Functional Safety Verification Methodology for ASIL-B Automotive Designs

Onkar Bhuskute

Marvell Technology

Problem Statement/Introduction

Introduction:-:-

- Functional Safety :-
  - Functional safety schemes for automobiles helps in identifying malfunctions (electric and electronic) and specifies actions and techniques to be adopted to mitigate risks and damage during instances of software or hardware failures.

- Functional Safety Verification ?:-
  - All chip designers set out to develop chips without bugs, but the stakes are much higher for those working on automotive designs. A cell phone crash may cause a reboot, but a bug in an advanced driver assistance system(ADAS), such as lane keeping, may cause another kind of crash – with much more serious consequences.

Problem Statement:-:-

- Serial Fault Injection
- Concurrent Fault Injection
- Generating FMEDA sheet (ISO-26262 compliant)

Proposed Methodology/Advantages

Proposed Methodology:-

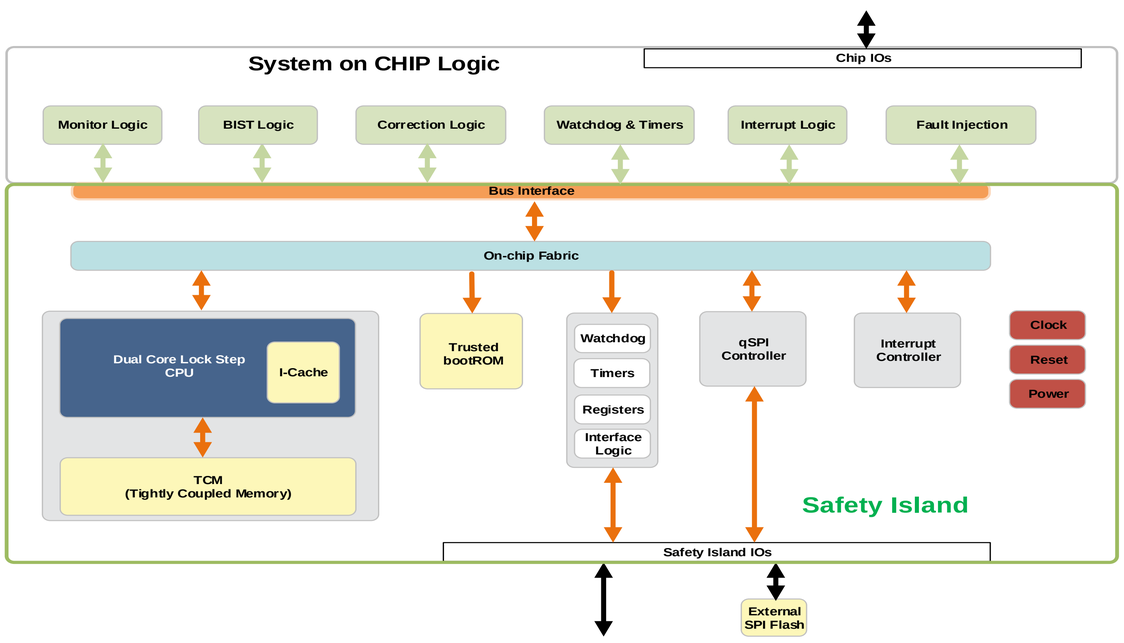
- Functional Safety Verification Plan is created along with the Functional verification Plan.
- Analyzed Safety Goals(SG) and Hardware safety requirement(HSR) against the top level architecture
- Possible failure modes are developed and analyzed their effects on the design along with the available Safety Mechanisms.
- Depending upon the failure mode and Safety Critical Path; the list of fault injection nodes is created.
- Launch the fault injection campaign

Advantages:-

- Used legacy UVM testbench for Fault injection with minimum effort.
- As per the result after fault injection on the Safety Critical Functionalities(paths); the Safety Mechanisms can be enhanced or more number of Safety Mechanisms are added to mitigate the risk of random failure.
- Random Fault injection is done to detect the random failures and its impact on Safety Mechanisms

