ISO26262: How to Manage it at your organization?

Andre Marchezan
Claudio Guercio Labate
Leandro Moreira da Silva
Robson Marcelo Vicente
Ford Motor Company Brasil Ltda.

ABSTRACT

The increased number of complex features has given more automatic and "intelligent" decisions for vehicle systems. Automatic emergency brake, activate steering assistance, remote parking are few examples of these features.

Development of such functionalities requires deep knowledge about system architecture and properly management to identify and threat hazard events caused by possible malfunction behaviors.

ISO26262 comes to governance this complex development by providing appropriate processes and guidelines to design a reliable and robust system for entire vehicle lifecycle (development, production, operation, service and decommission) to assure absence of unreasonable risk. Compliance to this standard is critical for OEM's and suppliers.

ISO26262 is ample and difficult to assimilate. It directly impacts culture changes for traditional automobile industry. Although the standard has been released for more than 10 years it is still relatively new for several organizations and engineers.

This paper proposes to identify the required organization changes to ensure company and team involvement in the execution of the safety lifecycle for a given component/system and create a measure method to manage ISO26262 implementation

INTRODUCTION

Vehicle complexity has increased over the years with the introduction of new features and standardization of drive-by-wire systems. Safety regulations and consumer demand for performance and convenience have led to an exponential spike in cars' software complexity. 15 years ago, an average vehicle sold in North America would have around 10 million code lines. This number has exponentially increased to about 100 million in 2019 and can achieve up to 1 billion in future with level 5 autonomous vehicles [1].

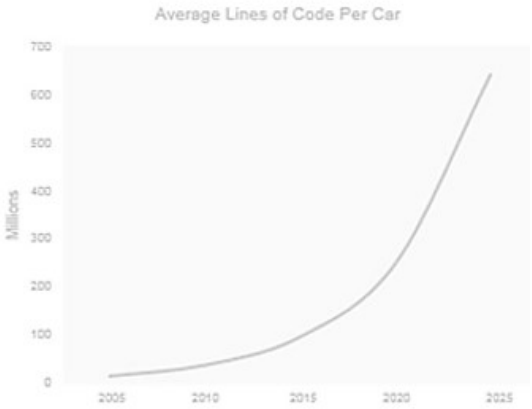

Figure 1: Evolution of Lines of Codes Per Car

Recalls associated to electrical systems have increased over time. According to United States National Highway Safety Administration, in 2019 there were 85 recalls at automotive industry caused by software issues (3.2 times greater when compared to 10 years earlier). Software issues recall responded to almost 20% of all total recalls during the year of 2019 [2].

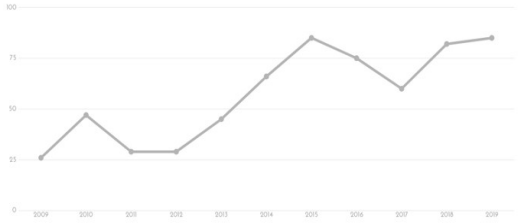

Figure 2. Number of Software related recalls in USA

It was inevitable that a functional safety standard would need to be created to govern the design, development, and implementation of automotive complex systems. ISO 26262 introduced those standards in 2011; while an update version of this standard was released in 2018.

Before we start discussing functional safety standard and how to manage it inside of an automotive company, it is important to understand the functional safety context. Safety is defined as being free of any unacceptable risk that could lead to human harm. Risk can be defined as the union of the severity of harm and the probability of harm occurs. Functional safety is defined as the process of achieving the

absence of unreasonable risk that is caused by hazards caused by malfunctioning of an electric or electronic systems. A malfunction can be either a systematic failure (e.g.: software issue) which can be eliminated only by changing the design or manufacturing process; or it can be a random hardware failure which can occur at any time, unexpected, during the vehicle lifetime (production, operation, service, and decommissioning).

Functional Safety is a process that takes role during whole V-Model Lifecycle (Figure 3). Functional Safety starts at left side of the V-Model. It initiates early at concept phase development and requirement definition (system, hardware, software, and integration). And is concluded at the right side of the V-Model by completing hardware, software unit, integration, and system validation (Figure 4).

