Original Article
https://doi.org/10.56094/jss.v58i2.252

International System Safety Society

www.jsystemsafety.com

Journal of System Safety

Established 1965 Vol. 58 No. 2 (2023)

Review of the Latest Developments in Automotive Safety Standardization for Driving Automation Systems

Rami Debouk[ab]

[a] *Corresponding author email: rami.debouk@gm.com*
[b] *General Motors R&D, Warren, MI*

Keywords
functional safety, safety of the intended functionality, driving automation systems

Peer-Reviewed
Gold Open Access
Zero APC Fees
CC-BY-ND 4.0 License

Online: 22-Jun-2023

Cite As:
Debouk, R. Review of the Latest Developments in Automotive Safety Standardization for Driving Automation Systems. Journal of System Safety. 2023;58(2):40-45. https://doi.org/10.56094/jss.v58i2.252

ABSTRACT

The ISO 26262: Functional Safety – Road Vehicles Standard has been the de-facto automotive functional safety standard since it was first released in 2011. With the introduction of complex driving automation systems, new standardization efforts to deal with safety of these systems have been initiated to address emerging gaps such as the human/automation roles and responsibilities in the presence/absence of the driver/user, the impact of the technological limitations and the verification and validation needs of automation systems to name a few. This paper highlights some of these gaps and introduces some of the latest developments in automotive safety standardization for driving automation systems.

INTRODUCTION

Safety-critical systems are systems that have the ability to create potentially hazardous issues in case they do not operate properly or as designed (Ericson-II, 2005), (Leveson, 2001). These systems are in general analyzed using rigorous and systematic safety processes (Bahr, 1997), for instance ISO 26262 (ISO 26262, 2018), Functional Safety – Road Vehicles, in the automotive domain.

The effort of standardization in the area of automotive functional safety accelerated in the last couple of decades as automotive systems became more complex, integrated and software intensive. As a matter of fact, the automotive industry is not as regulated as other industries, hence harmonized guidelines and best practices across the industry may have not been widely available. This definitely helped kick off the automotive functional safety standardization into a higher gear, and it all started with the adaptation of existing standards to the automotive domain.

ISO 26262 was launched as the adaptation of (IEC 61508, 2010) to comply with needs specific to the application sector of Electrical/Electronic systems within road vehicles. ISO 26262 applies to all activities during the safety lifecycle of system development. At the concept phase, the hazard and risk assessment process focuses on identifying possible hazards caused by malfunctioning behavior of E/E safety-related systems and mitigating them through the identification of safety goals. The design phase includes system, hardware, and software development with requirements derived from the safety goals. ISO 26262 also prescribes the functional safety management activities to be performed during the safety lifecycle and provides requirements on the supporting processes.

However, ISO 26262 application faced some challenges, especially with the introduction and development of automations levels 2 and above driving automation systems (DAS) (SAE J3016, 2021). These systems split the roles and responsibilities of performing the dynamic driving tasks between the driver and the automation system: Levels 2 and 3 still have the driver responsible for some of these tasks while the automation system is fully responsible for these tasks in Levels 4 and 5. Moreover, they may be impacted by some technological limitations in the components they use not to mention that some of these components may not be fully specified, e.g., a Machine Learning (ML) component. Consequently, many standards/documents were drafted and published to address these issues that were not fully addressed by ISO 26262.

This paper is organized as follows. An overview of ISO 26262 and some identified challenges in applying it to DAS are presented first. Next, some of the recently developed automotive safety standards, specifications and guidelines are listed and a brief overview of some of these standards, specifications, and guidelines is provided while focusing on the specific issues they address. Finally, some thoughts on the current state in using the automotive safety standards is provided.

ISO 26262

Overview

ISO 26262 is the de facto standard for functional safety in the automotive electronics domain. It is the adaptation of IEC 61508 to comply with needs specific to the application sector of Electrical/Electronic systems within road vehicles. The adaptation applies to the automotive safety lifecycle of safety-related systems comprised of electrical, electronic, and software elements that provide safety-related functions.

