WHITEPAPER

Smart Strategic Approach for Functional Safety Implementation

Chandrashekara N
Santosh Kumar Molleti

August 2015

L&T Technology Services

Table of Contents

Abstract

ISO-26262 is a standard defining requirements and providing guidelines for achieving functional safety in E/E systems installed in road vehicles. The standard ISO-26262 is considered a best practice framework for achieving functional safety goals in road vehicles.

Functional safety is becoming a critical parameter for consumers while choosing vehicles, which is driving the automotive organizations to consider implementing functional safety practices like ISO-26262 during E/E product development.

Organizations are creating dedicated Functional Safety teams at different organizational levels to achieve safety goals, which is adding additional 20% to 40% effort/cost based on ASIL levels (ASIL-B to ASIL-D).

This Paper describes an innovative methodology developed by L&T Technology Services to incorporate the functional safety practices into the existing E/E software development life cycle process. Adopting this innovative process approach, we at L&T Technology Services have been able to achieve reduction in the additional safety implementation effort of approximately 10-20% (ASIL-B to ASIL-D) in two projects.

1. Introduction

ISO-26262 addresses the needs for an automotive-specific international standard that focuses on safety critical components. The objective of Functional Safety is freedom from unacceptable risk of physical injury or of damage to the health of people either directly or indirectly.

ISO-26262 is a derivative of IEC 61508, the generic functional safety standard for electrical and electronic (E/E) systems. ISO-26262 is intended to be applied to safety-related systems that include one or more electrical and/or electronic (E/E) systems and that are installed in series production passenger cars with a maximum gross vehicle mass up to 3,500 kg.

ISO-26262 addresses possible hazards caused by malfunctioning behavior of E/E safety-related systems, including interaction of these systems.

2. Approach-To-Concept

2.1. History

The E/E systems in modern cars have increased year-on-year adding to more functionality and complexity in both the hardware and software. So the safety practices are becoming more regulated which motivates automotive organizations to adopt standardized set of practices for designing and testing the products.

This is creating a psychological environment, where functional safety is a critical topic that needs to be addressed completely by the safety experts only.

At L&T Technology Services, we have functional safety experts working on customer projects with functional safety requirements on the following activities:

i. Safety analysis: Hazard analysis, Fault tree analysis & reliability analysis
ii. Functional safety concept assessment
iii. Process Gap Assessment with legacy system/software
iv. ASIL Decomposition
v. Functional safety verification & validation activities

2.2. Evolution

At L&T Technology Services, we have come up with an approach to incorporate the ISO-26262 standard in the existing software development life cycle process.

The intent of this process is to incorporate the functional safety practices in the software development process as a regular activity without explicit statement of Functional Safety needs. This will help to create an environment in which all the software development engineers will partially become safety engineers, thus enabling a reduction in safety review/assessment effort.

3. Methodology

At L&T Technology Services, we are adopting the following methodology along with the existing software development life cycle process.

3.1. Hazard Analysis & Risk Assessment

This method is practiced to identify and categorize hazardous events of items (software module failure) and to specify safety goals and ASILs related to the prevention or mitigation of these hazards in order to avoid unreasonable risk.

The hazards of the item is systematically determined, with techniques such as expert brainstorming, checklists and FMEA, in terms of the conditions or events that can be observed at the module level. The effect of hazards is documented for relevant operational situations.

Based on the criticality of the hazard, a different architecture, design and test plan is created (e.g. testing the module for Statement coverage, Branch coverage and MCDC).

Example:

Possible effects: Unexpected behavior of software module.

Failure mode description: Without initializing the Ethernet driver a data packet has been received by the Ethernet hardware unit, resulting in an unexpected receive interrupt.

Applied measure: In ISR, the received interrupts flags are cleared and the ISR returns without any action.

3.2. Fault Injection Test

This method includes injection of arbitrary faults in order to test safety mechanisms (e.g. by corrupting the variables of the software).

Example:

Possible effects: Global memory corruption (the length field of the Ethernet frame is corrupted).

Failure mode description: The length field of a received Ethernet packet is corrupted.

Applied measure: The length field of the received Ethernet frame is verified with the maximum accepted value before processing it.

3.3. Resource Usage Test

To ensure the fulfillment of requirements influenced by the hardware architectural design with sufficient tolerance, properties such as average and maximum processor performance, minimum or maximum execution times, storage usage (e.g. RAM for stack and heap, ROM for program and data) and the bandwidth of communication links (e.g. data busses) have to be determined.

Example1:

For Timing Requirements:

Possible effects: Maximum execution time taken by the tasks leads to overall system performance delays.

