Integrated Automotive Software Quality Management System in compliance with Automotive SPICE, ISO 26262, ISO 21448 and ISO 21434 Standards

Thota Krishna Hema

L&T Technology Services

DOI: 10.29322/IJSRP.12.01.2022.p12123

Abstract- With the increase in Automation of cars, the complexity of Automotive products increased in terms of safety and security. Functional safety and Cybersecurity are not add-on features to attract business they are essential for development and default on-demand expectations from the End users. This paper is about the Integration of Quality standards and Product development standards called Automotive SPICE V3.1, ISO 26262:2018, ISO 21448: 2019, and ISO 21434:2021. Automotive Industry is facing challenges with the definition of the Quality Management System in adherence to current international standards and frameworks. This paper provides a hybrid model on Integrating Automotive SPICE, Safety Engineering, and Security Engineering.

Index Terms- Automotive Quality Management System, Automotive Cybersecurity, Automotive Functional Safety, Automotive SPICE, SOTIF

I. INTRODUCTION

The average automotive vehicle life expectancy is 10 to 12 years. The Automotive system is getting complex day-to-day with the increase in automation. With the help of Artificial Intelligence (AI) and Machine Learning (ML), modern-day’s passenger cars can perform tasks similar to a virtual assistant. This brought in a new sort of challenge to Automotive Manufacturers (OEMs) and Automotive suppliers in terms of Safety and Security. Currently, we are implementing and Exhibiting adherence to Automotive SPICE and ISO standards separately with individual expert teams. This approach makes us ambiguous while developing of product and in the end, the cost of conformance/compliance certification increases to multiple folds with this Individual approach when compared to normal Automotive product development. An Integrated Quality Management system with the combination of Automotive SPICE(ASPICE) framework and ISO standards for Cybersecurity (ISO 21434), Functional Safety (ISO 26262), and SOTIF (ISO 21448) can be possible due to some commonalities among them.

This hybrid approach on Integrating ASPICE framework and ISO Standards in one Quality Management System saves the cost of development, would be efficient in implementation and the optimization of product design happens with the minimum number of revisions and less rework.

Automotive SPICE framework is about Automotive product’s System Engineering, Software Engineering and mainly focuses on four key concepts Qualified Inputs to get Qualified Outputs, Agree and Summarize, Divide and control and traceability. Functional Safety is about in-vehicle electronics malfunctioning which causes harm to the driver and passengers in the car. SOTIF is about driving scenarios at different operational environments and Misuses. Whereas cybersecurity is about the malicious human attack on vehicles through interfaces in Software and Hardware. Cybersecurity can impact functional safety and SOTIF by the identification of new cybersecurity critical assets which need to be secured.

Here we are proposing a Hybrid Model called Integrated Quality Management System which satisfies the integrated implementation of ASPICE, ISO 21448, ISO 26262, and ISO 21434 together in order to save developmental cost, with less rework, to increase the effectiveness and efficiency of the existing system, to raise the productivity of resources by bringing in clarity of work in terms of step-by-step process.

Challenges with Integrated Quality Management System:
Until now we discussed the pros of an Integrated Quality Management System. The main challenge here is even though these frameworks and standards look similar, there are a lot of differences in their implementation. An integrated approach may not be the easy approach as each standard has been developed independently and has a different set of requirements.

Definition:
“This Integrated Quality Management System is to fetch synchronization among the implementation of ASPICE framework and ISO standards to optimize the Automotive software development process by regulating the differences in standards and bringing them into the common agreement”

II. RESEARCH ELABORATIONS

Every Quality or Product Development Framework or ISO Standard is developed based on the following factors:
1) Framework
2) Product Lifecycle
3) Processes and Work products

