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 leak the other.

- Security measures as authentication, encryption etc. can limit the system's availability to the user.
- Safety measures as error injection, BIST etc. can lead to security weaknesses.
- Improper implementations of memory controllers can cause failures in 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

- Thorough review of the implementation with multiple stakeholders – Systems, Architecture, Design, Verification, DFT, Software etc.
- Identifying system scenarios cutting across security and safety functional elements and customer use cases.
- Non-functional specifications to ensure the functionality meets all the design objectives.
- The checking of correctness of the implementation, e.g. redundancy in the logic, logical data sanitization, etc.
- Double-checking the implementation against the non-functional specifications.
- Identifying the test cases targeting the data paths for the secure/non-secure parts simultaneously.
- The implementation of the test cases for the secure/non-secure memory parts.
- Ensuring the correctness of the implementation for the secure configuration and high-level validation at system level to avoid any implementation flaws in the logic functionalities.
- DFT logic verification, addressing any possible security/data leakage issues.
- Debug verification to ensure SW development and optimum debug features.
- Functional coverage – security, safety and debug and read/write operation of the logic.
- Formal analysis – security & safety aspects are independent of each other and are implemented and verified using conventional methods.

Results Table

As discussed above, various aspects of SoC verification have been targeted to cover the complexity posed by the simultaneous co-existence of security and safety functional aspects for the configurable memory.

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

Conclusion

With the increase in demand for secure data processing, EWS, OTA updates etc. in automobiles, solutions implementing a configurable and sharable secure and non-secure memory is gaining traction. In this context, conventional approaches to SoC verification are no longer sufficient to guarantee the system's functionality across myriad and in-flight use case scenarios. A thorough analysis of the implications of the architectural 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 methodology implementation is generic in nature and easily portable.
- Also, it highlights the immense value and quality that it 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