RIC 2011
How Do Safety Systems with Software Fail?

Sushil Birla
NRC/RES/DE

Pascal Regnier
IRSN/DSR/SAMS/BASEC

March 8, 2011

1

Outline

- Objective of the study
- Research method
- Comparative characterization
- Analytical findings
- Supporting examples from real life mishaps
- Interim inferences
- Some open questions
- Some next steps
  - Follow up investigation
  - Dissemination

2

Objective of the study

- Examine the role of Failure Mode and Effects Analysis **(FMEA)** and Fault Tree Analysis **(FTA)** in regulatory assurance of Complex Logic in DI&C safety systems
- Scope of the study:
  - Broadened from "Software" to "Complex Logic"
  - Narrowed to role in "regulatory assurance"

Concern: Fitness for the purpose of risk informing licensing review

ACRS ⟶ SRM

3

Research method

- Characterize, contrasting with hardware
- Analyze validity of applying traditional FMEA
- Validate analysis with examples from experience
- Find and analyze opposing viewpoints
- Draw conclusions
- Formulate direction of further investigations

4

Characterization

Traditional Hardwired Logic	Complex Logic
Inherently caused by physical degradation	Inherently caused by engineering defect
Simpler system; mature practice → Engineering & manufacturing defects easier to eliminate	Complex system; immature practice → Undetected engineering defects likely
Limited number of failure modes, well understood	Number of potential faults very high; not well understood. In a high-quality process actual number of faults is smaller
Fault propagation paths (functional ↔ physical) well understood	Many possible, unknown propagation paths; not well understood
Design can reduce occurrence-frequency but cannot eliminate faults	Design can eliminate all known faults

5

Analytical findings

- Potential faults in Complex Logic
  - Numbers very high;
  - Not well understood;
- Only a very small and unknown number of these potential faults are actually present in the logic

Faults propagation paths:
- Very large number
- Paths not visible from the functional point of view

6

Bruce-4 Reactor, Canada

January 1990: Small Loss of Cooling Accident
Culprit: Reactor refueling machine
Cause: Software fault

FMEA could not have identified this fault mode

FMEA limitations:
- Typically, source code is not analyzed
- Unfamiliar minutiae of the computing architecture
- Hard to find needle in a haystack

7

Palo Verde Reactor, USA

May 2005 Core Protection Calculator in Unit 2:
- Chance discovery of a safety significant fault

Cause: Software fault – misunderstood requirement

FMEA could not have identified this fault mode

FMEA limitations:
- Typically, source code is not analyzed
- Typically, code is not traced to actual needs
- Hard to find needle in a haystack

8

Telephone network, USA

January 90 AT&T's #4ESS Toll Switching:
- Major service outage in national network

Cause: Software fault

FMEA could not have identified this fault mode

FMEA limitations:
- Typically, source code is not analyzed
- Unfamiliar minutiae of the "C" programming language
- Hard to find needle in a haystack

9

Ariane 5 Rocket, Europe

June 1996 Ariane 501 Launcher self-destructed
Cause: Loss of guidance and attitude information
Culprit: Inertial reference system
Root cause: Software specification and design defects

FMEA could not have identified this fault mode

FMEA limitations:
- Typically, source code is not analyzed
- Unfamiliar minutiae of the "C" programming language
- Hard to find needle in a haystack

10

Interim inferences

- Don't depend on FMEA to assure complex logic
- Pursue improvement in other assurance techniques
- Clarify appropriate use of FMEA and FTA
  - Hazard analysis of complex systems

11

Some open questions

Under what verifiable conditions can design information be deemed dependable for use in safety assurance?

Examples of concerns:
- Incomplete, inconsistent, ambiguous requirements
- Inadequate or unverifiable architectural constraints

12

Some next steps

- Learn from "contrarian" viewpoints
  - Dr. Kwon, Korea Atomic Energy Research Institute (KAERI)
  - Herb Hecht, SOHAR
  - Robyn Lutz, Iowa State University
  - Pete Goddard, TRW ← Raytheon ← Hughes Aircraft Co.
- Publish NUREG/IA on IRSN-NRC collaborative work

Acronyms used

- ACRS – Advisory Committee on Reactor Safeguards
- AT&T – American Telephone & Telegraph
- EPRI – Electric Power Research Institute
- FMEA – Fault Mode Effects and Analysis
- FTA – Fault Tree Analysis
- KAERI – Korean Atomic Energy Research Institute
- IRSN – Institut de Radioprotection et de Sûreté Nucléaire
- NRC – U.S. Nuclear Regulatory Commission

Acronyms used (cont.)

- RES – Office of Nuclear Regulatory Research
- SOHAR – Software and Hardware Reliability
- SRM – Staff Requirement Memoranda