Whitepaper on ISO 26262
Automotive Functional Safety Standard

Author: Kirthiga L

Corresponding Author: Mohammed Sadiq Hussain

qad@srmtech.com

Abstract

For modern electric and driverless vehicles, the ISO 26262 Automotive Safety Standard provides crucial guidance on the construction of electronic hardware with a tolerable level of risk. The standard and derivative works, on the other hand, are sometimes riddled with jargon, acronyms, and presumed knowledge requirements, making comprehension difficult and time Consume. This article aims to provide a clear, brief overview of the standard's major features for developers, so that they can have a working understanding of the standard's methodological requirements.

1. Introduction

The advancement and prevalence of automated driving in recent years has necessitated the development of standards such as ISO 26262, which defines functional safety as well as features that aid in the prevention of accidents in the event of an emergency. ISO 26262 has been adopted as a recommended national standard (with the prefix 'GB/T') in China, where there is a high level of technical innovation. In October 2017, GB/T 34590, a Chinese translation of ISO 26262, 1st Edition, was released, and it went into effect in May 2018. A growing number of companies are promoting functional safety not only among car manufacturers (OEMs), but also among Tier 1 electronics equipment suppliers, making it a more needed issue.

In light of this, an increasing number of companies are pushing functional safety not only among car manufacturers (OEMs), but also among Tier 1 electronics equipment suppliers, making it a more significant global need. We will discuss these principles from a semiconductor manufacturer's perspective, including how they affect the automotive sector, in this article, as interest in functional safety and ISO 26262 rises and actions and answers are needed.

What is the definition of functional safety?

First, let’s consider the meaning of functional safety.

1.1 The meaning of the word "safe"

Most people would struggle to give an immediate answer if asked what the definition of the word "safe" is. The word ‘safe' is defined as having 'no unacceptable risk' in the first edition of the worldwide basic safety standard ISO/IEC Guide 51 (which is an introductory guideline on safety). This double negative may be difficult to grasp at first, therefore 'freedom from risk that is not tolerable' would be a better alternative. In any event, it's difficult to define ‘safe' in a single sentence, so let's review the term once more.

The opposite of ‘safe’ is ‘dangerous’. So, what is ‘dangerous’? ‘Dangerous’ conditions can be referred to as ones that are ‘at risk’. In general, risk can be large or small. Therefore, by taking measures against large risk that is ‘dangerous’ and reducing it to an acceptable range, this ‘dangerous’ state then becomes a ‘safe’ state. Or to put it another way, a ‘state without an unacceptably large risk’. So now we see that ‘safe=no unacceptable risk’ as mentioned in the beginning.

1.2 Achieving functional safety

To avoid major accidents, the concept of functional safety has arisen. It is vital to design things based on the assumption that people make mistakes and things break. To achieve functional safety, designers must take into account both systematic and random unsuccessful in order to prevent harm from being caused by the object's movement or actions.

Systematic failures, often known as bugs, are failures that occur during the design process. To avoid systemic failures, a design flow that does not induce design flaws must be created. It begins with the establishment of specifications based on needs, and then each step is explained, including design, verification, prototyping, and assessment, with reviews performed at each level. It's also important to keep track of the papers that are created at each stage and be able to refer to and retrieve them at any moment.

Random failures, on the other hand, occur after the product has been manufactured. Because random failures are unavoidable, a safety mechanism must be in place to prevent harm even if they do occur.

2. *ISO 26262 and Related Standards*

Let's have a look at the ISO 26262 functional safety standard now that we've grasped the concept of functional safety. Keep in mind that there are a slew of additional functional safety criteria that aren't specific to the car industry.

2.1 Regarding the major standards

Before we go into detail about ISO 26262, we would like to explain the key standards.

Foremost are international standards (IS) published by ISO, which stands for International Organization for Standardization, is a non-governmental organization headquartered in Geneva, Switzerland. You may have heard of some

of the more well-known standards such as ISO 9001: Quality Management System, and ISO 14001: Environmental Management System.

