Verification Methodology for Functional Safety Critical Work Loads

G Prashanth Reddy (SoC Design Engineer)

Debajyoti Mukherjee (Verification Lead)

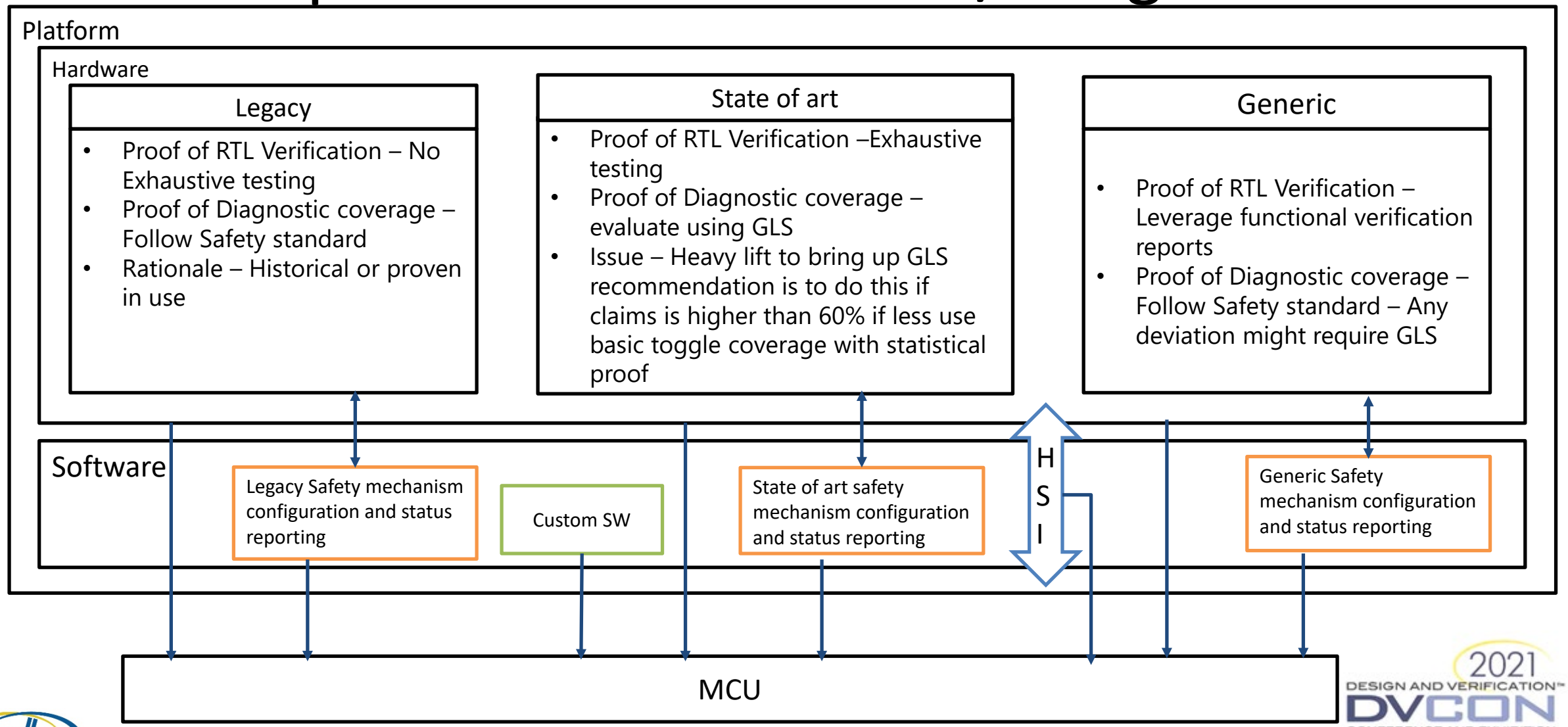
accellera SYSTEMS INITIATIVE™

2021 DESIGN AND VERIFICATION™ DVCON CONFERENCE AND EXHIBITION INDIA

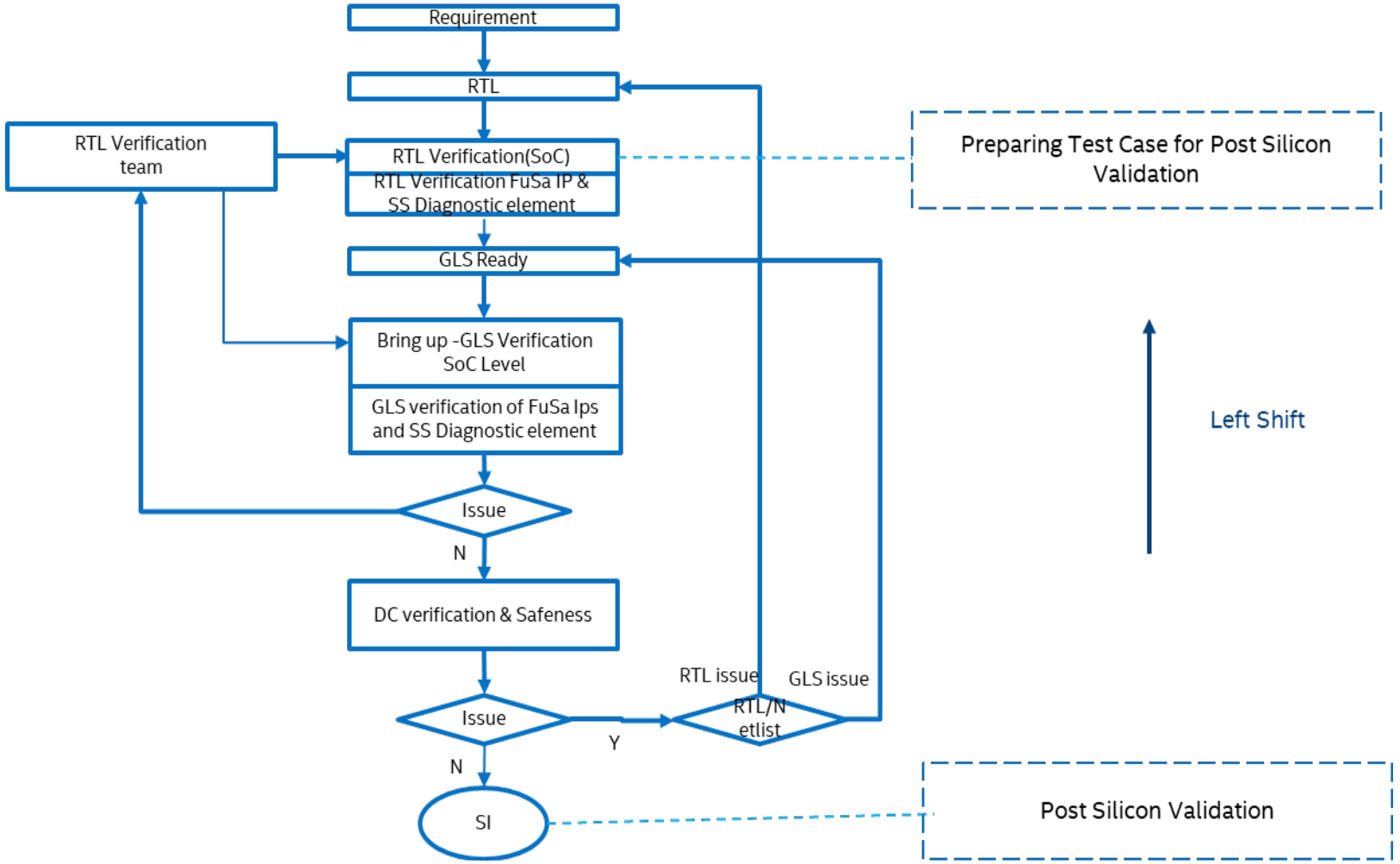
Problem Statement/Introduction

- Introduction
  - High Computing Workload with shorter Process Safety Time(PST) demanding high end SoC(system on chip) to co-ordinate 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 start of art safety measures
  - Developing strategy for verification by analyzing various HW and SW safety mechanisms
  - Understand hardware and software interface and provide end to end verification / validation strategy

