Establishing Freedom From Interference and detecting Data Access Violations, Control Flow Violations within Automotive Safety Software

Authors: Akhila Shamsunder, Swasati Baishya, Sandeep Chandrashekar, Karan Mundhra

Table of contents

Table of contents

Introduction

Head up Display
Electric Power Steering
Data Communication
Electronic Stability Control
Instrument Cluster
Adaptive Cruise Control
Airbag deployment
Airbag Deployment
Tire Pressure Control
Electronic Throttle Control
Night Vision
Engine Control
Interior Lightning
Antilock Braking
Navigation System
Automatic Braking System
Windshield Wiper Control
Lane Departure Warning
Lane correction
Regenerative Braking
Driver Alertness Monitoring
Security System
Adaptive Front Control
Battery Management
Active Suspension
Seat Position Control

And many more….

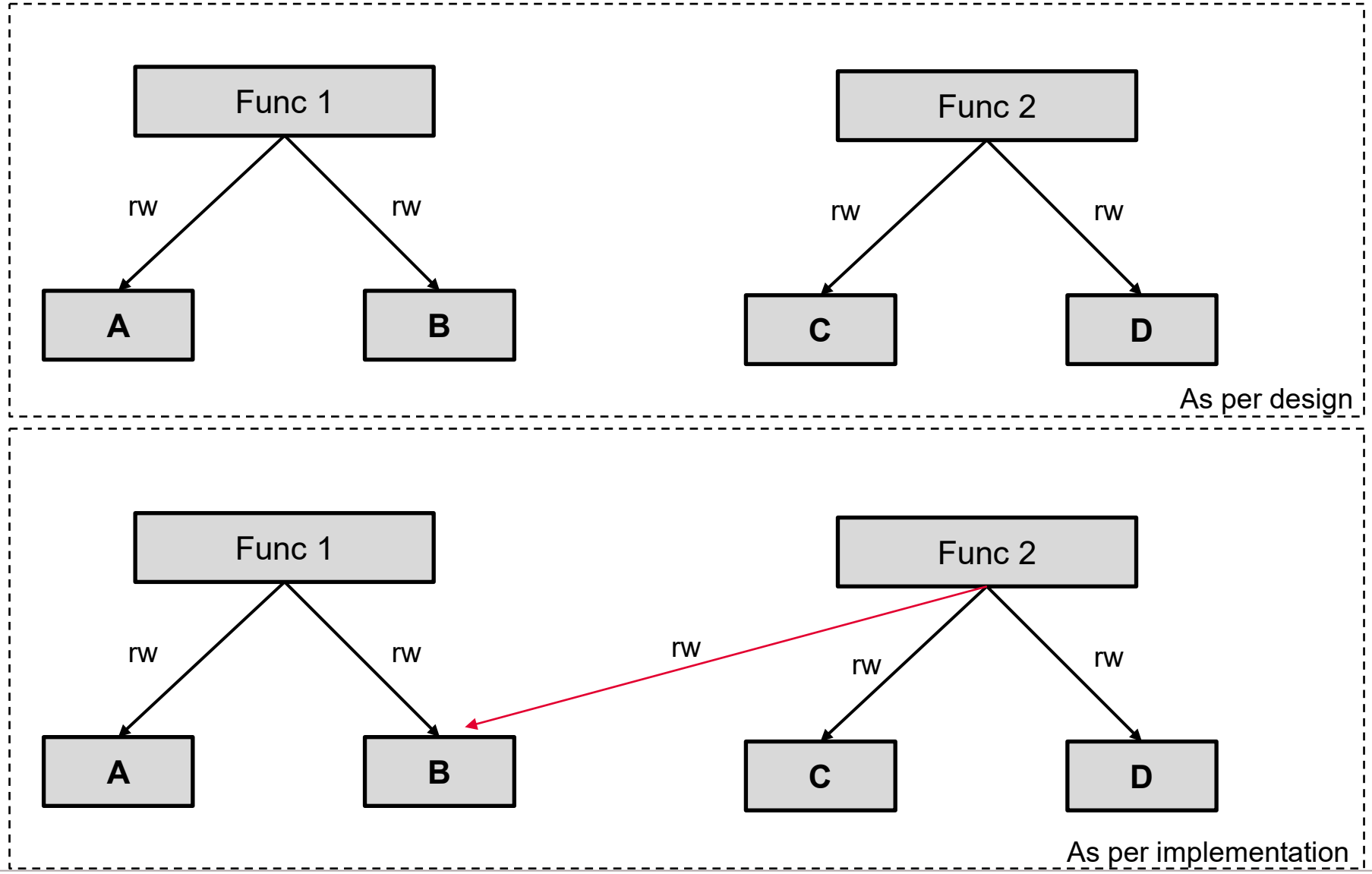
Table of contents

Freedom From Interference

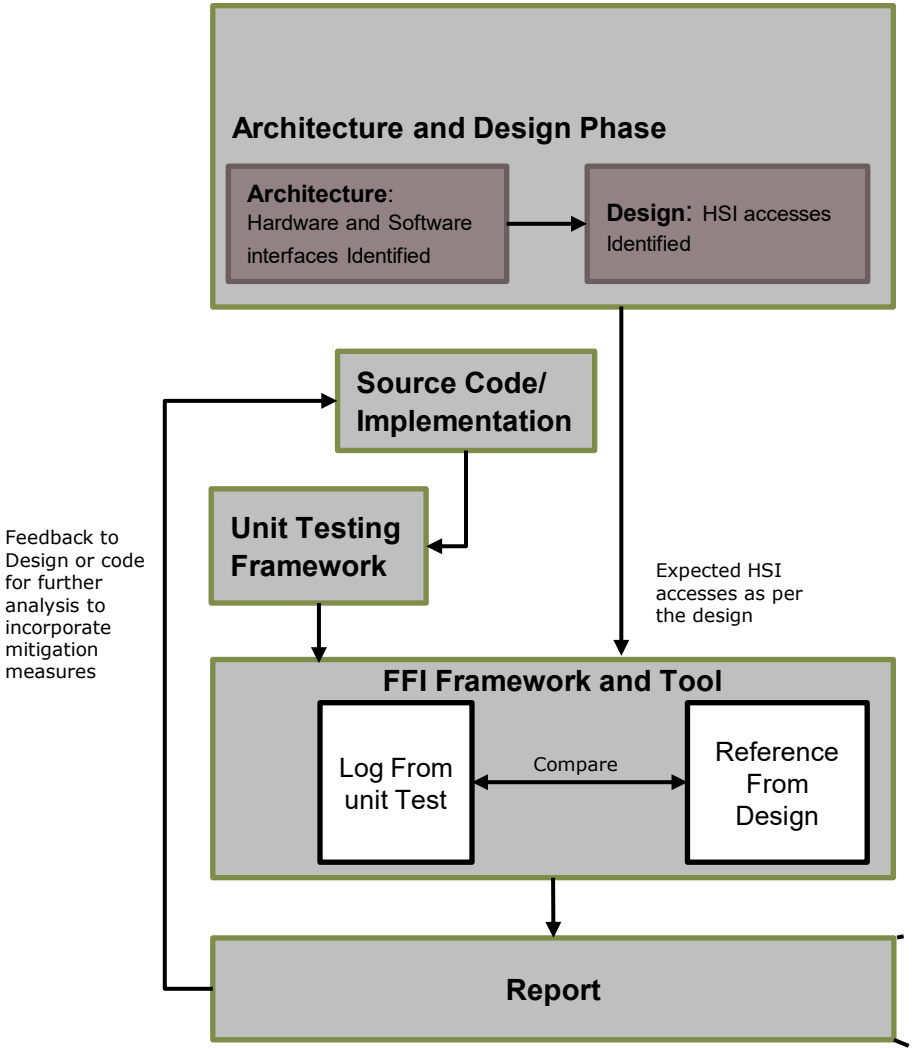
- Freedom From Interference is:
  - Absence of cascading failures leading to undefined behavior in the system
- One of the primary causes leading to such failures is unintended access to memory regions, primarily global variables and hardware registers

The safety objective of a system is to avoid such cascading failures, where unintended access to a memory location by a software element leads to the failure of another software element.

Example of FFI



A method to for FFI Verification



Example of the "HSI" Report

Function Name	Memory / Address accessed	HSI verification Result
Func 1	0xAB123456	Pass
Func 2	0xAB1234EE	Pass
Func 3	0xAB1234EF	Fail

Table of contents

Control Flow Analysis

- Control flow violations can occur due to unintended execution of instructions or function calls. Such violations can lead to unintended behavior in the system.
- Control Flow Analysis is performed as a safety measure to overcome control flow violations. By definition, it is a static code analysis method to determine the control flow of a program. It can occur due to unintended execution of instructions or function calls leading to unintended behavior in the system.