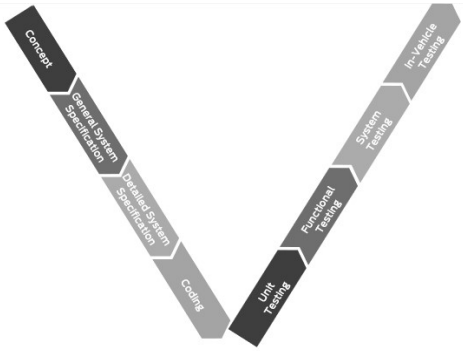

Figure 3: V-Model

Figure 4: ISO26262 Implementation in phases

The company must define who would be the project manager that could also lead with Functional safety management. Functional Safety is one of the issues that project managers must coordinate when developing electronics for vehicles.

Usually, the problems come at the end of the project, as the safety of the product cannot be proven, but it is possible when the organization works together and methodologies from the work product are developed during an initial period.

If the company does not make a management of Functional Safety, means that ISO 26262 is not compliance and There is no Functional Safety develop on the process.

Safety management from ISO26262 requires more procedures that must be defined and applied for electronics development. When we go through the complete ISO 26262, it is possible to find many topics that make deep on usual project management, and it requires specific knowledge from Functional Safety area. This means that some confirmation and reviews are required to develop Safety concept, safety cases, technical Requirements.

Procedures should be defined taking into consideration the company lifecycle, definition of tools management, type of performance analyses and management configuration. Quality management is supported by ISO 26262 and qualified/trained people to the work assigned. This requires the company to be at a management competence level from the organization.

Referring to Functional Safety in your process, you can ensure that your system identifies, establishing a way how to improve the information and solve the problem to guarantee the Safety functionality, where the system can ensure that Functional Safety is met from vehicle production, when detect violation of safety goals and process could be defined/updated.

An automotive company which follows ISO 26262 has a competitive edge in the market, it assures that a high level of safety is achieved. The scope of this paper is to discuss functional safety management during whole vehicle lifecycle and propose a measure method to governance its implementation

HARD CULTURAL CHANGES

The implementation of a standard requires considerable effort to ensure effectiveness. The management commitment, teamwork and knowledge cascading throughout the company are critical to get success for maintaining these standard systems [3]. Some important obstacles to effective implementation are communication, lack of involvement, properly responsibilities, processes, culture and resistance to change [4]. The behavior of employees is also critical for certification and maintaining of any standards [5].

First vision about ISO 26262 standard without a deep analysis seems cost increase. It is an initial difficulty regarding safety culture development once the product price reduction is an important part of traditional tradeoff considered by vehicles companies even though, after 90’s, this mentality has been changing because quality management system implementation requests i.e.: Automotive Industry Action Group (AIAG)/QS9000 [6].

The ISO 26262 standard requires stricter documentation for evidence-based safety. It imposes a special approach to understand and implement these additional work products. Each work product needs a previous verification and after confirmation review for different teams. It is a significant work culture change

because implementation of simple requirements needs little individual operations afford. However, complex requirements require the participation of several people, for more complex decisions and technically demanding activities.

Despite this workload seems cost, it could be an opportunity to reduce field problem and consequently cost of poor quality because the ISO 26262 system supports and motivates the effective achievement of functional safety protecting safety and quality [7].

REFLECTING IMPLEMENTATION COSTS

When we talk about costs for implementing functional safety, we are talking about a number that is very hard to determine for the automotive industry. It depends on how complex is the system and ASIL Rated determined at Hazard Analysis and Risk Assessment. It is expected less investment to deliver a ASIL A compliance system when compared to an ASIL D. It shall also be considered that it may be possible to decompose a ASIL D requirement in different combinations (e.g.: ASIL A + ASIL C, ASIL B + ASIL B, 2 * ASIL A + ASIL B or 4 * ASIL A) [8] and this requirement decompose will directly affect project costs. It is expected that a system that was able to decompose into 4 * ASIL A requirements to be less expensive than the one which could not be decomposed at different sub-sets. How much less? Difficult to provide an estimative. Headcount, functional safety training, hardware components (with higher robustness and reliability), software coding and management are all good examples about how ISO26262 impacts the budget planning.