Failure mode description: Process flow got stuck in an endless loop or the task execution time is more than the task budgeted time.

Applied measure:

i. Software timeout is used to exit from the respective function.
ii. Wait until the task budgeted time expires then kill the currently running task (i.e. exit from the running task).

Example2:

For Memory Requirements:

Possible effects: Maximum consumption of the system memory (RAM/ROM) slows the overall system execution.

Failure mode description: Best coding practices are not followed during the software implementation.

Applied measure:

i. Usage of macros and inline functions based on the needs.
ii. Avoid usage of recursive functions.

3.4. Boundary Values Test

This method applies to parameters or variables, values approaching and crossing the boundaries and out of range values.

Possible effects: Unexpected behavior of the software module.

Failure mode description: Invalid value passing or global memory corruption.

Applied measure:

i. Parameters or variables range should be verified at development level.
ii. Test plan should be prepared for boundary checks.

4. Case Study

AUTOSAR 4.0.3 BSW Stack Safety Reviews:

This project was executed for one of the world leaders in the Electronic Design Automation (EDA) Tools business.

Project Goal:

The key objective of this project was to ensure that the customer BSW stack was compliant to ISO-26262 (ASIL-B).

Scope of Work:

i. Review the BSW module design and unit test cases with respect to AUTOSAR 4.0.3 software specification (SWS).
ii. Review the OS module design and unit test cases with respect to OSEK requirement specifications.
iii. Write the design, develop & testing steps for each functional requirement.

Automotive Standards Used:

i. AUTOSAR 4.0.3 SWS Requirements
ii. ISO-26262 Functional Safety

5. Benefits of the L&T Technolgy Services Methodology

By incorporating the functional safety standards in the existing software development life cycle process; the following key benefits can be achieved:

i. Development engineers are aware of and adhere to the functional safety standards along with the normal software development life cycle process.

ii. Smaller teams for functional safety implementation and assessment will reduce resource requirement at the organizational level which in turn will reduce the cost.

iii. The developed software product is functionally safe (built with ISO-26262 guidelines), which is also reliable and will help in meeting customer expectations.

6. References

[i]. ISO-26262 is a Functional Safety standard, titled "Road vehicles — Functional safety"

[ii]. IEC 61508 Functional safety of electrical/electronic/programmable electronic safety-related systems

[iii]. http://www.autosar.org/

7. About the Authors

Chandrashekara N, Technical Delivery Manager, L&T Technology Services

Chandrashekara has totally 15 years of experience in the Automotive Domain (6 years — North American OEM, 6 years — European Tier1, and 3 years in R&D). He has handled a multimillion USD program for developing low-cost embedded ECU and setting up of a 120 member Software Engineering Services division at a Tier1. As an Embedded S/W Architect, he has been involved in System & Software Architecture definition and migration for embedded applications (AUTOSAR & Non-AUTOSAR). He has carried out Functional Safety Training, Safety Assessment (software and product/process), Safety Process Implementation, besides implementation of software quality processes for the Embedded Controls Division.

Santosh Kumar Molleti, Project Manager, L&T Technology Services

Santosh Kumar has totally 8 years of experience in Automotive Embedded Software Development. He has expertise in AUTOSAR architecture and application software development for Body Control Modules especially in exterior lights & power modes. As an AUTOSAR Architect, he has been involved in integration of various BSW stacks with various MCAL drivers and migration of legacy (Non-AUTOSAR) software to AUTOSAR complaint, including the development of software modules as per the ISO-26262 functional safety standards.

About L&T Technology Services

L&T Technology Services is a wholly-owned subsidiary of Larsen & Toubro with a focus on the Engineering Services space, partnering with a large number of Fortune 500 companies globally. We offer design and development solutions throughout the entire product development chain across various industries such as Industrial Products, Medical Devices, Automotive, Aerospace, Railways, Off-Highway & Polymer, Commercial Vehicles, Telecom & Hi-Tech, and the Process Industry. The company also offers solutions in the areas of Mechanical Engineering Services, Embedded Systems & Engineering Application Software, Product Lifecycle Management, Engineering Analytics, Power Electronics, and M2M and the Internet-of-Things (IoT).

With a multi-disciplinary and multi-domain presence, we challenge ourselves every day to help clients achieve a sustainable competitive advantage through value-creating products, processes and services. Headquartered in India, with over 10,000 highly skilled professionals, 11 global delivery centers and operations in 35 locations around the world, we constantly find flexible ways of working, tailored to our assignments and customer needs.

For more information, visit us at www.lnttechservices.com