Control flow violations can be identified by safety measures like
Range and Plausibility check, Boundary value and Equivalence class checks,
Requirement based testing, Inspection reviews, Control flow analysis

A method for Control Flow Analysis

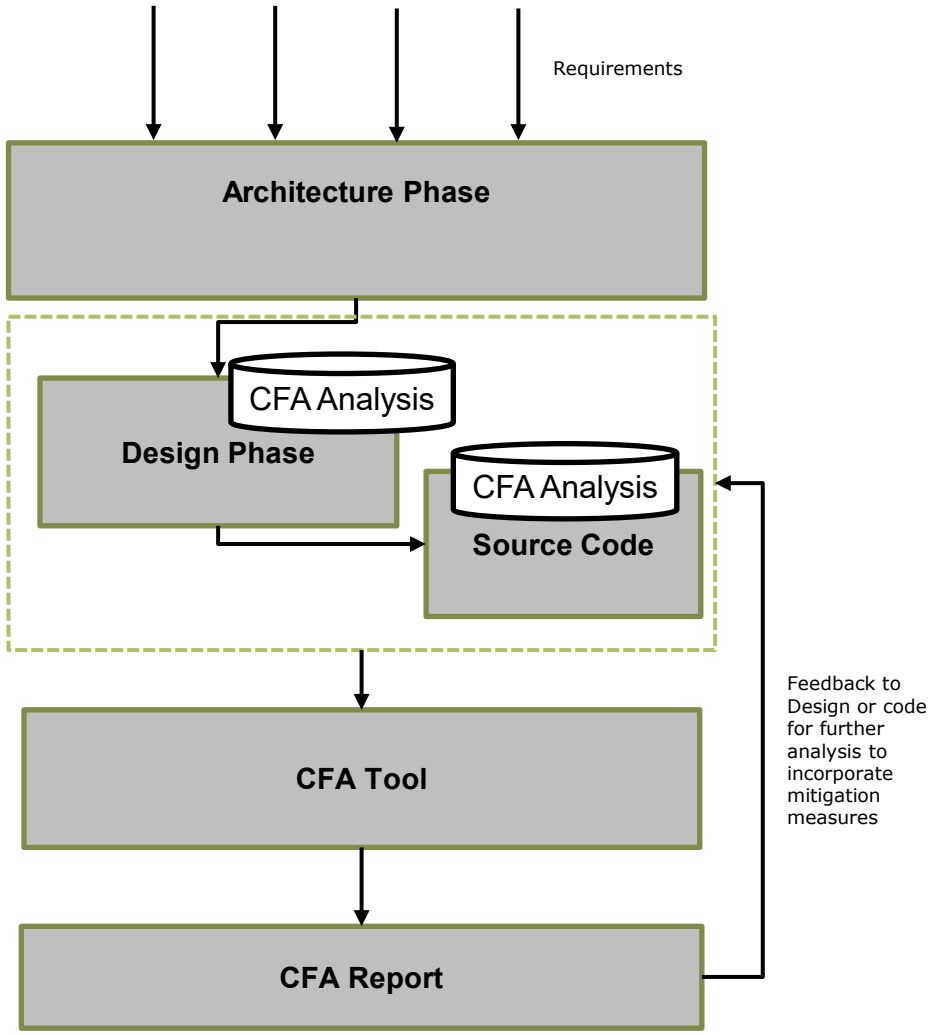


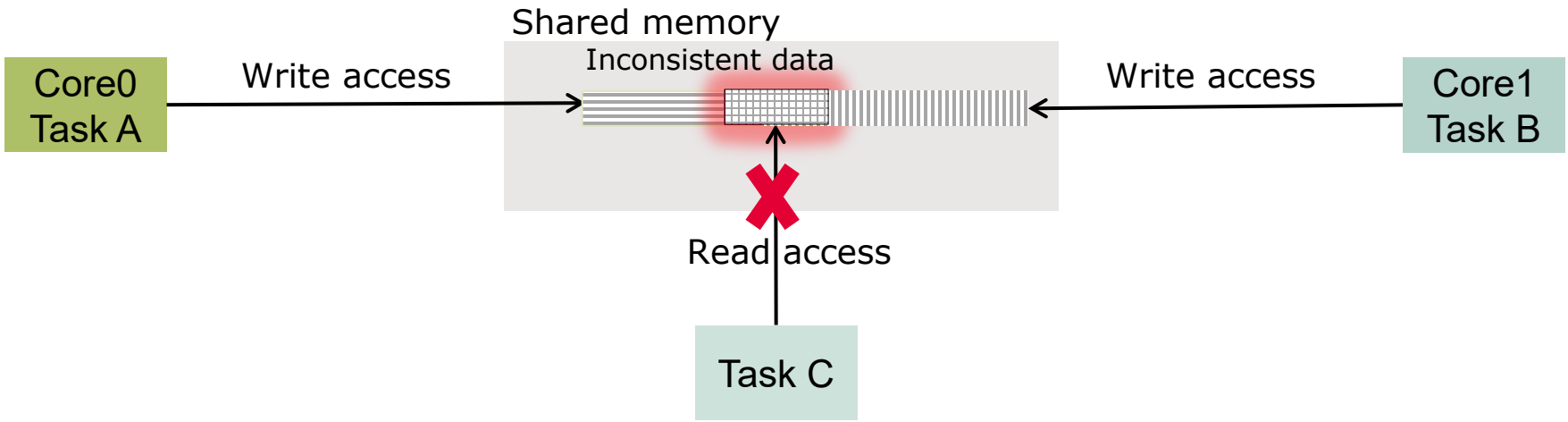
Table of contents

Data Access Analysis

- Data Flow Violations can occur due to incorrect handling of shared data.
- Data Access Analysis is performed as a safety measure to overcome data flow