SoC verification of Security x Safety aspects for memory programmed into secure and non-secure regions in Automotive devices

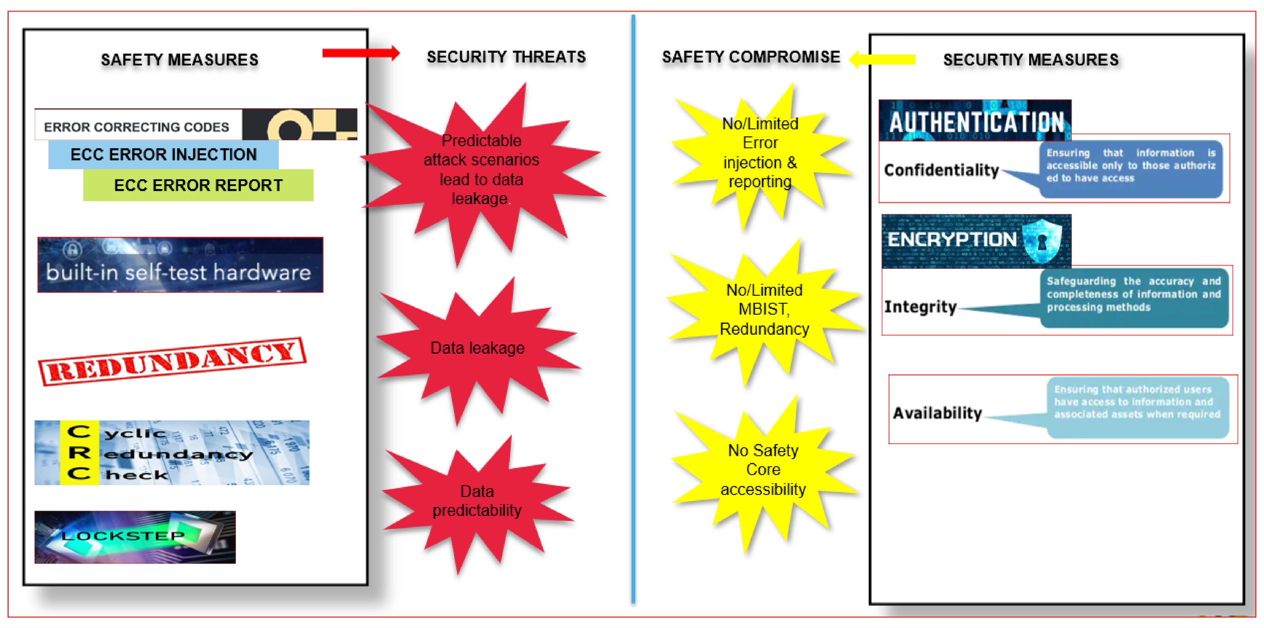
Ruchi Bora
Ramit Rastogi
NXP Semiconductors

Problem Statement/Introduction

Generally, in automotive devices, memories are implemented as either secure (limited access) or non-secure (open access). In such cases, the security and safety aspects are independent of each other and are implemented and verified using conventional methods. *With the requirement of the memories to be partly configurable as secure and non-secure at the same time, the security and safety aspects can't be considered in isolation. Their implementation should be such that one aspect doesn't limit the other.*

- Security measures as authentication, encryption etc. can limit the safety mechanisms and system availability
  e.g. reporting/logging of Safety-relevant diagnostic information
- Safety measures as error injection, BIST etc., can lead to security weaknesses
  e.g. data leakage from a secure memory

These aspects cut across multiple IPs and sub-systems across the SoC, including the DFT & Debug logic, and therefore, cannot be restricted to IP or sub-system level verification. Apart from the typical integration and data integrity checks at SoC level, additional cross-functional-system scenarios and customer use-case scenarios need to be targeted to expose any architectural & design issues early in the cycle.



Proposed Methodology

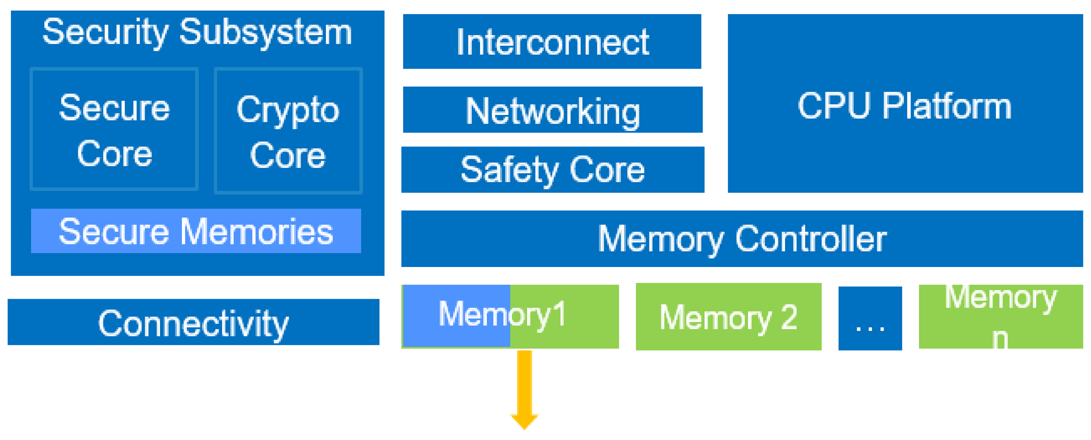
PLANNING
- Thorough reviews of the implementation with multiple stake-holders – Systems, Architecture, Design, Verification, DFT, Software etc..
- *Identifying System-level scenarios cutting across Security and Safety functional domains and customer use-cases*
- Mapping of the verification scenarios to the specification to avoid any obvious misses