Next is IATF 16949, a global technical specification and quality management standard for the automotive industry. IATF is short for the International Automotive Task Force. IATF 16949 is designed to be used in conjunction with ISO 9001:2015 and contains supplemental requirements specific to the automotive industry.

IATF 16949 supersedes and replaces the current ISO 26262 standard that defines the requirements of a Quality Management System.

2.2 Where ISO 26262 and other functional safety standards came from

ISO 26262, as previously stated, is a functional safety standard for electrical and electronic systems in road vehicles that is based on IEC 61508, which is regarded the parent standard for functional safety.

The International Electro Technical Commission (IEC) published IEC 61508 as an international standard for the functional safety of Electrical/Electronic/Programmable Electronic Safety-related Systems in all types of industry, including power plants, factories, machinery, railways, medical equipment, and home appliances (International Electro technical Commission). Based on the main concept and structure of IEC 61508 and adapted for car electric/electronic systems, ISO 26262 was created.

In fact, IEC 61508 has spawned a slew of functional safety standards for a variety of sectors. IEC 61511 (Safety Instrumented Systems for the Process Industry Sector), IEC 62061 (Safety of Machinery), IEC 13849 (Safety-Related Parts of Machinery Control Systems), IEC 61800-5-2 (Adjustable Speed Electric Drive Systems), IEC 60335-1 (Household and Similar Electrical Appliances), IEC 61513 (Nuclear Power Plants), IEC 62278 (Railway Applications), ISO 13482 (Electrical Equipment for Furnaces).

At this point, it's important to note that ISO 26262 is not a legal document. As a result, noncompliance with ISO 26262 is not considered unlawful. Automobile manufacturers, on the other hand, will not buy items that do not meet this standard since they must demonstrate that vehicles are safe by building electronic and electrical systems in accordance with ISO 26262. This assures that no one (not only the driver and passengers, but also pedestrians) will be hurt if the electrical/electronic systems fail.

FUNCTIONAL SAFETY STANDARDS							
IEC 61508							
DO 254	ISO 26262	IEC 61511	IEC 62061	IEC 61513 IEC 62138	IEC 62404 ISO 13485	EN 50128
Aerospace Defence	Automotive	Industrial Controls	Machine Tooling	Nuclear Power	Medical Devices	Railway Transport

Hierarchy of Safety Standards

2.3 Compliance with ISO 26262

It is required to respond to both procedures and products in order to comply with ISO 26262. Process response is the reaction to the development flow that summarises the development procedures, etc. Processes relate to a set of inputs, processes, and outputs, whereas process response is the response to the development flow that describes the development procedures, etc. Maintaining internal laws and development standards necessitates the establishment of a development process for papers and evaluations.

At the same time, product response is a response to product functions, so if a failure occurs somewhere in a target product, that failure is detected and some type of safety mechanism is in place that performs some type of processing to avoid danger.

Now let's delve a little deeper into both types of responses.

From the viewpoint of people make mistakes, failures created at the time of design (bugs) are described as systematic failures, and process response is required as a countermeasure to avoid such failures. In order to prevent bugs from being created during the design phase, the necessary documents and reviews must be specified during development, to be kept and used as evidence.

Furthermore, problems that occur in the market (and factory) are described as random failures (or random hardware failures) that necessitate product response as a countermeasure. It is crucial to build with varied margins in mind to avoid damage, but from a functional safety standpoint, it is also necessary to design to prevent injuries even in the event of failure. As a result, designers must implement safety mechanisms to detect problems and respond appropriately. The numerous sorts of failures for each function, as well as their accompanying safety measures, must be considered during the initial requirements review in the design stage. Adding a safety mechanism to account for random failures is part of the product response.

2.4 Product responsibility for designers

Perhaps you have heard of product liability. This means that manufacturers and/or other entities can be held liable in the event a defect in a product causes damages to human life, body, or property. As designers need to prove that there are no design flaws (bugs) in the design of their products by leaving evidence (i.e. their design rationale and design assumptions), dealing with product reliability can be considered a type of process response.