violations. By definition, it is a process of analyzing memory regions accessed by software programs in a multi-thread, multi-core, and pre-emptive execution environment.

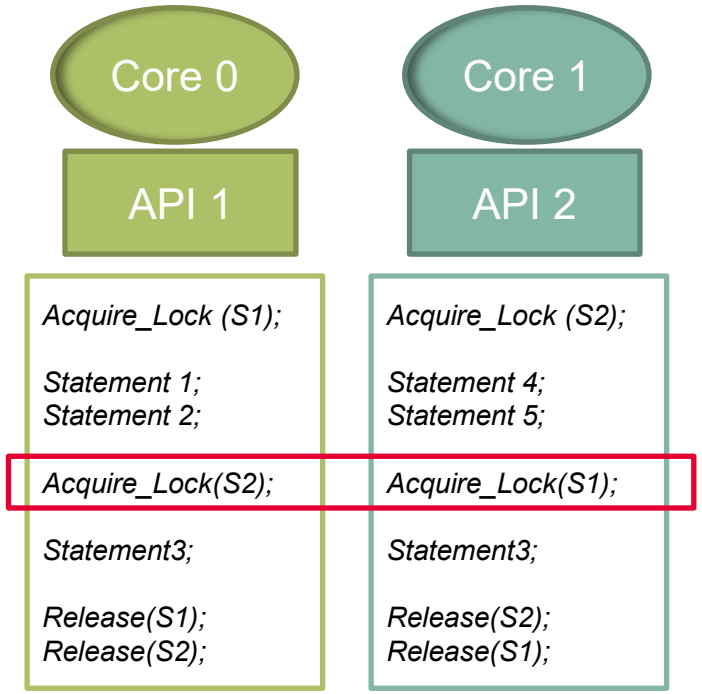
Data flow violations can be identified by safety measures like requirement-based testing, unit verification to cover equivalence class and boundary value analysis, static analysis, inspection reviews, safety analysis and Data Access analysis

Example for Data Flow Violation: Shared memory access (Concurrent Tasks)