ISO 26262 develops a structured and systematic process for safety analysis to guarantee product integrity and avoid recalls in the field. Requirements cover concept phase to decommissioning alongside safety management and supporting processes. Below is a highlight of the major activities described in the standard. The reader is referred to (Debouk, Overview of the 2nd Edition of ISO 26262: Functional Safety - Road Vehicles, 2019) and (Debouk & Joyce, ISO 26262 Hazard and Risk Assessment Methodology, 2010) for a comprehensive overview of the standard and its hazard analysis and risk assessment process.

At the concept phase of ISO 26262 is the hazard analysis and risk assessment process. This process provides an automotive specific risk-based approach for determining risk classes. Potential hazards caused by malfunctioning behavior are identified and categorized and safety goals related to the prevention or mitigation of these potential hazards are formulated. Each safety goal is assigned an Automotive Safety Integrity Level (ASIL) and the ASIL is determined by a systematic evaluation of hazardous situations. In determining the ASIL one considers the estimation of the following factors: severity, probability of exposure and controllability. It is worth noting here that controllability is defined as the ability to avoid harm by actions of traffic participants. Functional safety requirements needed to avoid an unreasonable risk for each potential hazard are derived from the safety goals which are not expressed in terms of technological solutions, rather in terms of functional objectives. Functional safety requirements inherit the ASIL of the safety goal from which they are derived.

The product development at the system level per ISO 26262 starts with developing the technical safety concept. The technical safety concept specifies the technical safety requirements and their allocation to system elements (hardware and software). The technical safety requirements inherit the ASIL of the functional safety requirements they refine and specify safety mechanisms to detect faults and mitigate or control failures that may lead to the violation of these functional safety requirements and hence the safety goals. Safety mechanisms are technical solution to detect and mitigate (through avoidance or control) faults/failures in order to maintain intended functionality or achieve or maintain a safe state. The technical safety concept defines the system architectural design as well. The development of the technical safety concept is then detailed at both the hardware and software levels. Once the hardware and software developments are complete, all elements are integrated and tested. Finally, safety validation is completed at the vehicle level, that is evidence is provided that safety goals have been met. Figure 1 below graphically represents this development.

A safety case is published before releasing to production and it is a documentation to communicate a clear, comprehensive, and defensible argument (supported by evidence compiled in work products) that a system is acceptably safe to operate in a particular context.

KEY CHALLENGES

In the context of L2 to L5 DAS, the application of ISO 26262 faces a couple of challenges. A few of these challenges is discussed below:

- *Determination of the controllability parameter:* controllability is defined in ISO 26262 as the ability to avoid harm by actions of traffic participants. Since the role of the automation system in performing the dynamic driving tasks increases as the level of automation increases, the relevance of the controllability parameter becomes somehow questionable in determining the ASIL when performing the hazard analysis and risk assessment.
- *Definition of the safe state:* in the presence of human drivers, many systems relied on them as part of the definition of the safe state making the system fail safe or silent. However, with the reduced responsibility of human drivers in performing the dynamic driving tasks, fail-operational behavior and availability requirements maybe needed to maintain that the automation system achieves or reaches a safe state following the occurrence of a malfunctioning behavior.
- *Addressing hazards due to nominal performance:* ISO 26262 did not analyze hazards of nominal performance such as ones due to incomplete specifications or technology

