Canadian Nuclear Safety Commission | Commission canadienne de sûreté nucléaire

Dynamic Reliability Analysis of Radiation Induced Failure Modes in FPGA-based 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
  - Digital system reliability modelling
- Dynamic Reliability
  - Dynamic Flowgraph Methodology (DFM)
  - Background, Theory and DFM Software (Dymonda)
  - DFM/Fault Tree Comparison
  - FPGA-based Test System
  - DFM/Fault Tree Comparison Results
- Conclusions

Introduction

- Modern reliability methods include dynamic (time-dependent) properties
- Designed to model and analyze modern digital instrumentation and control systems
- Potential for more accurate modelling of FPGA-based systems
- Dynamic modelling of test systems and comparisons with Fault Tree results
- Method chosen was the “Dynamic Flowgraph Methodology” (DFM)

Research Purpose

- Compare traditional and modern safety analysis methods for analysis of FPGA-based I&C systems
  - Compare similarities/differences
  - Evaluate strengths/weaknesses of each method

DFM Background

- Dynamic Flowgraph Methodology
- Inductive and Deductive Analysis
- Dynamic (Time Dependence)
- Equivalent of Fault Tree and FMEA in one model
- Probabilities and Uncertainties
- Used in Nuclear and Aerospace Applications
- ASCA Inc. (Applied Science Consulting Firm)
- Dymonda Software
- VTT (Finland) created a separate version

DFM Background (Models)

- Directed Graph Model (Signal Flow Graph)
  - All DFM models contain nodes, transfer boxes, edges
- Nodes:
  - Process Variables
- Transfer/Transition Boxes:
  - Describe relationship/transfer function (Transition Tables)
- Edges
  - Connect Nodes/Boxes

DFM Background (Rationale)

- Time Dependant
  - Feedback
  - Control Loops
- Multi Valued Logic (MVL)
- Complete System Model
- Issues
  - Computationally intensive (“State Explosion”)
  - Need detailed information

DFM Theory

- Minimal Cut Set (MCS)[1,2]
  - A set of events that cause the top event if they occur (Cut Set)
  - A cut set that does not contain other cut sets as a subset (MCS)

$$MCS_j = \bigcap_{i=1}^{n} X_i^{(j)} = \prod_{i=1}^{n} X_i^{(j)} \quad (1)$$

$$TOP = \bigcup_{j=1}^{m} MCS_j = 1 - \bigcap_{j=1}^{m} (1 - MCS_j) = 1 - \prod_{j=1}^{m} (1 - MCS_j) \quad (2)$$

DFM Theory

- Multi Valued Logic
  - Each node has an arbitrary number of states
  - Prime Implicant (PI) is the MVL version of MCS

- Base:
  - Set of PIs that are the logical analog of the TOP function
  - Irredundant Base: Not a base if any PI removed
  - Complete Base: All PI for that Top Event

DFM Theory

- Restrictions on DFM Analysis
  - Physical Consistency Rules
  - Variable must take on one state
  - Cannot have multiple states (per time step)
  - Sum of PI gives Top Event[1,2]

$$\bigcup_{i=1}^{n} A_i = T \tag{3}$$

$$A_i \bigcap A_j = F, for\ i \neq j \tag{4}$$

$$Top\ Event = PI_1 \mathrm{V} \ldots \mathrm{V}\ PI_n \tag{5}$$

DFM Theory and Dymonda (Software)

- Timed Fault Tree (TFT) Construction
  - System backtracks through model from top event
  - Order based on model's logical sequence

- Timed Prime Implicant (TPI) Identification
  - Software creates "Critical Transition Table"
  - Logic reduction operations produce PIs

Dymonda Features (Software)

- Dynamic Consistency Rules
  - Increasing/Decreasing
  - Rate Rules
  - Sink States
- Probabilities and Uncertainties
- Exact Quantification (EQ)
  - Standard DFM probability is the sum of all PI
  - Convert PI to “Mutually Exclusive Implicants” (MEI)

DFM vs Fault Tree Comparison

- DFM/Dymonda designed to model digital control systems
  - FPGA-based systems are digital systems
  - Potential for better modeling and analysis
- Little information on comparisons between results from Fault Tree Analysis (FTA) and DFM models[2]
- More research should be done to compare these methods
- CAFTA software (EPRI) used to create fault trees for comparison

DFM vs Fault Tree Comparison

- Some Comparisons from US NRC documents
- "…the application of the DFM or Markov/CCMT techniques has been capable of identifying several risk relevant sequences that were not included in conventional PRA models."[3]
- "…, the ET/FT approach has been found to overestimate the predicted Top Event frequencies"[4]