SoC VERIF PLAN
- Verifying the configurability features – secure/non-secure memory, size and accessibility via the intended secure core
- Design integration and data sanctity checks for the complete memory including the secure and non-secure parts
- Multi-master test scenarios targeting the data paths for the secure/non-secure parts simultaneously
- Error injection and response paths for configurable secure/non-secure memory parts
- *Proper handling of the reactions in case of Security and Safety violations at system level to avoid any compromises with the device functionality*
- DFT logic verification, addressing any possible secure data leakage issues
- Debug verification to ensure SW development and optimum debug features

MONITORS & CHECKERS
- *Assertions for checking access restrictions, data leakage, device state and other corner scenarios*
- Requisite status register checks done to highlight any unexpected errors, upon the completion of a test scenario

COVERAGE
- Functional coverage - security, safety and debug and valid cross- combination of these
- Toggle coverage analysis of all concerned IPs – custom logic, security master, memory controller etc.
- Complete code coverage analysis of all the custom logic added at SoC, including DFT and debug logic, to achieve the said implementation

Implementation Details/Diagram

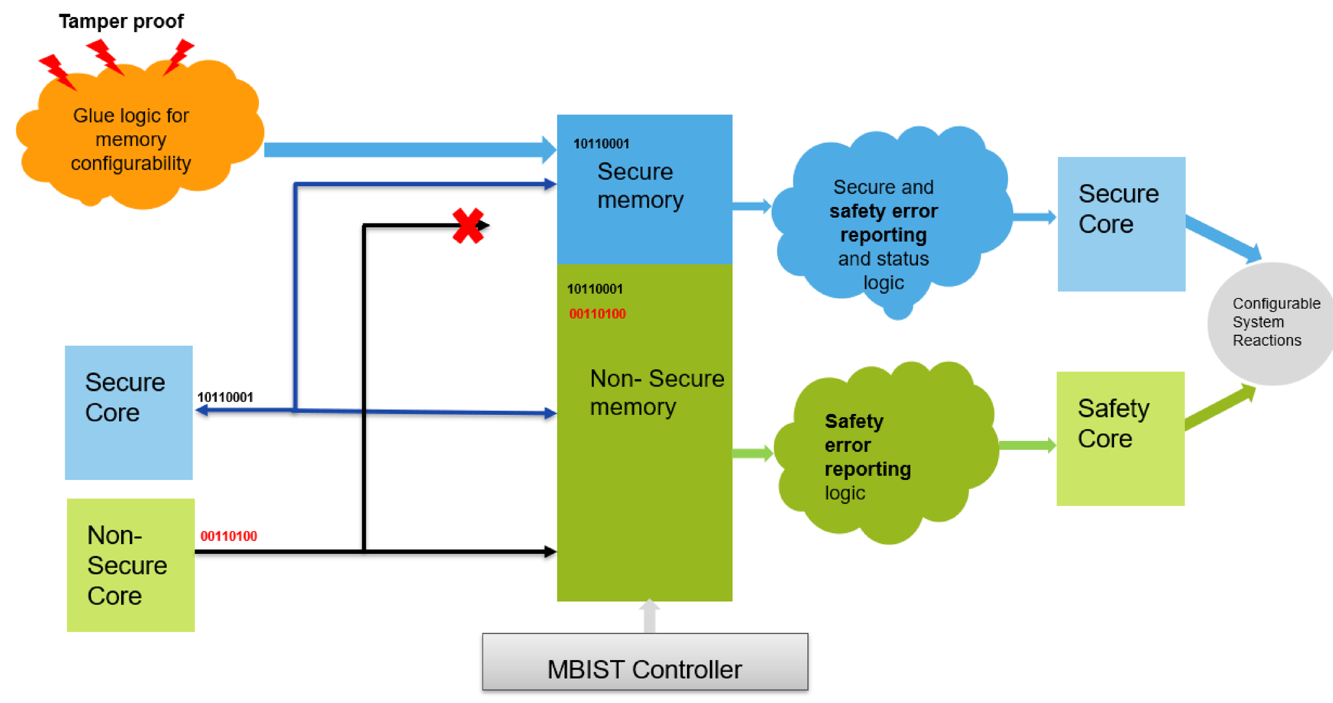


The memory can be made partly secure via a combination of static and dynamic device configuration handled by the secure core.