3. *Key Components of ISO 26262*

Each aspect of the automotive product development process, from specification to design, implementation, integration, verification, validation, and production release, includes functional safety elements. The ISO 26262 standard for Automotive Electric/Electronic Systems is an adaption of the Functional Safety standard IEC 61508. ISO 26262 is a functional safety standard for automotive equipment that applies throughout the lifecycle of all electronic and electrical safety systems in automobiles.

The standard intends to address potential dangers in automobiles caused by faulty electronic and electrical equipment. Despite the fact that the standard is labelled "Road vehicles – Functional safety," it applies to the functional safety of electrical and electronic systems as well as systems as a whole or mechanical subsystem.

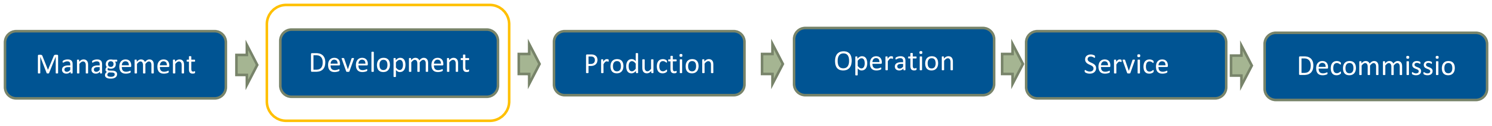
To monitor functional safety and regulate product quality, ISO 26262 employs a series of procedures.

Goals of ISO 26262

- Provides an automobile safety lifecycle (management, development, production, operation, servicing, and decommissioning) and assists in customising the required actions during these phases.
- Specifies the item's necessary safety requirements for obtaining an acceptable residual risk using an automotive-specific risk-based approach (Automotive Safety Integrity Levels, ASILs).
- Specifies validation and confirmation standards to guarantee that an adequate and acceptable degree of safety is attained.

Automotive Safety Lifecycle

Ten volumes make up ISO 26262. It is designed for series production cars, and contains sections specific to automotive. For example, ISO 26262 section 7 specifies the safety criteria for production, operation, servicing, and decommissioning.



The ISO 26262 automotive safety lifecycle includes the full manufacturing process. This includes appointing a safety manager, creating a safety strategy, and defining confirmation measures such as safety review, audit, and assessment. These specifications will be utilised in the development of E/E systems and elements.

4. *Importance of ISO 26262 in Automotive Development*

It was inevitable that functional safety standards would emerge to control the design, development, and deployment of automotive electronic systems as they grew in complexity and moved beyond clocks and radios in automobile development.

The standards were first introduced to the automotive industry by ISO 26262 in 2011, but considerable technology advancements in subsequent years prompted an upgrade in 2018. ISO 26262 first presented those requirements to the automotive sector in 2011, but significant technological improvements in recent years necessitated an upgrade in 2018.

Hardware and software safety risks must be handled and documented throughout the product lifecycle, according to ISO 26262. Though safety design was once considered a part of general requirements, in automobile development, working in isolation between hardware and software teams does not ensure the level of functional safety coverage required by ISO 26262. Many tools do an excellent job of requirements management and traceability during a specific phase, but they don't give a solid auditable trail for phase-to-phase traceability.

ISO 26262 provides a broader, holistic approach by documenting attention throughout the development, decision-making, ad selection process of supporting tools. It aims to bridge the gap between the high-level design phase and the low-level component creation, integration, and testing phases of the lifecycle.

Compliance with ISO 26262 becomes an afterthought and an auditing nightmare when teams aren't equipped with the necessary tools, implementation techniques, and best practises.