DFM and FTA (Preliminary Comparison)

- Preliminary DFM/FTA Comparisons
  - Static systems
  - Simple dynamic systems (register)

  – Preliminary Results
    - Same results for static systems
    - Very similar results for simple dynamic systems

- Next phase involved a more complex dynamic system

Test System

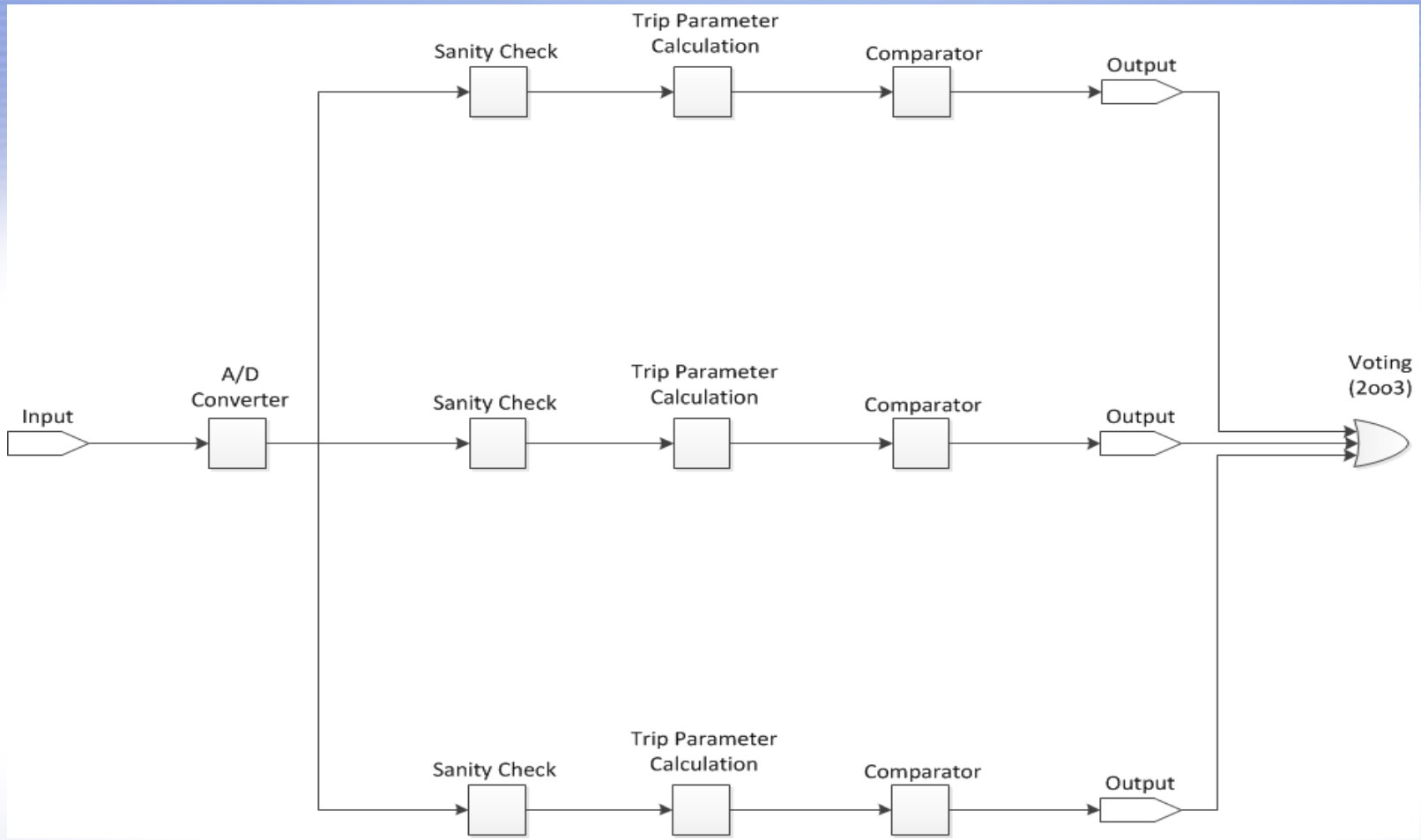
- Modelling will be performed on a test system
  - Reactor Trip Logic developed with a reference to:
    - EPRI TR-109390[5]
    - Westinghouse AP1000 (Ch. 7)[6,7]
  - Sub-Systems include
    - Analog-to-Digital Converter (ADC)
    - Sanity Check (SC)
    - Trip Parameter Calculation (Overtemperature)
    - Comparator (COMP)

Test System

- Test System
  - Single Channel, Single Parameter (Over Temperature)
  - Three redundant circuits with voting logic

