Verification Methodology for Functional Safety Critical Work Loads

G Prashanth Reddy

Debajyoti Mukherjee

accellera SYSTEMS INITIATIVE™

2021 DESIGN AND VERIFICATION™ DVCON CONFERENCE AND EXHIBITION INDIA

Problem Statement/Introduction

Introduction

- High computing workload with shorter Process Safety Time(PST) demanding high end SOC (system on chip) to coordinate and execute functional safety workloads
- State of art safety measures schemes in hardware and software being implemented to meet required safety goals and SIL/ASIL targets
- Industry BKMs for Safety work products like FMEDA ,DFA are available however BKMs for verification and validation are lacking

Problem Statement

- Understand state of art safety measures
- Developing strategy for verification by analyzing various HW & SW safety mechanisms
- Understand hardware and software interface and provide end to end verification/validation strategy

Proposed Methodology/Advantages

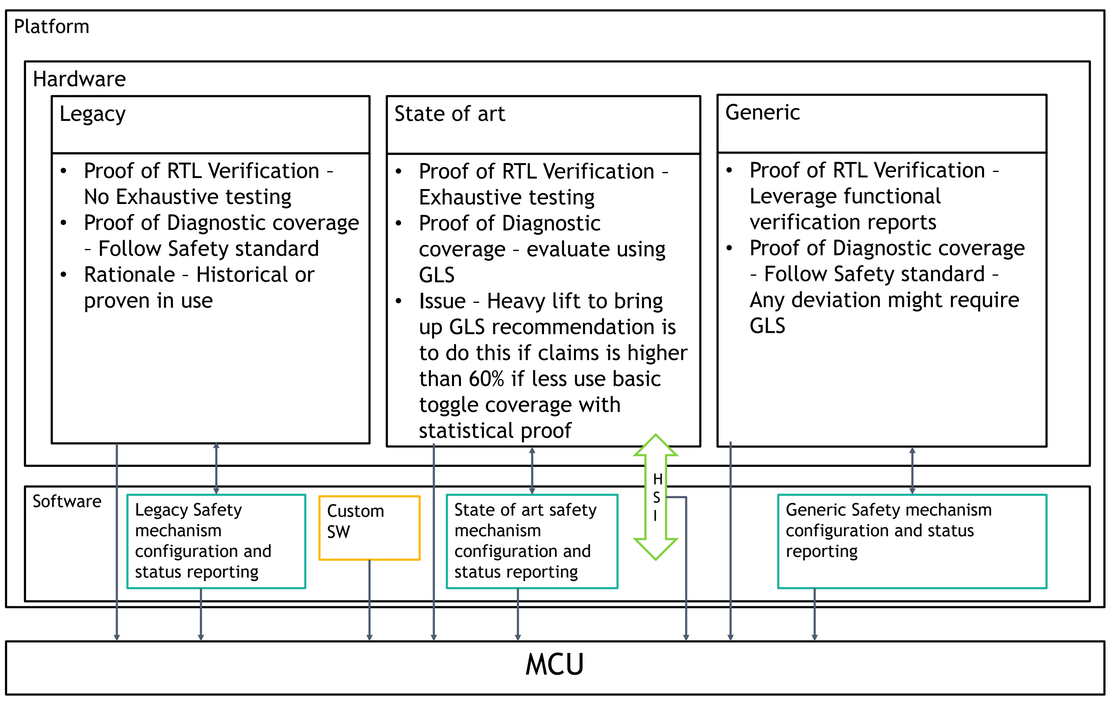
Proposed Methodology to prove evidence for Diagnostic coverage and implementation

- HWSR (Hardware Safety Requirement)
  - Legacy : Historical Evidence
  - State-Of-Art : Validation done on Case by Case Basis
  - Generic (Example : ECC/Parity) : Negative Validation on Parity / ECC / BIST logic
- SWSR (Software Safety Requirement)
  - Generic : Post-Si Validation
- HW-SW Interface
  - Both Pre-Silicon and Post-Silicon
- End-to-End
  - Entire SW Stack + RTOS + Pre-Silicon + Post-Silicon