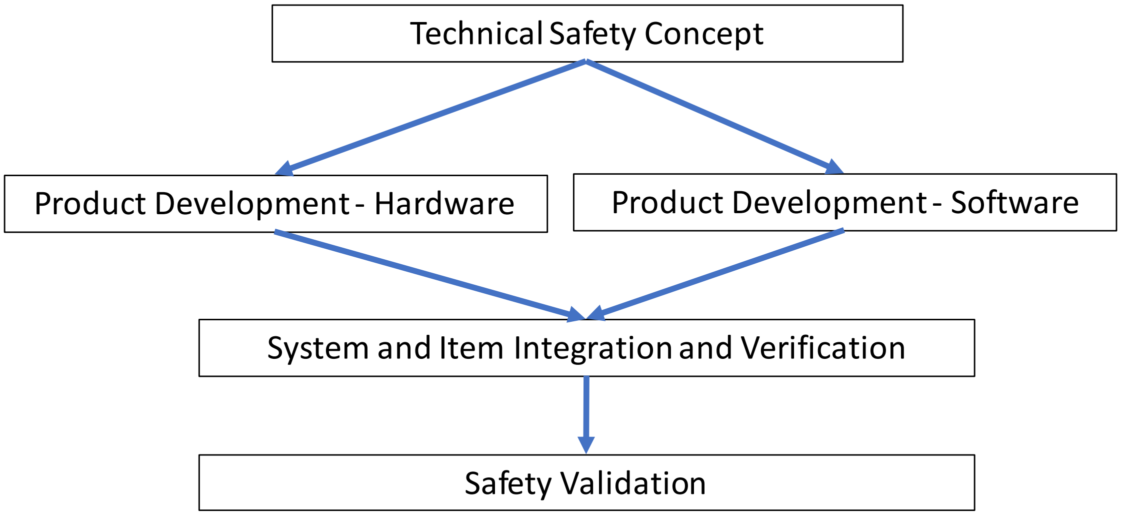
Technical Safety Concept
Product Development - Hardware
Product Development - Software
System and Item Integration and Verification
Safety Validation

Figure 1: Product Development per ISO 26262

limitations. The latter are referred to as functional insufficiencies and are addressed in the Safety Of The Intended Functionality (SOTIF) standard ISO 21448 (ISO 21448, 2022).

- *Analyzing cybersecurity threats and their impact on safety:* As hazards may be caused or triggered by security threats, these threats are to be considered and analyzed as part of the hazard analysis and risk assessment. ISO 26262 recognized this issue and required synchronization of analyses between safety and security responsible teams at few instances in the vehicle development process.
- *Considering operational safety:* operational safety considers in general the health of the systems and components of the vehicle and with a less involved human driver such topic requires some planned procedures to monitor these systems and components.
- *Dealing with the use of Artificial Intelligence (AI) and ML models or components:* AI/ML models or components are usually treated as black boxes making them not fully specified and resulting in challenges when analyzing and verifying them.

AUTOMOTIVE SAFETY STANDARDS, SPECIFICATIONS AND GUIDELINES FOR DAS

In order to address the challenges listed above, many standards, specifications and guidelines were drafted and published by many organizations. A non-exhaustive list of these standards/documents is provided in Table 1, and some of these standards/documents are briefly discussed afterwards.

ISO FDIS 21448: Road vehicles - Safety of the intended functionality

SOTIF by definition deals with the absence of unreasonable risk resulting from functional insufficiencies or due to reasonably foreseeable misuses. A functional insufficiency is either an insufficiency of specification or a performance limitation, hence SOTIF complements the scope of ISO 26262 by addressing hazards caused by the intended functionality, i.e., the nominal performance. This is depicted in Figure 2 below.

Table 1: Automotive safety standards, specifications, and guidelines

ISO 21448: Road vehicles - Safety of the intended functionality (https://www.iso.org/standard/77490.html)
UL 4600 Ed. 2-2022: Standard for Evaluation of Autonomous Products (https://www.shopulstandards.com/ProductDetail.aspx?productid=UL4600)
ISO/FDIS 34502: Road vehicles - Engineering framework and process of scenario-based safety evaluation (https://www.iso.org/standard/78951.html)
ISO/TR 4804: Road vehicles - Safety and cybersecurity for automated driving systems - Design, verification and validation methods (https://www.iso.org/standard/80363.html)
ISO AWI TS 5083: Road vehicles - Safety for automated driving systems - Design, verification and validation (https://www.iso.org/standard/81920.html)
SAE J3016: Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles (https://webstore.ansi.org/standards/sae/sae30162021)
SAE J3018: Safety-Relevant Guidance for On-Road Testing of Prototype Automated Driving System (ADS)-Operated Vehicles (https://webstore.ansi.org/standards/sae/sae30182020)
SAE J2980: Considerations for ISO 26262 ASIL Hazard Classification (https://webstore.ansi.org/standards/sae/sae29802018)
SAE J3206: Safety Principles (https://webstore.ansi.org/standards/sae/sae32062021)
BSI PAS 1880: Guidelines for developing and assessing control systems for automated vehicles (https://www.bsigroup.com/en-GB/CAV/pas-1880/)
BSI PAS 1881: Assuring the safety of automated vehicle trials and testing – Specification (https://www.bsigroup.com/en-GB/CAV/pas-1881/)
BSI PAS 1883: Operational design domain (ODD) taxonomy for an automated driving system (ADS) – Specification (https://www.bsigroup.com/en-GB/CAV/pas-1883/)

