Formal and Simulation Methods Unite to Rescue the Damsel in Distress – "Unclassified Faults"

Siri Rajanedi, Prashantkumar Ravindra
Analog Devices

accellera SYSTEMS INITIATIVE

2025 DESIGN AND VERIFICATION™ DVCON CONFERENCE AND EXHIBITION UNITED STATES
SAN JOSE, CA, USA
FEBRUARY 24-27, 2025

INTRODUCTION

- Functional Safety (FuSa) ensures system's correctness and failure management
- Fault Injection (FI) evaluates the Diagnostic Coverage (DC), fault effects
- DC helps to assess the effectiveness of the Safety Mechanism
- Unclassified faults are the faults that are Unobserved functionally and Undetected by Safety Mechanism (UU)
- UU faults must be analyzed and reclassified to confidently finalize the achieved DC
- This poster contrasts formal and simulation methods for UU fault analysis

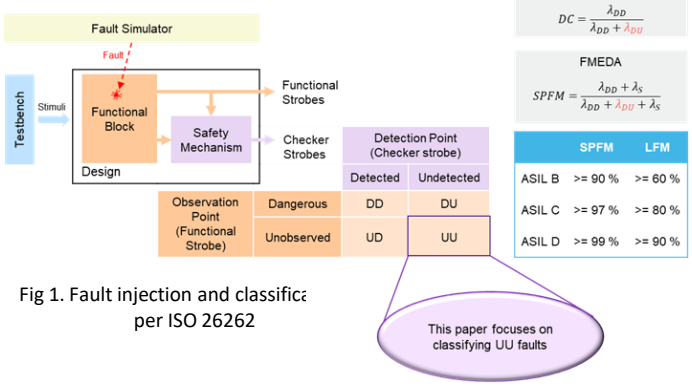

Fig 1. Fault injection and classifica per ISO 26262

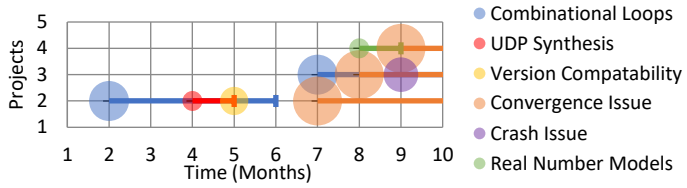

Fig 2. Fault analysis v/s time spent

CHALLENGES

- UU faults = Insufficient Stimulus + Structurally out of COI + Structurally in and functionally out of COI
- Solutions [1] = Formal analysis + Structural analysis + Constraints (Barriers / Stopats)
- Convergence issues + Tool limitations = Delays + Insignificant ROI
- Prompted an exploration of alternate methods to classify UUs
- Simulation based Fault Barrier analysis identifies design barriers blocking fault propagation
- Ranks barriers by their contribution to non-propagation
- Leverages existing fault simulation setup

DESCRIPTION

- Barrier = First design signal where fault propagation ceases
- A barrier can block multiple faults, and a fault can be blocked by multiple barriers
- This necessitates an iterative process of eliminating fault barriers
- After barrier removal, simulation helps determine the final classification
- Barriers exhibiting similar characteristics can be expertly categorized and analyzed together

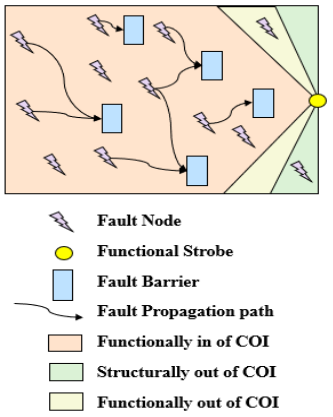

Fig 3. Fault and barrier visualization

```
1 Barrier ID,Barrier Node,FanIn Strength,Faults
2 1,spitb_sim_top.dut_top.SPI_TOP_0.SPI_REGCTL_0.Cont Assign at /proj/fsdv_dev/srajaned/design/spi/rtl/SPI_REGCTL.sv:1069,259,{446 447 45
```

