Static Structural Analysis and Formal Verification of SoC with Software Safety Mechanisms for Functional Safety

Hyunsun Ahn
Samsung Electronics Co., Ltd., Korea

Euisang Yoon
Siemens EDA, Korea

accellera SYSTEMS INITIATIVE

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

INTRODUCTION

BackGround

- Conducting safety verification for software safety mechanisms in large SoCs requires fault campaigns, which are essential but tedious and complex tasks.

Requirement

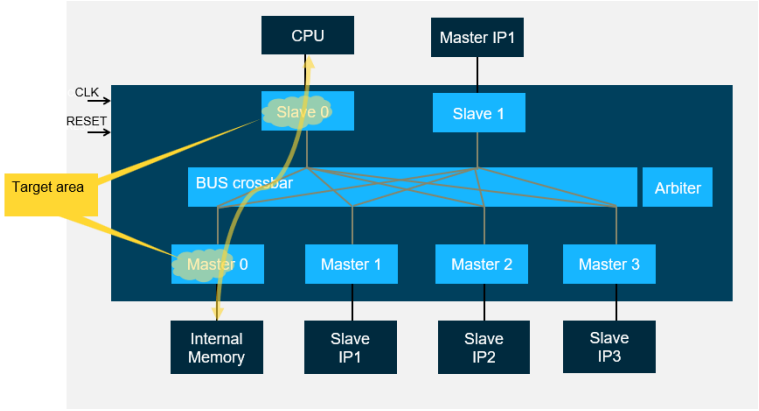
- There is a need for a new approach to effectively and quickly perform safety verification in the early stages of the design process.

Approach

- An integrated approach using static analysis and formal verification techniques can be proposed.

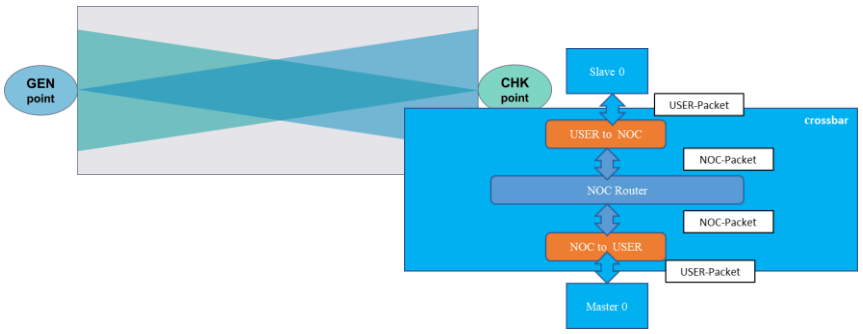
GAP ANALYSIS

- Target Area is Defined for Diagnostic Coverage Improvement with Software Safety Mechanisms.



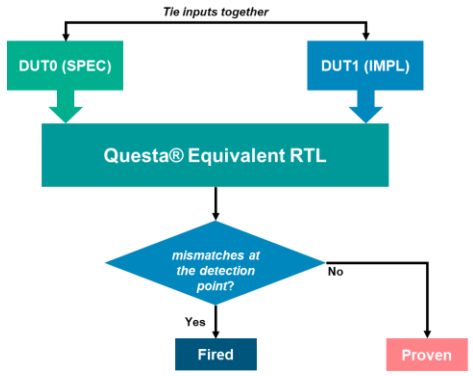
STRUCTURAL STATIC ANALYSIS

- Static structural analysis focuses on identifying design patterns and protocols that can reduce the scope of proof.
- SafetyScope™ provides RiverFlowMode analysis, which supports data path analysis for protocol connectivity and data packet flow.



FORMAL VERIFICATION

- Questa® Equivalent RTL is used as a formal verification solution.
- Normal RTL and faulty RTL are compared through a formal equivalence check.



INPUTS
DUT0 = Original RTL
DUT1 = DUT0 with fault asserted

DESIRED OUTPUT
Does the detection point of the fault case mismatch the detection point of the original case, indicating that the safety mechanism can detect the fault?

When the detection point indicates that the fault Is not detected, the detection points are equivalent.

RESULTS

- In the Samsung automotive case study, an additional 4.41% coverage was proposed by software safety mechanisms, through static analysis and formal verification techniques.

BUS Logic	Result 1(from [4]): Fault simulation with partially configured hardware SMs Detected (%)		Result 2: Fault simulation with fully configured hardware SMs Detected (%)		Result 3: Fault simulation + Judgement results Detected (%)		Result 4: Fault simulation + Judgement result + static and formal analysis for software SMs Detected (%)	
NOC in Safety Island	Total 65.87%		Total 66.50%		Total 89.21%		**Total 93.62%**	
	Fault Simulation	65.87%	Fault Simulation	66.50%	Fault Simulation	66.50%	Fault Simulation	66.50%
					Judgment	22.71%	Judgement	22.71%
							Software SM	**4.41%**

CONCLUSION

- Structural analysis and formal verification allow for enhancing fault detection resolution without the need for a traditional fault simulation process, and a case study on a Samsung automotive design highlighted the effectiveness of this approach.
- Future work for further extension includes limiting design size in creating design cones for formal attention, seamless communication between tools, and exploring the possibility of dynamic formal analysis.

Contact information

hyunsun.ahn@samsung.com, bumju.kim@samsung.com
Jh23.park@samsung.com, ys31.kim@samsung.com
seonilb.choi@samsung.com

SAMSUNG SIEMENS

euisang.yoon@siemens.com, namyul.cho@siemens.com
arun.gogineni@siemens.com, ann.keffer@siemens.com
sungjinpark@siemens.com, sungyun.yoo@siemens.com