A Meta-Model-Based Approach for Semantic Fault Modeling on Multiple Abstraction Levels

M. Schwarz

M. Chaari, B.-A. Tabacaru, W. Ecker
Outline

- Motivation
- Objectives
- Limitations
- Concept
- Simulation
- Conclusion
Motivation - Applications

Electronic devices are crucial in many aspects of modern society, such as:

- Mobility
- Communication
- Health care
- Finance
Motivation - Challenges

- Error prone transistors, due to technology scaling
- Constant or increasing dependability requirements
- Increasing complexity in design & verification
- Early detection of sensitive

Dependability taxonomy after Laprie [1]
Motivation – Fault Injection

Well-known technique to measure the impact of resilience techniques [2]

- Deliberate insertion of faults into a system
- Determine system’s response
- Widely used at the logic gate level
- Missing fault models at higher abstraction levels
Objectives

A structured approach to define fault models:

- Enable early incorporation in the design process
- Reduce time-to-market
- Evaluate fault tolerance techniques at the fitting abstraction level
- Enhance fault injection for RTL- and TLM-layer
Limitations - Abstraction

“The action of factoring out unnecessary details, identifying relevant similarities between objects and synthesizing those facts into a concept or class”

Primary goals:

- Get a better understanding of complex structures
- Simplify tasks performed on complex structures

Abstraction is performed with a given field of application in mind
Limitations – Domain Specialization

Fault models must be tailored to the requirements of the targeted domain.
Concept – Meta-Model

“An explicit model of the constructs and rules needed to build specific models within a domain of interest”
Concept – Meta-Model

*Ontological meta-model* [3] serves as common foundation for libraries:
- Enables automatic code generation
- Reusability

Bit-flip as smallest observable change:
- Resilience articulation point [4]
- Creation of accumulated models of higher order

Source: Herkersdorf, A. et al.: Resilience articulation point (RAP) [4]
Concept - Threats

Threats: faults, errors and failures
Target: Valid application points for threats
**Concept - Domain**

Domain: Areas of interest and/or functionality
Simulation – General Framework
Simulation - Flow

Automatic construction of the meta-model-related frameworks via the *Metagen* [5] code generation tool
Simulation - Setup

Target System
- 32-bit MIPS-architecture
- Automatic testbench generation

Simulation
- Fault injection
- Randomized workload
- One campaign per VHDL module
- 300 unique runs / campaign

Result
All observed errors were covered by the defined fault models
Conclusion

- A systematic approach
- Implicit assumptions during abstraction → specialization
- Fault models can be aggregated
- New layer of semantic information
- The meta-modeling-based approach enables formalization of fault models
Questions

Finalize slide set with questions slide
References


Contact Information

TU Kaiserslautern:
Michael Schwarz  
Schwarz@eit.uni-kl.de

Infineon Technologies AG:
M. Chaari  
Moomen.Chaari@infineon.com

B.-A. Tabacaru  
Bogdan-Andrei.Tabacaru@infineon.com

W. Ecker  
Wolfgang.Ecker@Infineon.com