High-level Comparison of Standards with respect to software product development:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>ASPICE</th>
<th>ISO 26262</th>
<th>ISO 21448</th>
<th>ISO 21434</th>
</tr>
</thead>
<tbody>
<tr>
<td>Goal</td>
<td>Automotive Grade Software Development</td>
<td>To protect health/life of humans inside car</td>
<td>To protect health/life of humans inside car and other road users</td>
<td>To Protect Assets</td>
</tr>
<tr>
<td>Lifecycle Applicability</td>
<td>All Phases</td>
<td>All Phases</td>
<td>Implicit to ISO 26262</td>
<td>All Phases</td>
</tr>
<tr>
<td>Risk Based</td>
<td>Project Risk</td>
<td>Functional Safety Risk</td>
<td>Functional Safety and SOTIF Risk</td>
<td>Security and Safety Risks</td>
</tr>
<tr>
<td>Risk Assessment Model</td>
<td>Risk Matrix with ratings</td>
<td>HARA (Hazard Analysis and Risk Assessment)</td>
<td>HARA (Hazard Analysis and Risk Assessment) based on STPA (System Theoretic Process Analysis)</td>
<td>TARA (Threat Analysis and Risk Assessment)</td>
</tr>
<tr>
<td>Process and Management</td>
<td>Organizational and Product Oriented</td>
<td>Organizational and Product Oriented</td>
<td>Implicit to ISO 26262</td>
<td>Organizational and Product Oriented</td>
</tr>
<tr>
<td>Life cycle Model</td>
<td>V-Model with System, Software, Support and Management Process Areas</td>
<td>V-Model with System, Hardware and Software development</td>
<td>Implicit which is based on ISO 26262, Concept Phase and Risk Analysis</td>
<td>Implicit which does not have a dedicated V-Model, System design and Supporting Processes</td>
</tr>
<tr>
<td>Supporting Processes</td>
<td>Many</td>
<td>Many</td>
<td>Depends on ISO 26262</td>
<td>Depends on ISO 26262</td>
</tr>
<tr>
<td>Continuous Activities</td>
<td>Adherence Assessments</td>
<td>Passive Monitoring</td>
<td>Active Monitoring</td>
<td>Active Monitoring, Incident Response, Event Assessment</td>
</tr>
<tr>
<td>Methods</td>
<td>Adherence Dashboards based on N, P, L, F Ratings</td>
<td>HARA, FTA, FMEA, HAZOP, Fail Operational, Redundancy</td>
<td>HARA, STPA, FTA, FMEA, HAZOP, Fail Operational, Redundancy</td>
<td>TARA, Cryptography, ID/IP, Key Management, Firewall, Secure Flash/Boot, Hypervisor, Synchronized time Manager</td>
</tr>
</tbody>
</table>

A High-level Integration of ASPICE, Functional Safety, SOTIF and Cybersecurity:
Differences Between HARA and TARA:

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Hazard Analysis and Risk Assessment (HARA)</th>
<th>Threat Analysis and Risk Assessment (TARA)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aim</td>
<td>To Identify Hazards and Assess the Level of Safety Risks i.e., ASILs</td>
<td>To Identify Threat Scenarios and Assess the Level of Cybersecurity Risks i.e., CALs</td>
</tr>
<tr>
<td>Important terms</td>
<td>Hazards, Operating Scenarios, Driving Situation, Deviation, Possible cause, Consequences, Severity, Exposure, Controllability, ASIL, Safety Goal, Safety State, FTTI</td>
<td>Asset Identification, Impact rating, Threat scenarios, Attack path, Attack feasibility rating, Risk level, Risk Determination, Risk Treatment Decision, Cybersecurity Goal, Cybersecurity Concept</td>
</tr>
<tr>
<td>Risk Level</td>
<td>ASIL (Automotive Safety Integrity Level) A, B, C and D</td>
<td>CAL (Cybersecurity Assurance Levels) CAL 1, 2, 3, and 4. Risk Values from 1 to 5</td>
</tr>
<tr>
<td>Inputs</td>
<td>Item Definition</td>
<td>Item Definition</td>
</tr>
<tr>
<td>Outputs</td>
<td>Hazards, ASIL levels, Safety Goals</td>
<td>Threat Scenarios, Risk Levels and Cybersecurity Goals</td>
</tr>
<tr>
<td>Procedure</td>
<td>Identification and Analysis of all probable malfunctions in expected operational scenarios and identification of hazardous situation for each hazard, determination of ASIL Levels and Safety Goals</td>
<td>Identification and Analysis of all probable assets of an item and associated threats that can cause a damage scenario. Determine the cybersecurity risk level and cybersecurity goal for each threat scenario</td>
</tr>
</tbody>
</table>

Cybersecurity Impact categories are of four types. They are Privacy, Operational, Financial, and Safety. When a Cybersecurity attack leads to a safety hazard, then we need to perform HARA as part of a TARA. Only when the category of cybersecurity Impact is safety. Introduction of cybersecurity controls can cause functional safety hazards due to new architecture element introduction like key or crypto primitives. If the element fails due to malfunction it can lead to a safety hazard. The safety mechanism activation may be a target for the malicious hacker.

Synchronized Safety and Security: Example of Firewall Introduction in Automotive System in terms of Cybersecurity.