Best Practices of ISO 26262

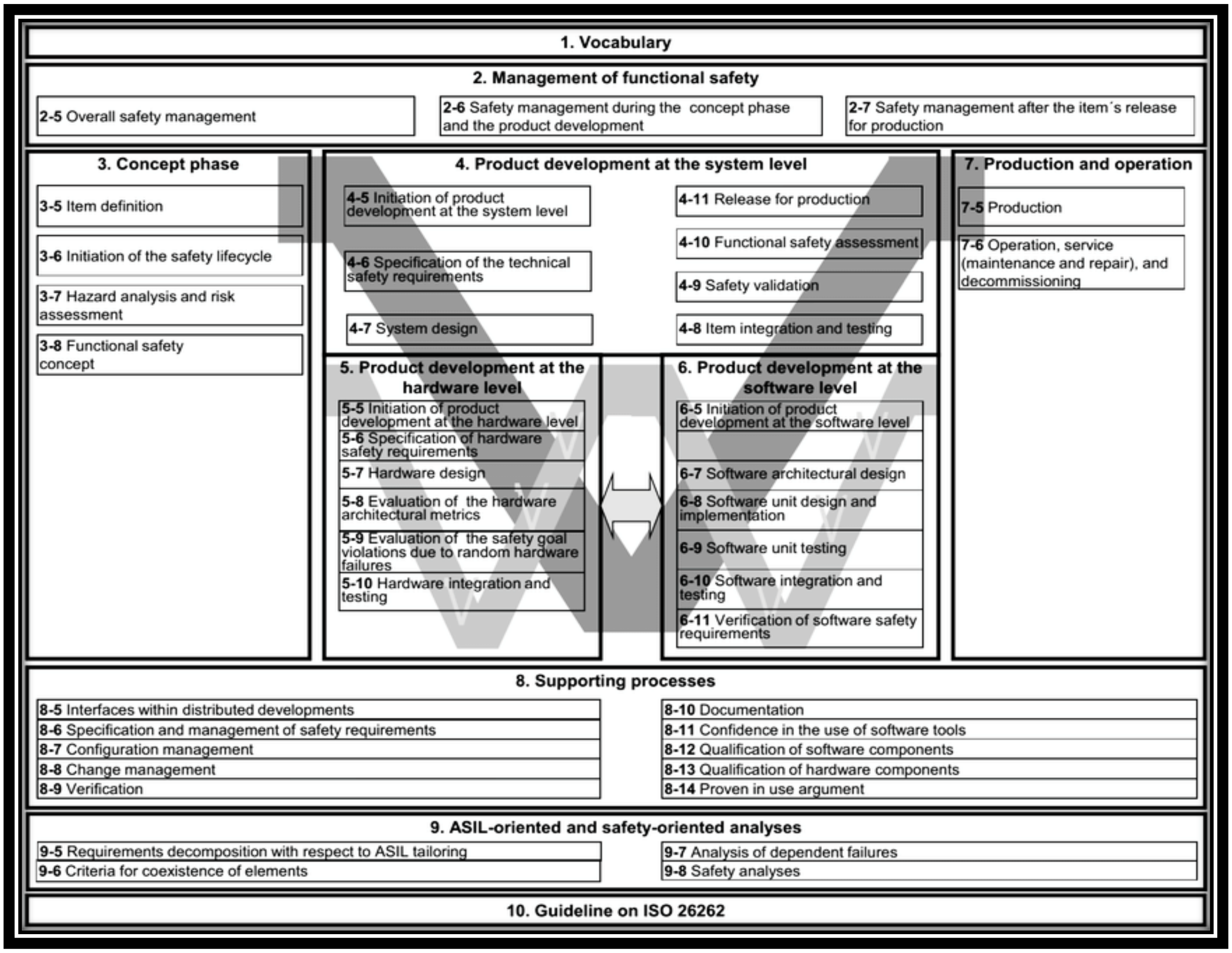
The holistic approach to functional safety highlights multiple fundamental features of excellent systems engineering methods, all of which build on one another. The first stage is collaboration. In collaborative development, ISO 26262 mandates the documentation of formal and informal contacts as well as decision points. However, because the supply chain's team members and worldwide partners are spread around the globe, paperwork must be done with as little disruption as possible.

Clear traceability of requirements, functions, implementations, and tests throughout the lifecycle process helps tool vendors ensure that new versions of a solution won't break existing software or hardware. Traceability also provides a path for verification of requirements and validation of the system. Verification and validation (V&V) makes sure engineers are designing the right thing and building it right. Noncompliant development processes might not have the same level of rigor and consistency required for functional safety.

Risk risks are identified, analysed, and mitigated to achieve functional safety. ISO 26262 teaches teams how to establish a risk level that is acceptable and how to document the complete mitigation procedure. Customers must be convinced that their tools will not cause difficulties, and traceability provides a mechanism to assure that new versions of a tool will not harm current software or hardware.