Implementation Details / Diagram

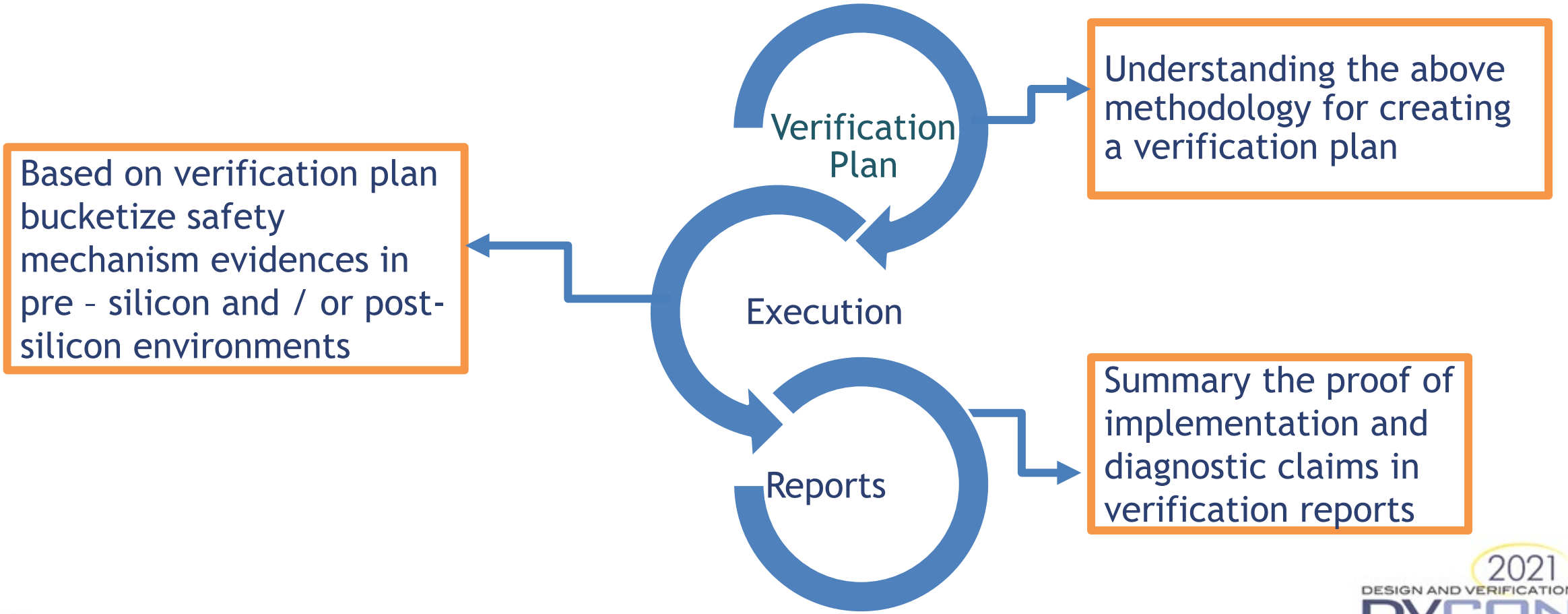


Implementation Details/Flow Chart



Results Table

The current poster summarizes the process improvement in the below chart



Conclusion

- Summarize the process mentioned as per Safe / Interest
- 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

Reference

- Cadence Safety Standard ISO26262 , IEC61508

Questions