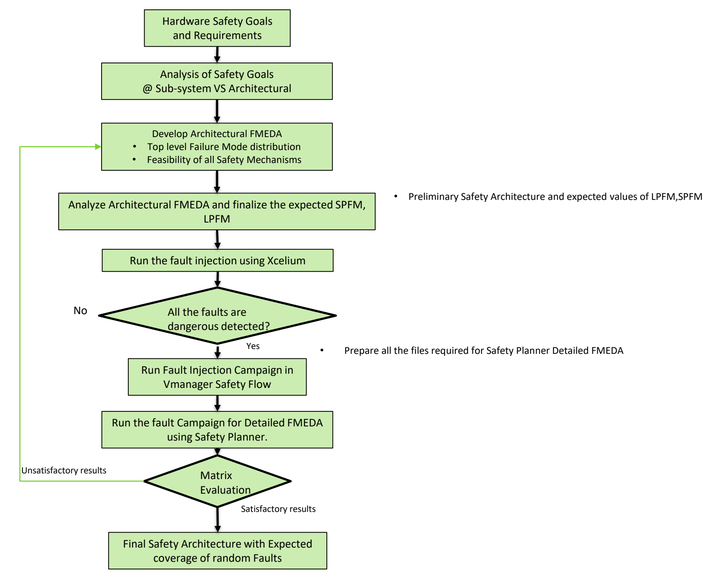
Implementation Details/Diagram

General Safety Island with Key Safety Mechanisms



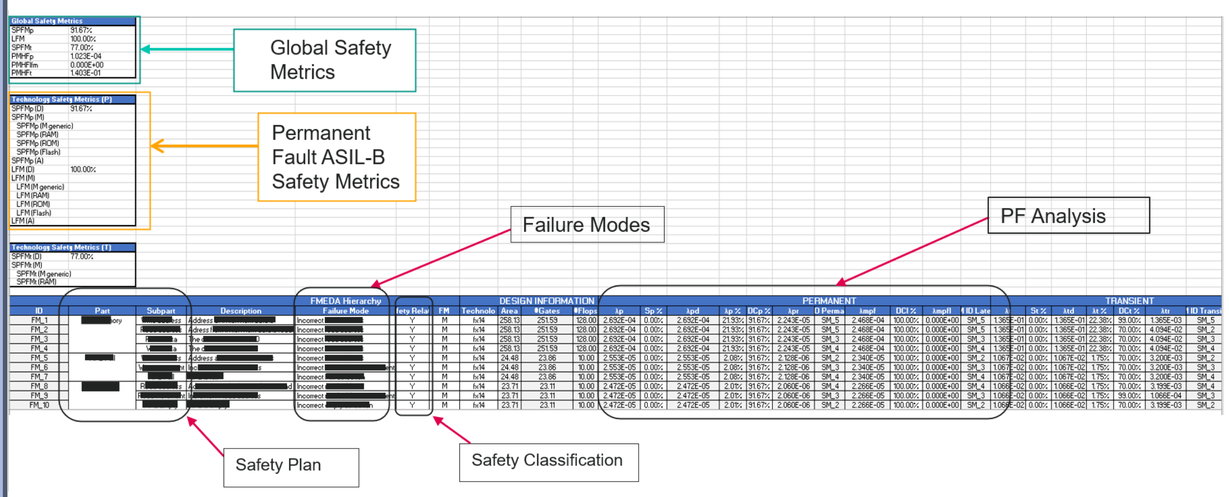
Implementation Details/Flow Chart

Functional Safety Verification Flow



Results Table

FMEDA Results and SM Results(ISO-26262 Terminology)



Conclusion

- Legacy UVM testbench used for functional verification is reused in Functional Safety Verification.
- The random faults are injected on Safety Critical Path and its effected are evaluated.
- ISO-26262 compliant output is evaluated on requirements for ASIL-B designs and iterations are done until the optimum results are achieved.

REFERENCES

- ISO 26262-5:2018, Road vehicles — Functional safety — Part 5: Product development at the hardware level
- ISO 26262-9:2018, Road vehicles — Functional safety — Part 9: Automotive Safety Integrity Level (ASIL)-oriented and safety-oriented analyses
- Cadence Online Support Website and Document.

© Accellera Systems Initiative