Benefits of ISO 26262 For an Organization

The ISO 26262 standard was published to help companies ensure functional safety of their electrical and electronic systems. The objective of ISO 26262, which organisations are considering implementing, is to detect and analyse risk early in the product development process. Additionally, they must set safety objectives and implement a thorough validation approach to fulfil these objectives.


1. Vocabulary
2. Management of functional safety
2-5 Overall safety management
2-6 Safety management during the concept phase and the product development
2-7 Safety management after the item´s release for production
3. Concept phase
3-5 Item definition
3-6 Initiation of the safety lifecycle
3-7 Hazard analysis and risk assessment
3-8 Functional safety concept
4. Product development at the system level
4-5 Initiation of product development at the system level
4-6 Specification of the technical safety requirements
4-7 System design
4-11 Release for production
4-10 Functional safety assessment
4-9 Safety validation
4-8 Item integration and testing
5. Product development at the hardware level
5-5 Initiation of product development at the hardware level
5-6 Specification of hardware safety requirements
5-7 Hardware design
5-8 Evaluation of the hardware architectural metrics
5-9 Evaluation of the safety goal violations due to random hardware failures
5-10 Hardware integration and testing
6. Product development at the software level
6-5 Initiation of product development at the software level
6-7 Software architectural design
6-8 Software unit design and implementation
6-9 Software unit testing
6-10 Software integration and testing
6-11 Verification of software safety requirements
7. Production and operation
7-5 Production
7-6 Operation, service (maintenance and repair), and decommissioning
8. Supporting processes
8-5 Interfaces within distributed developments
8-6 Specification and management of safety requirements
8-7 Configuration management
8-8 Change management
8-9 Verification
8-10 Documentation
8-11 Confidence in the use of software tools
8-12 Qualification of software components
8-13 Qualification of hardware components
8-14 Proven in use argument
9. ASIL-oriented and safety-oriented analyses
9-5 Requirements decomposition with respect to ASIL tailoring
9-6 Criteria for coexistence of elements
9-7 Analysis of dependent failures
9-8 Safety analyses
10. Guideline on ISO 26262

5. *Automotive Safety Integrity Level (ASIL)*

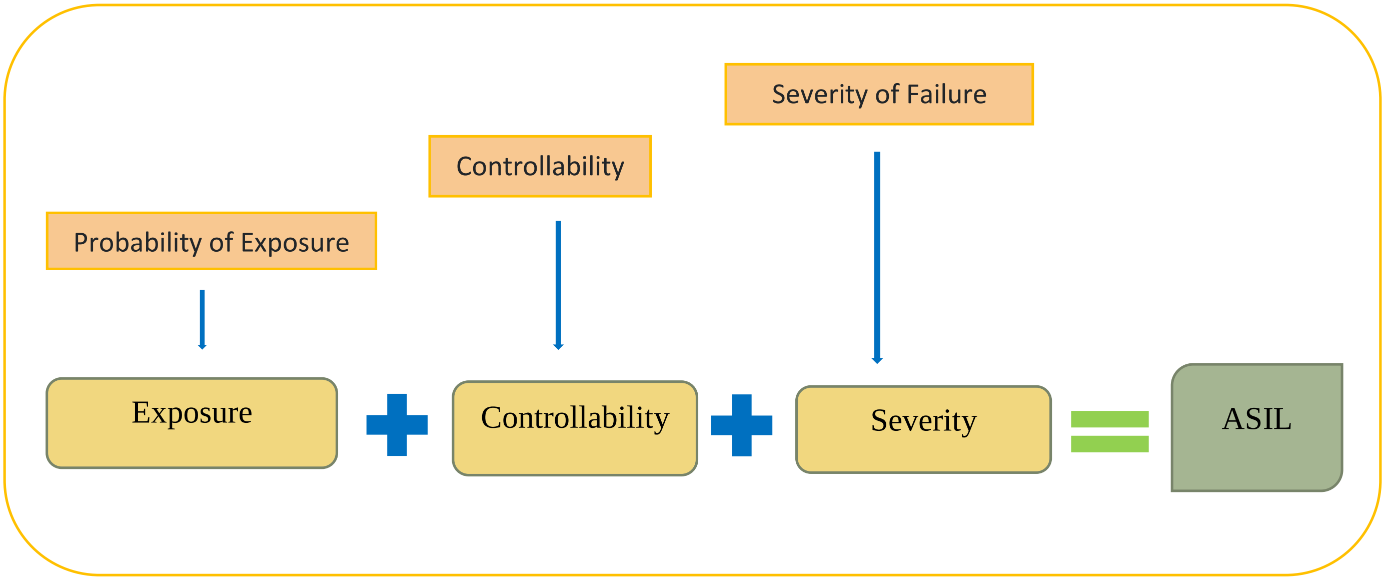
An important part of ISO 26262 compliance is the ASIL. The ASIL is determined at the outset of the development process. The planned functionalities of the system are assessed in terms of potential hazards. "What will happen to the driver and other road users if there is a failure?" the ASIL wonders.

