

Call for papers submission – SAE Functional Safety Conference 2021

Title:

Achieving Functional Safety Goals in SEooC microcontroller peripherals: Methods and approaches to produce the desired diagnostic coverage.

Author Details:

Name: Priyasloka Arya

Organization: LDRA

Email: priyasloka.arya@ldra.com

Abstract: (170 words)

The microcontroller is an integral part of an Electronic Control Unit (ECU); however, the treatment of its diagnostic system and testing is distinct when the microcontroller is considered as a Safety Element out of Context (SEooC).

A diagnostic system (Offboard and Onboard) is a critical aspect of the ECU's monitoring system. Each fault is identified with a diagnostic trouble code (DTC) and captured in fault memory as a part of EEPROM.

The quality of fault/error detection and mitigation is quantified as diagnostic coverage which establishes the robustness of safety measures in terms of measurement and assessment. Moreover, the effectiveness of diagnostic coverage/diagnostic testing can be demonstrated by fault-injection tests because fault scenario occurrences are sporadic.

This paper will reflect on the approaches (as use cases) to develop diagnostic testing strategies for some peripherals of a microcontroller, how to choose diagnostic testing from available methods while ensuring required higher diagnostic coverage could be achieved and how to establish traceability from failure modes to diagnostic mechanism design specification and diagnostic test procedures.

Keywords:

ISO 26262, SAE J3061, Safety, Security, Traceability, Failure Mode, Safety goal, Safety Requirement, FMEA, FMEDA, diagnostic coverage, SEooC, ECU, Diagnostic Coverage, PMHF, SPFM, LFM, FIT, ASIL