To implement the configurable memory, a multi-pronged design approach is used whereby there are updates across the SoC implementation, not limiting to custom logic, DFT, Security subsystem, fuse implementation, memory controller, handling of Safety faults, Debug logic etc.

All these aspects are only stitched together during the SoC implementation, making SoC verification very complex and span across multiple functional domains of Security, Safety, DFT and Debug.

Implementation Details/Flow Chart



SoC verification has to ensure :

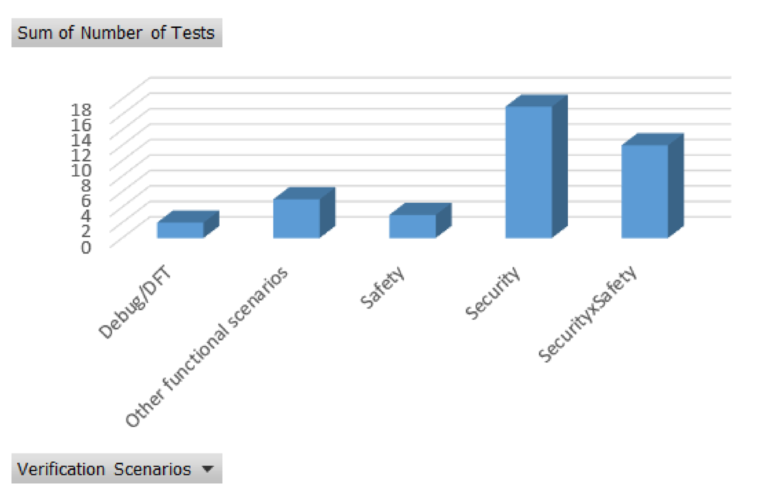
- Correct functionality of the custom logic that determines the nature (secure or non-secure) and size of the secure memory
- Glue logic itself is tamper-proof (implemented via triple-voted FFs, password needed for updating the configuration)
- Correct access restrictions are implemented for configuration and data path of the secure part of the memory
- Error injection and reporting is differently handled for both the secure and non-secure part
- Expected system reactions are generated by appropriate cores in case of ECC errors/tamper and other malicious attacks
- MBIST capability is limited - present only for the non-secure part and blocked for the secure part of the memory
- No data leakage through the DFT implementation
- Debugger accesses are granted/restricted according to the memory configuration

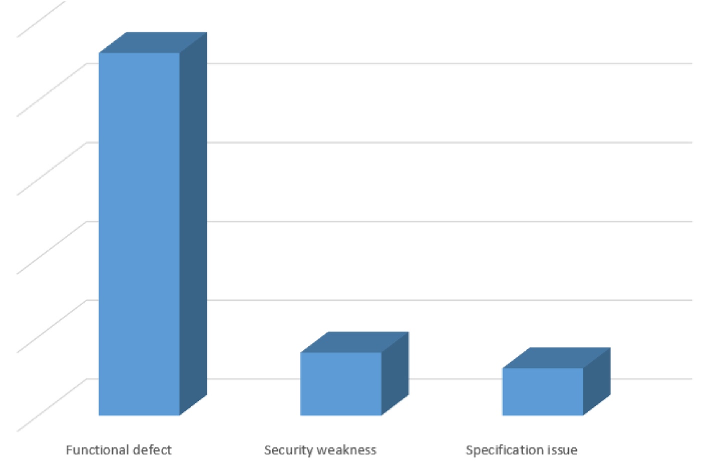
Results Table

As discussed above, varied aspects of SoC verification have been targeted to cover the complexity posed by the simultaneous co-existence of Security and Safety features for the configurable memory.

As part of this approach, below issues were detected in the RTL development phase, mitigating risk during further design stages.

- Security weaknesses in the architecture and design
- Functional issues in design implementation
- Specification defects





Relative defect trend

Conclusion

With the increase in demand for secure data processing, FW OTA updates etc. in automobiles, solutions implementing a configurable and shareable secure and safe memory is gaining traction. In this context, conventional approaches to SoC verification are no longer sufficient to guarantee the system functionality across myriad and in-filed use-case scenarios. A thorough analysis of the of the architecture and design aspects to come-up with a multi-dimensional SoC verification approach is the need of the hour.

- Such an approach is intended to cover various scenarios across Security and Safety domains, addressing the key aspects of data leakage due to security weaknesses and safety violations that may occur.
- It also provides a SoC verification template for future devices implementing configurable secure and non-secure memories. The test scenarios and the testbench implementation is generic in nature and easily portable.
- Also, it highlights the immense value and quality that's brought-forth as a result of collaboration across multiple functions along-with security and safety verification teams.

REFERENCES

Architecture and Design implementation of configurable memories for complex automotive devices