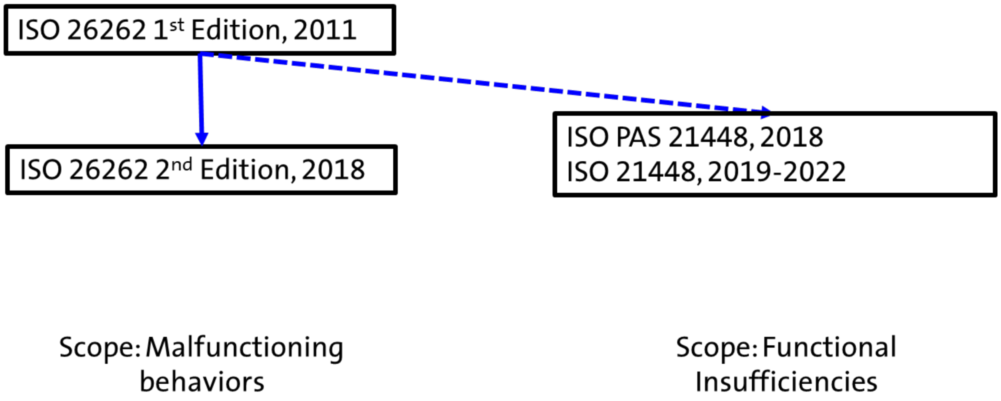
ISO 26262 1st Edition, 2011
ISO 26262 2nd Edition, 2018
ISO PAS 21448, 2018
ISO 21448, 2019-2022
Scope: Malfunctioning behaviors
Scope: Functional Insufficiencies

Figure 2: Scope of ISO 26262 vs ISO 21448

ISO 21448 provides guidance on the applicable design, verification and validation measures needed to achieve SOTIF. This includes the system specification, identification and evaluation of hazards caused by the intended functionality, and any modifications needed to reduce the risk due to SOTIF. In addition, the verification and validation strategy and activities are discussed as well as the method to accept the residual risk following the SOTIF activities. ISO 21448 includes an annex to address AI/ML components. The expectation is that ISO 21448 is complementing the safety activities performed while following ISO 26262.

UL 4600 Ed. 2-2022: Standard for Evaluation of Autonomous Products

UL 4600 is intended to work with existing standards to provide the additional elements necessary to assure that safety aspects of fully autonomous item operation have been considered in a comprehensive manner when creating a safety case. It is currently in its second edition with the first edition released in 2020. While use of existing functional safety standards is highly desirable, it is likely that there will be gaps between successful conformance to those standards and the creation of an acceptable safety case for complex autonomous items.

The main goal of UL 4600 is to make sure that the cumulative work products produced as a consequence of following other standards and other best practices do not leave any holes that present an unreasonable risk to autonomous product safety. In particular, compatibility with ISO 26262 and ISO21448 has been considered.

Two areas out of scope for this standard are setting acceptable risk levels and setting forth requirements for ethical product release decisions and any ethical aspects of product behavior.

ISO/FDIS 34502: Road vehicles - Engineering framework and process of scenario-based safety evaluation

ISO 34502 provides guidance and a state-of-the-art engineering framework for automated driving systems test scenarios and scenario-based safety evaluation processes. Therefore, ISO 21448 would benefit from the proposed process in identifying and evaluating scenarios, the latter being integral to the SOTIF safety activities.