Advantage

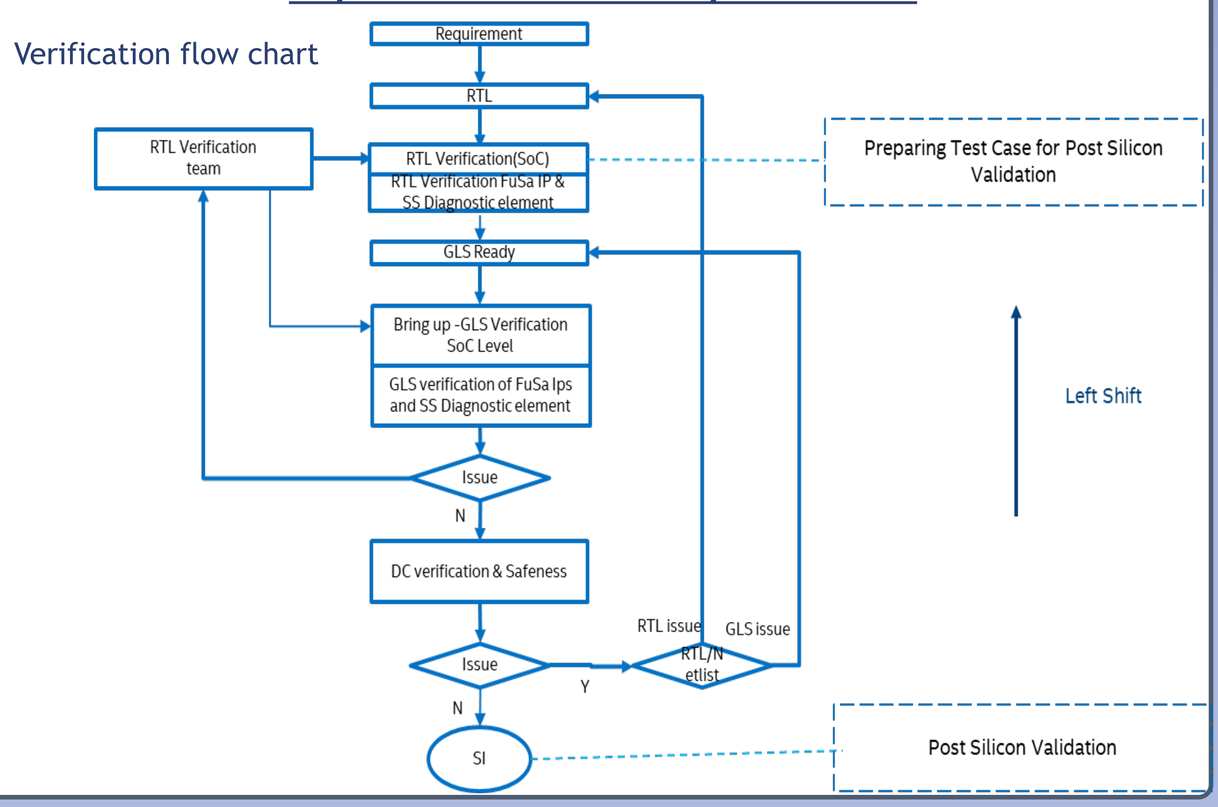
- All Standard Template Library can be validated in the Emulators before validating the same on a Post-silicon environment
- Will avoid Verification / Validation to be in the critical path
- Will accelerate closing safety signoff faster

Implementation Details/Diagram



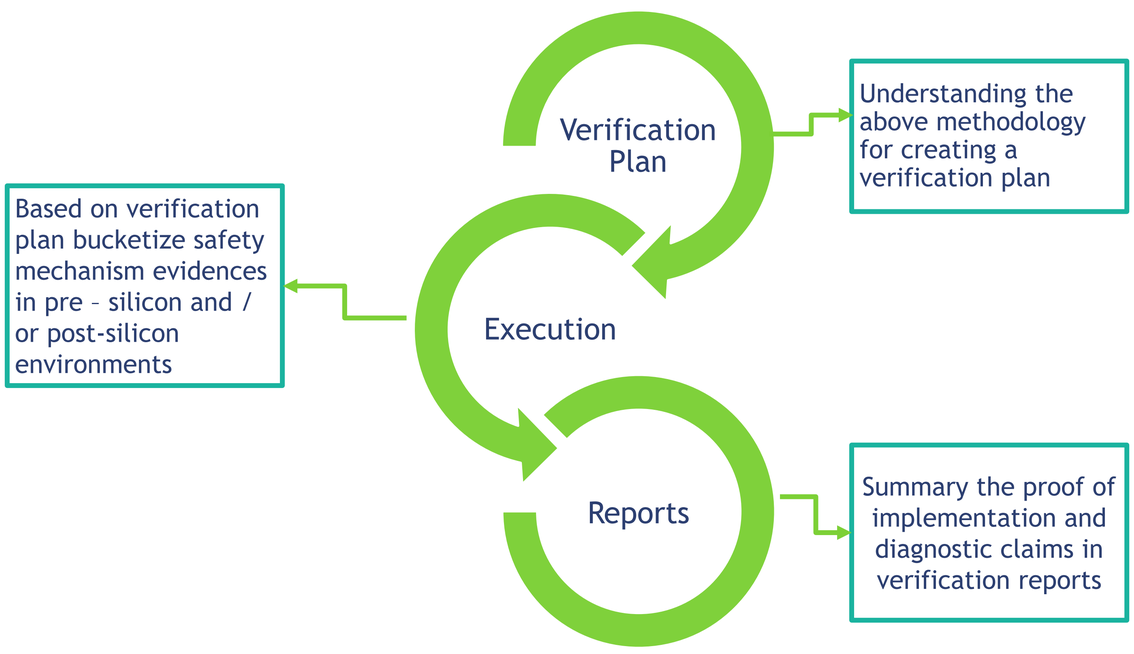
Implementation Details/Flow Chart

Verification flow chart



Results Table

The current poster summarizes the process improvement in the below chart



Conclusion

- Summarize the process mentioned as per Safety standard
- Best known practices to develop a verification test plan , execution and report findings
- Future Scope
  - As a future scope or goals for verification team is to ensure safeness claims for the designs where safeness functionality is tightly coupled with real-time functionalities.
  - Shift-left methodology in RTL to separate our safe blocks with functional blocks and mask them at FMEDA reports rather than proving the safeness for entire blocks in verification will reduce Time-To-Market and resource overhead

REFERENCES

Safety Standards ISO26262 , IEC61508