Transition to ISO 26262-6 compliant development through gap analysis

Jim Allen

29-MAR-2021
Abstract

ISO 26262 2011 First Edition has been superseded by 2018 Second Edition and both have become a base requirement for winning new business. ISO 26262 Part 2, Management of functional safety, emphasizes the importance of having a process in place to execute a Functional Safety project and to have trained staff to design product per the process. To execute a Functional Safety project it is important to quickly establish if your existing processes can be mapped to ISO 26262 or if you have to create new work flow and procedures. It is important to create the Safety Plan quickly and to conduct a conformation review so that the entire team recognizes deliverables and responsibilities. If you have never executed a ISO 26262 project it is also a good idea to contract expert advice by requesting a Gap Analysis. This formal feedback is important to drive and direct necessary resources and focus on deliverables necessary to meet the expectations of the Assessors.
Project Background

Three project categories at BorgWarner

1. Driver Software
   - Hardware

2. HW Abstraction Layer (HAL)
   - Driver Software
   - Hardware

3. Application SW
   - Base Calibration
   - HW Abstraction Layer (HAL)
   - Driver Software
   - Hardware

Project sharing today is based on category 3 + additional requirements

- Application SW
- Base Calibration
- HW Abstraction Layer (HAL)
- Driver Software
- Hardware

- ODB II Support
- New Processors

- Simulink models
- Calibration guide
- Model-Based Design

- ASIL-B
- Cybersecurity
Project Starting Point

- Company process training
- Practical product experience
- Implementing Functional Safety Req from customer
- Implementing Technical Safety Req from customer
- External training on specific tools and in areas of interest

Upgrading development process to ISO 26262:2018
- Staffing Function Safety Engineering team
- Staffing System & Software Quality Assurance (QA) team

Development Interface Agreement (DIA)

Safety Plan was delivered
The Project Mid Point

- Hardware Design
  - Provided to customer first for in vehicle testing of new software and features

HARA and Functional Safety Concept provided by the customer, then co-develop Technical Safety Requirements

Leverage COTS tool – ANSYS medini™ analyze
Hardware Analysis

- ISO 26262 provides detailed instruction for hardware with explicitly defined metrics and calculation methods.

- This is not the case for Software requirements or ISO 26262-6.
  - Due to the potential of systematic failure in software.
  - Is our Model-Based Design development process ISO compliant?
The ISO 26262 Gap Analysis

Project Objectives

Independent evaluation prior to final Audit and Assessment

Evaluate the implemented process and ensure work products are of sufficient quality

Technical Objectives

Implementation methods for Freedom from Interference using MBD

ISO consideration between “purchased code” and “reuse code”

Efficiency improvements in using MathWorks toolchain

Review of Tool Qualification artifacts
Weeklong daily interviews were held with the product development team to review their work products.

AM – Interview and work product reviews + feedback from previous day
PM – Analysis and review of results

Final deliverables:
- Gap Analysis Report
- Examples (model/scripts)

With the knowledge gained from the Gap Analysis Report, resources could now be directed to start the process of filling the gaps and ensuring that we would have the necessary work products for an Audit and Assessment.
The ISO 26262 Gap Analysis

- Weeklong daily interviews were held with the product development team to review their work products.
- AM – Interview and work product reviews + feedback from previous day
- PM – Analysis and review of results

- Final deliverables:
  - Gap Analysis Report
  - Examples (model/scripts)

- With the knowledge gained from the Gap Analysis Report, resources could now be directed to start the process of filling the gaps and ensuring that we would have the necessary work products for an Audit and Assessment.
Like many automotive projects, this project starts from a base of legacy production program.

Most of the design were from bottom up

Need to reconcile and ensure safety analysis is done per ISO requirement

Filling the Architecture Gap

System Engineer
(ISO 26262-4)

Focuses on software requirement and performing FMEA and DFA work. The results are documented, reviewed, and traced inside Polarion.

Software Engineer
(ISO 26262-6)

Focuses on software implementation and model verification workflow based on customer feature/functions and direction from System Engineering.

System engineering was new and was iterated with updates to software functions/features

Very practical way for executing ISO project with legacy base software
Filling the Unit Test Gap (ASPICE 3.0, SWE.3 – SWE.4)

- Polyspace was used for static code analysis
  - Run-time errors
  - Coding standards (e.g., MISRA)
  - Coding metrics

- Issue: the turnaround time for Polyspace was too long for development feedback – 2 weeks for a run
Filling the Unit Test Gap (ASPICE 3.0, SWE.3 – SWE4)

- Polyspace was used for static code analysis
  - Run-time errors
  - Coding standards (e.g., MISRA)
  - Coding metrics

- Issue: the turnaround time for Polyspace was too long for development feedback – 2 weeks for a run

- Result
  - Went from 2 weeks to overnight runs provide “near real time” feedback.
  - Polyspace Access was also used for generating Web accessible report back to development team.

Implement recommendation configurations with MathWorks guidance

Implement parallel processing
Create batch processing

Multi-core CPU

Improve Server compute power
Filling the Gaps – Tool Qualification

- For MathWorks tools, tool qualification was done based on internal know-how from BorgWarner’s technical expertise.
- For MathWorks toolchain, the results were reviewed against IEC Certification Kit as offered by supplier with similar contents.

ISO Work products

MathWorks IEC Certification Kit

ISO 26262

ISO26262-8:2018 Clause 11
Confidence in the use of Software Tool

- Tool Requirement, test case, and traceability
- Independent review of tool development process

- Planned tool usage
- Tool classification analysis

BorgWarner will be leveraging MathWorks Certification Kit for ISO tool qualification
Lessons learned in roles, tools, and process migration

- A Functional Safety project requires a lot of extra work that must be completed in ISO 26262-compliant fashion and on schedule to satisfy the end customer and an independent assessor.

- Sharing what we learned with other teams in the department working on Functional Safety projects created more awareness of the required processes and deliverables.

- Training classes in Functional Safety are essential for the product development teams success.

- Bring awareness to management of the role of software engineering in the architecture phase of the project and the additional work products required by a Functional Safety project.

- Sharing the advantages of using tools to automate and reduce the workload of manually creating the additional work products, for example the Polyspace automation project.

- A Gap Analysis can be a great way to assess the current situation and develop an actionable plan for moving forward. This should be considered early on during project development cycle.

- Tool qualification should be planned and performed as part of the project planning process.
ISO26262 Gap Analysis

Thank you!