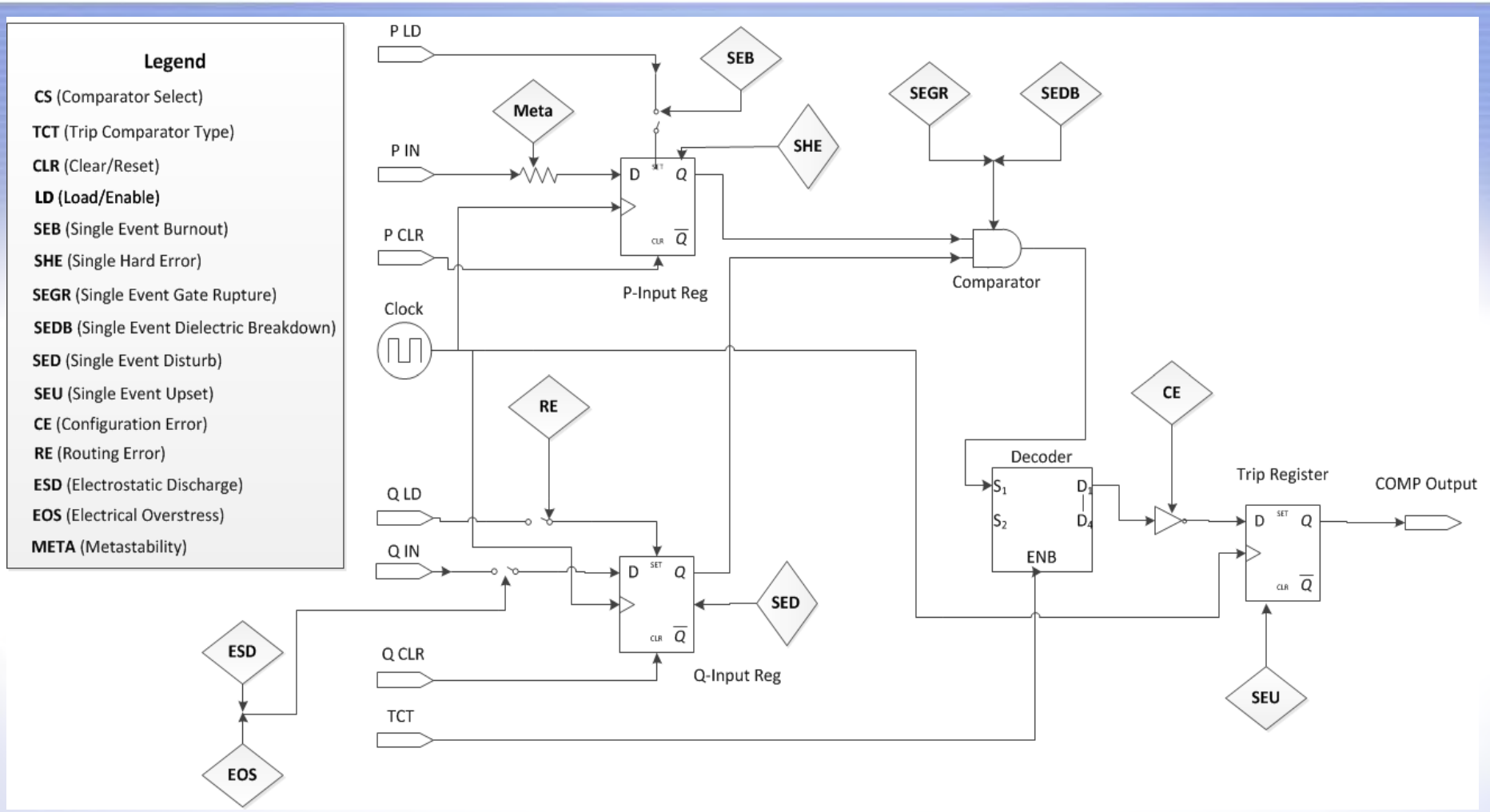
- Difference from US NRC Research
  - NRC project took a macroscopic approach
    - Complete system (Computer, Valve, Pumps, etc)
  - This project focused on design of FPGA-based systems
    - Considered registers, mux, decoders, logic gates, etc.
    - Failure modes due to SEE, aging process and human factors
    - Common Cause Failures (CCF) not included at this point

Test System Model (Overview)



High Level Block Diagram for FPGA-based Test System

Test System Model (COMP)



FPGA Comparator Flowgraph Model[5,6]

Test System Analysis

- Two Top Events
  - Spurious Trip
  - Missed Trip

- Comparison Included Several Factors:
  - Total Probability
  - Number of PI/MCS
  - Similarities/Differences between PI/MCS
  - Birnbaum Structural Importance (BSI) Measures