III. RESULTS OR FINDING

Framework:

The framework is a skeleton which is put into organized practices. ASPICE is a well-defined Framework with Base practices, Process Outcomes, and Work product expectations. But other three ISO standards discussed in this paper are built on a Risk-Based Framework. Risk Management as per ASPICE is defined in MAN.5 Process Area. Although it is not in VDA Scope, many organizations consider this process area as in their organizational scope. ASPICE recommends identifying and Analyzing risks to avoid potential issues. But
for other ISO standards Risk is a core concept. Even though there are a few commonalities, they are not identical in the Risk-based framework. The Integration can be possible by modeling the individual parts of frameworks and methodologies at the high-level concept. Let us consider a Risk-based Framework.

FUSA risk levels are ASILs (Automotive Safety Integrity Levels) and Cybersecurity risk levels are CALs (Cybersecurity Assurance Levels). SOTIF risks are expressed in terms of Exposure (E), Severity (S), and Controllability (C).

Product Lifecycle:

A common Lifecycle across the ISO standards includes
1) Concept Phase
2) Product Development Phase
3) Post Development Phase or Production, Operation, and Maintenance Phase

ASPICE has V-Model for Primary Lifecycle Processes which includes System Engineering and Software Engineering Processes with Support, Acquisition, Supply, Management, Reuse, and Process Improvement Group Processes. ISO 26262 has V-Model for System, Hardware, and Software Development. ISO 21448 has no explicit V-Model or Product Lifecycle. It is Implicit in the functional safety life cycle. ISO 21434 also has an Implicit V-Model for Product Lifecycle which we can extract from ISO 26262.

All these three ISO Standards look similar at a high level.

<table>
<thead>
<tr>
<th>ISO Standards</th>
<th>Concept Phase</th>
<th>Product Development Phase</th>
<th>Post Development Phase</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>9.3. Item Definition</td>
<td>10.4.1. Design</td>
<td>13. Operations and Maintenance</td>
</tr>
<tr>
<td></td>
<td>9.5. Cybersecurity Concept</td>
<td>11. Cybersecurity Validation</td>
<td>13.4. Updates</td>
</tr>
<tr>
<td></td>
<td></td>
<td>5. Product Development at the Hardware Level</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>6. Product Development at the Software Level</td>
<td></td>
</tr>
</tbody>
</table>
Processes and Outcomes:

The Automotive SPICE framework has clearly expressed processes, outcomes, and respective work products. Similarly for ISO 26262, ISO 21448, ISO 21434 standards have clauses, sub-clauses, and associated work products. These clauses and Sub-clauses help in defining process flows say example process for Software Integration testing. For Integration, we need to design work products to satisfy more than one standard like the Software Integration Test Specification template.

ISO 21434 and ISO 21448 do not have separate explicit V-Models at the Product development Phase. These are Implicit to ISO 26262 V-Model. Requirements for Cybersecurity are more when compared to Functional Safety, SOTIF, and ASPICE. Here is the Venn-diagram of ASPICE, Functional Safety, SOTIF, and Cybersecurity
Here are some of the example work-products with the categorization of Integration:

1) Easy to Integrate
   - Item Definition
   - Safety and Security Concept
   - Safety and Security requirements for Post-development
   - Software Integration Specification
   - Software Verification Specification

2) Partially possible to Integrate
   - Risk Assessment and Decisions
   - Safety and Security Goals
   - Safety and Security claims
   - Revised Safety and Security Specification

3) Unique Work products
   - Safety Analysis report
   - Vulnerability Analysis report
   - Cybersecurity Incident response plan

IV. CONCLUSIONS

- It is possible to integrate Automotive SPICE, ISO 26262, ISO 21448 and, ISO 21434 as Quality Management System even though there are different requirements involved and independently defined by different development teams.
- Integration of Quality Management System enables regulating and integration of differences and variations in the implementation of these standards into a common agreement.
- The Integration of Quality Management System is considered by following aspects.
  - Framework
  - Product Lifecycle
  - Processes and Outcomes
- Integration of Automotive SPICE, ISO 26262, ISO 21448, and ISO 21434 as Quality Management System brings add-on benefits like to save the cost of implementation, avoiding unnecessary rework caused by lack of clarification, to increase effectiveness and efficiency by the usage of united outcome work products and easy to use.

ACKNOWLEDGMENT

I would like to express my deep gratitude to Dr. Philip Koopman, Associate Professor, Carnegie Mellon University for his valuable and constructive suggestions during the planning and development of this research work. His willingness to give his time so generously has been very much appreciated.

I would also like to thank the colleagues of the L&T technology Services for enabling me to visit their offshore development centers to observe their autonomous car project work.

REFERENCES

AUTHORS

First Author – Thota Krishna Hema, Specialist, Automotive Quality Assurance, L&T Technology Services, thota.hema@ltts.com

Correspondence Author – Thota Krishna Hema, thota.hema@ltts.com, askhemathota@gmail.com, 91-9347955949.