Regarding headcount, ISO 26262 immediately requires at least one safety manager and a dedicated headcount for each vehicle system. Refer to Figure 5: 10 systems = 10 heads. We can consider these costs as "entry costs" to responsibly ensure that these valuable systems do not inadvertently cause damage. Ignoring the implementation of ISO 26262 is assume the risk of losses with high values (e.g.: litigation, warranty and recall in the future, not to mention the risk of loss of human life)

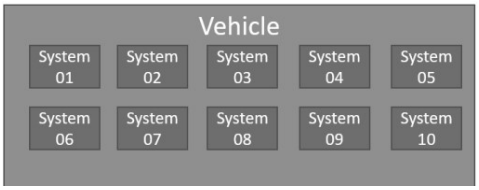

Figure 5: Headcount Allocation

MEASUREMENT PROPOSAL

Checklist is a versatile, customizable and effective tool to make an initial engagement assessment and manage actions to implement ISO 26262 in companies. As it is a strategic tool for completing tasks, it consists of a list of items that are completed when each task is performed.

After all, it gives the necessary support to identify non-conformities and ensure that everything works properly.

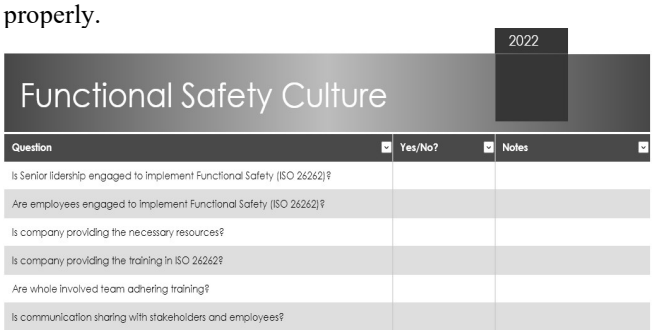

Figure 6: Functional Safety Culture Checklist

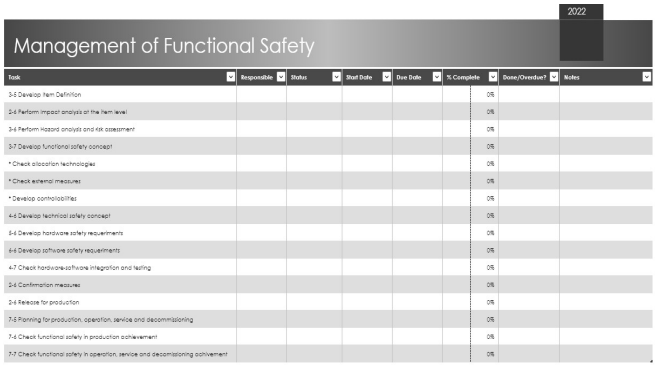

Figure 7: Functional Safety Management Checklist

CONCLUSION

The increasing competitiveness of the market requires to attend standards available. There are several obstacles as bureaucracy and documents to deal. Besides that, cultural changes are vital during implementation journey. It is not easy to move from a cost driven to a quality driven culture. It may take several months if not years, but the benefits are real. Financials normally do not properly monetize the cost of poor quality. The cost of poor quality comprises not only the costs resulting from the defective product, but also compromises processes (productive and non-productive) and even worse, poor quality also weaken consumer relationships. ISO 26262 implementation is not possible if the company does not change its mindset.

REFERENCES

[1] FILLOUX, FREDERIC. Reinventing the car, episode 5

[2] NHTSA DATABASE – MARCH 2020

[3] CHIN, K. S. The critical maintenance issues of the ISO 9000 system: Hong Kong manufacturing industries perspective. Work Study, v. 49, nº 3, p. 89-96, 2000

[4] FUENTES, C. M. Analysis of the implementation of ISO 9000 quality assurance systems. Work Study, v. 49, nº 6, p.229-241, 2000.

[5] CHENG, S. P.; TUMMALA, V. M. An employee involvement strategy for ISO 9000registration and maintenance: a case study for Hong Kong and China companies. International Journal of Quality & Reliability Management, v. 15, nº 8/9, p. 860-891, 1998.

[6] AIAG, http://www.aiag.org/scriptcontent/index.cfm.

[7] ISO 26262 2nd Ed., Part 2 Table B.1, 2018.12

[8] ISO26262 2nd Ed., Part 9 Session 5.4.9, 2018.12