Comparison Results (Top Event)

Model	Clock State	CSG	DPC	MCS #
Missed Trip	1	6.67E-05	1.09E-05	1079
Missed Trip	0	1.27E-08	4.25E-09	9
Spurious Trip	1	1.35E-06	1.59E-06	663
Spurious Trip	0	2.03E-06	7.10E-07	69

FTA (CAFTA) Results

Model	SUM/MCSUB	EQ	PI #
Missed Trip	1.556E-05	1.554E-05	53
Spurious Trip	3.117E-05	3.116E-05	63

DFM (Dymonda) Results

Nomenclature:

CSG (Cut Set Generator)
DPC (Direct Probability Calculator)
MCSUB (Minimal Cut Set Upper Bound)
EQ (Exact Quantification)

Comparison Results (PI/MCS)

(Error States Shown in Red)

Node	State	Time Step	Probability
Clock	1	-1	N/A
SEGR	SEGR_Fail	-1	5.95E-04
SEU (T)	No SEU	0	N/A
Circuit "B"	0	0	2.285E-03
PI Probability:			1.359E-06

Similar PI/MCS
(Missed Trip)

Node	State	Time Step	Probability
Clock	0	-1	N/A
Trip_Reg (Prev)	1	-1	N/A
SEU (T)	SEU	0	6.53E-05
Circuit "C"	0	0	2.285E-03
PI Probability:			1.492E-07

Different PI/MCS
(Missed Trip)

Comparison Results (BSI)

Birnbaum Structural Importance (BSI):

- Compares relative component importance
- Number of PI/MCS containing a node/state divided by the total number of PI/MCS
- Does not require probabilities

Node	DFM	FTA (Clock 0)	FTA (Clock 1)
SEU (T)	0.981	0.996	0.999
CE (D)	0.825	0.996	0.999
SHE (P)	0.698	0.996	0.998
SED (Q) (DFM)	0.667	0.98	0.997
SEGR (FTA)	0.475	0.996	0.998
SEDB (FTA)	0.475	0.996	0.998

Node BSI Comparison

Potential Differences

- Potential reasons for differences between DFM and FTA results:
  - Initial Conditions
  - Time Steps
  - Retention
  - Circular Logic
  - Truncation

Conclusion

- DFM is a form of Time-Dependent reliability analysis that can be performed using the Dymonda software
- FMEA data used to inject failures into test system
- FTA and DFM analysis performed on test system
- Preliminary Results:
  - Similar results for static and simple dynamic systems
  - Noticeable differences for large, dynamic systems
  - Future work including
    - Common Cause Failures
    - Quantitative Measures (Sensitivity, Importance measures)

References

[1] ASCA Inc., 2013, Dymonda 7.0 Software Guide, ASCA Inc., Redondo Beach, California.

[2] Chu, T.L. et al, 2009, *Modeling a Digital Feedwater Control System Using Traditional Risk Assessment Methods*, U.S. Nuclear Regulatory Commission, Washington D.C.

[3] Aldemir, T., Guarro, S., Kirshenbaum, J., and et, al, 2009, *A Benchmark Implementation of Two Dynamic Methodologies for the Reliability Modeling of Digital Instrumentation and Control Systems*, U.S. Nuclear Regulatory Commission, Washington DC.

[4] Aldemir, T., Miller, D. W., Stovsky, M. P., and et, al, 2006, *Current State of Reliability Modeling Methodologies for Digital Systems and Their Acceptance Criteria for Nuclear Power Plant Assessments*, U.S. Nuclear Regulatory Commission, Washington DC.

[5] Electric Power Research Institute, (EPRI),1997, *Design Description of a Prototype Implementation of Three Reactor Protection System Channels Using Field-Programmable Gate Arrays*, EPRI, Oak Ridge Tennessee.

[6] AP1000 Design Control Document (Revision 15), *Chapter 7: Instrumentation and Controls*, Westinghouse.

[7] Park, Jin-Ho et al, 1992, *Optimization of Dynamic Terms in Core Overtemperature Delta-T Trip Function, Korea Atomic Eenrgy Research Institute, pp. 236-242..*

The End

- Thank you for your time
  - Questions?

E-mail: phillip.mcnelles@canada.ca

Canadian Nuclear Safety Commission | Commission canadienne de sûreté nucléaire

Canadian Nuclear Safety Commission

nuclearsafety.gc.ca

facebook.com/CanadianNuclearSafetyCommission

youtube.ca/cnscccsn

© CNSC Copyright 2013

CNSC CCSN

Canada