ISO/TR 4804: Road vehicles – Safety and cybersecurity for automated driving systems – Design, verification and validation methods

ISO 4804 describes guidelines in developing, verifying, and validating driving automation systems based on basic safety principles. It also considers safety- and cybersecurity-by-design. ISO 4804 is merely a technical report and will be withdrawn once ISO TS 5083 is published.

ISO AWI TS 5083: Road vehicles — Safety for automated driving systems — Design, verification and validation

This document provides an overview and guidance of the steps for developing and validating an automated vehicle equipped with a safe automated driving system. It considers and details steps for developing a safety concept, designing for safety, verifying, and validating DAS of Levels 3 and 4 as well as post deployment safety activities. In addition, it outlines cybersecurity considerations throughout all described steps. ISO TS 5083 includes an annex to address AI/ML components.

ISO TS 5083 will benefit from both ISO 26262 and ISO 21448 as the "generic" standards to which its application is intended, that is DAS features of Levels 3 and 4.

SAE J3016: Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles

This foundational report defines automation levels, operational design domains (ODD), object and event detection and response, minimal risk conditions among many others, all of which are fundamental in the development of the standards, specifications and guidelines for DAS features of Levels 2 and above.

BSI PAS 1881: Assuring the Safety of Automated Vehicle Trials and Testing – Specification

This publicly available specification specifies the minimum requirements for safety cases for automated vehicle trials and development testing in the United Kingdom to demonstrate activities can be undertaken safely. Even though BSI PAS 1881 deals with development vehicles, its application would benefit vehicle manufacturers in assessing their vehicles ahead of releasing them on public roads.

BSI PAS 1883: ODD Taxonomy for an Automated Driving System – Specification

This publicly available specification provides requirements for the minimum hierarchical taxonomy for specifying an ODD to enable the safe deployment of an automated driving system (Levels 3 and above in J3016). The ODD comprises the static and dynamic attributes within which an automated driving system is designed to function safely. It clearly aligns itself in support of the vehicle manufacturers designing DAS features.

FINAL THOUGHTS

For higher automation level systems (Levels 3 and above in J3016), no direct safety design or assessment guidance is provided in ISO 26262. Therefore, automotive safety engineers performing safety analysis on higher automation level systems need to go beyond what ISO 26262 requires. This can be achieved by interpreting and/or adapting ISO 26262 requirements in the context of the higher automation level systems they are analyzing. ISO TC22/SC32/WG08 that developed ISO 26262 is looking at the gaps and challenges currently in order to provide some guidance until the work on the 3rd Edition of ISO 26262 starts. In the meantime, ISO 21448 and ISO TS5083 (as well as others) are attempting to address some of these issues as well.

COMPETING INTERESTS

The author declares they have no potential competing interests.

ORCID IDS

Rami Debouk https://orcid.org/0009-0000-0542-5356

REFERENCES

[1] Bahr, N. J. (1997). System Safety Engineering and Risk Assessment: A Practical Approach. Taylor and Francis.

[2] Debouk, R. (2019). Overview of the 2nd Edition of ISO 26262: Functional Safety - Road Vehicles. Journal of System Safety, 55(1). https://doi.org/10.56094/jss.v55i1.55

[3] Debouk, R., & Joyce, J. (2010). ISO 26262 Hazard and Risk Assessment Methodology. Proceedings of the International System Safety Conference.

[4] Ericson-II, C. A. (2005). Hazard Analysis Techniques for System Safety. New Jersey: John Wiley & Sons. https://doi.org/10.1002/0471739421

[5] IEC 61508. (2010). IEC 61508, Functional Safety of Electrical/Electronic/Programmable Electronic Safety Related Systems Parts 1-7. Switzerland.

[6] ISO 21448. (2022). Road Vehicles - Safety of the Intended Functionality.

[7] ISO 26262. (2018). ISO 26262 2nd Ed. Road Vehicles - Functional Safety Parts 1-12.

[8] Leveson, N. (2001). Safeware: System Safety and Computers. Addison Wesley.

[9] SAE J3016. (2021). Taxonomy and Definitions for Terms Related to Driving Automation Systems for On Road Motor Vehicles.