Hazard analysis and risk assessment are performed at the start of the safety life cycle, culminating in an assessment of ASIL for all identified hazardous occurrences and safety goals.

Each hazardous occurrence is assigned a classification based on the severity (S) of injuries it is likely to cause:

Severity Classifications (S):
S0 No Injuries
S1 Light to moderate injuries
S2 Severe to life-threatening (survival probable) injuries
S3 Life-threatening (survival uncertain) to fatal injuries

Risk management understands that the severity of a potential harm is influenced by the likelihood of the injury occurring; that is, a hazardous event is regarded a lower risk for a particular hazard if it is less likely to occur. The possibility of an injurious hazard is further classified according to a combination of exposure (E) (the relative predicted frequency of the operational conditions in which the injury can possibly occur) and control (C) in this standard's hazard analysis and risk assessment method (the relative likelihood that the driver can act to prevent the injury).



The ASIL is calculated using a mix of the probability of exposure, the driver's potential controllability, and the severity of the prospective outcome if a critical incident occurs. The ASIL does not address the system's technologies; instead, it focuses solely on the risk to the driver and other road users.

Electronic Automotive Devices Today

A modern car comprises a variety of technological equipment. Some are evident, such as radar, entertainment, and navigation, while the majority are hidden from the driver but essential to the vehicle's functionality. Advanced computer-based artificial intelligence will be required for the next generation of autonomous cars.

In 2018, a car has between 100 and 300 microcontrollers or processors, 50 or more complicated electronic control units, 5 to 20 million lines of software code, and miles of wire harness to connect them.

All of these electronic devices must be deemed "safe" up to a certain risk threshold. Previously, car manufacturers and systems providers were responsible for guaranteeing safety. The purpose of automobile safety standards is to ensure that the whole automotive value chain prioritises safety. Functional safety is defined as "the absence of unacceptable risk owing to dangers induced by malfunctioning behaviour of electrical/electronic systems" by ISO 26262.

6. *Systematic Failure Management*

Despite the fact that the most of this work is devoted to the topic of random failures, we do include a brief discussion of systemic failure management. Using existing verification and design-for-testing processes and technology, the semiconductor industry is well prepared to address systematic failures. Random Failures are more difficult to deal with and necessitate more attention.

Summary

The purpose of this document is to provide a clear and comprehensive explanation of the essential parts of the ISO 26262 standard for Hardware IC development. By making the paper easy to read and avoiding the jargon that is frequently employed, it is intended that some parts of the standard and automobile safety solutions in general would be demystified. Here it has been given an overview of current automobile challenges as well as the ISO standard that was designed to protect both manufacturers and end-users.

Reference:

1. Microsoft Word - Optima ISO 26262 Primer White Paper 191125.docx (optima-da.com)
2. https://fscdn.rohm.com/en/products/databook/white_paper/iso26262_wp-e.pdf
3. https://www.siliconindia.com/events/siliconindia_events/Softec_Conf_Pune/Shrikant.pdf
4. https://www.embitel.com/wp-content/uploads/ISO-26262-Standard-Handbook.pdf