Fig 4. Barrier to fault mapping in Barrier analysis

```
1 Fault ID,Fault Node,Fault Type,Fault Injection Time,FanOut Strength,Barriers
447 446,spitb_sim_top.dut_top.SPI_TOP_0.SPI_REGCTL_0.data_phase_pre,SA0,100NS,1,{1}
```

Fig 5. Fault to barrier mapping in Barrier analysis

RESULTS

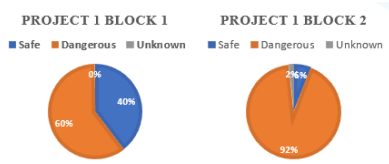

Fig 6. UU faults classified with only Formal

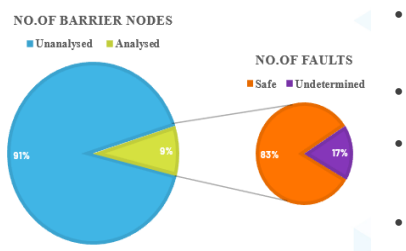

Fig 7. UU faults classified with Barrier Analysis

Project-1 (Digital design)

- Formal analysis applied post fault sims [2]
- Formal friendly -> Higher convergence of UU faults -> UU's formally reclassified and signed-off

Project-2 (Mixed-Signal design)

- Fault barrier analysis applied post formal based structural analysis
- Large set of barriers associated with DFT
- Prioritized one-to-one mapped barrier and fault nodes for prompt classification
- Design experts confirmed faults as safe
- Inconclusive faults subjected to debug for reclassification

CONCLUSIONS / KEY TAKEAWAYS

- "No single key unlocks every door"
- Formal method -> Digital block-level + Tool and design expertise + More compute resources
- Barrier Analysis (Simulation) method -> Mixed signal or High-seq digital + More manual effort
- Both, formal and simulation methods have distinct strengths and limitations
- An optimal approach aligning with design characteristics maximizes ROI
- Strategically combining both methods to mitigate UU faults boosts confidence in DC

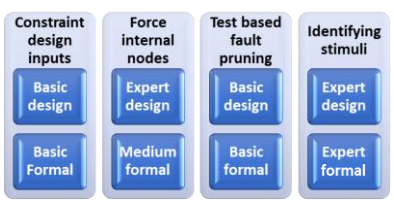

Fig 8. Expertise required for formal analysis

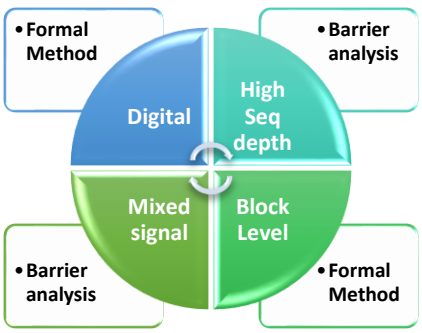

Fig 9. Formal and barrier analysis selection

Fig 10. Formal best practices

FUTURE WORK

- Further analysis of unanalyzed fault barriers is underway on Project-2
- Preparing to deploy Barrier analysis method in other production projects
- Prepare barrier analysis guidelines for RTL and GLS models
- Develop an advisory tool for tailoring formal and simulation method to design needs/types

REFERENCES

[1] Siri Rajanedi, Prashantkumar Ravindra, "Target Diagnostic Coverage is Achieved! What about Unclassified Faults?" CDNLive, India, August 2023.

[2] Praneeth Uddagiri, Veera Satya Sai Gavirni and Prashantkumar Ravindra, "Fault Injection Strategy to Validate ASIL-D Requirements of BMS Components" DVCON, India, September 2022.

ANALOG DEVICES

Contacts:
Siri Rajanedi : Siri.Rajanedi@analog.com
Prashant Ravindra: Prashantkumar.Ravindra@analog.com

Acknowledgement

Authors would like to thank the members of Analog Devices Automotive BU and Engineering Enablement for their support and collaborative work.

Authors would also like to thank the Cadence FuSa team for their collaboration.