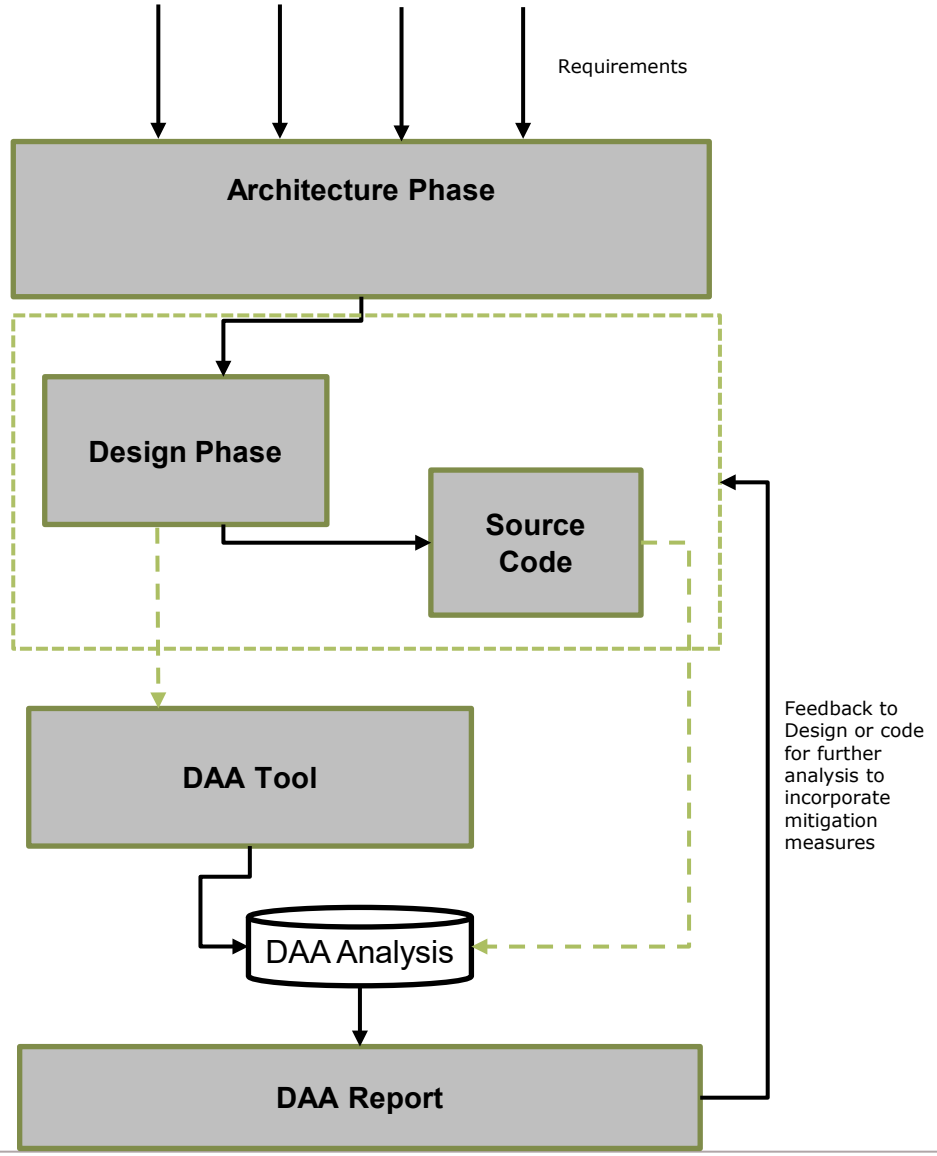
Not acceptable!!

Example for Data Flow Violation : Deadlock Scenario



Not acceptable!!

A method for Data Access Analysis



Areas to be focussed during Data Access Analysis

- Concurrency Issues
- Reentrancy
- Global Data and Critical Section
- Hardware Resources

Table of contents

Conclusion

- FFI Verification, Data Access Analysis and Control Flow Analysis:
  - Can also be achieved in different methods than what is proposed in the paper. For example, logging a hardware trace.
  - Aids in identifying issues at an early stage of development, thus ensuring a safe and reliable system.
  - Probability of bugs detected at a later stage is reduced.
  - Proper synchronization between different hardware and software resources is also analyzed.
- The framework has been successful in identifying the unintended access of hardware resources that are due to erroneous design or code. CFA, DAA, and FFI verification proposed in this paper have at an early stage helped in identifying violations and thus improving the quality of the product

Table of contents

References & Acknowledgments

- ISO 26262, Road vehicles - Functional safety, ISO copyright office, 2011-11-15
- Freedom from Interference for AUTOSAR-based ECUs: a partitioned AUTOSAR
- Infineon TriCore Architecture Manual
- ISO/IEC 61508, Functional safety of electrical/electronic/programmable electronic safety-related Systems, IEC central office, 2010
- Sandeep Chandrashekar, Akhila Shamsunder, Swasati Baishya, Sumit Khandelwal; Infineon Technologies; Shared resource analysis for embedded multi-core systems, United States Patent, US11061745B2, 2021-07-1

We (authors of the paper) thank the entire automotive software team at Infineon for continuous support in improving and deploying the methods described in the paper.

Part of your life. Part of tomorrow.