate Arrays (FPGAs) in Nuclear Power Plant I&C System.* Palo Alto, California, 2009.

[5] EPRI, TR-1022983, *Recommended Approaches and Design Criteria for Application of Field Programmable Gate Arrays in Nuclear Power Plant Instrumentation and Control Systems,* Palo Alto, California, 2011.

[6] Valtion Teknillinen Tutkimuskeskus (VTT), *The current state of FPGA technology in the nuclear domain.* Vuorimiehentie, Finland, 2011.

Canadian Nuclear Safety Commission | Commission canadienne de sûreté nucléaire

Canadian Nuclear Safety Commission

nuclearsafety.gc.ca

facebook.com/CanadianNuclearSafetyCommission

youtube.ca/cnscccsn

CNSC CCSN

Canada