AUTOMOTIVE BASICS

Just a collective information..

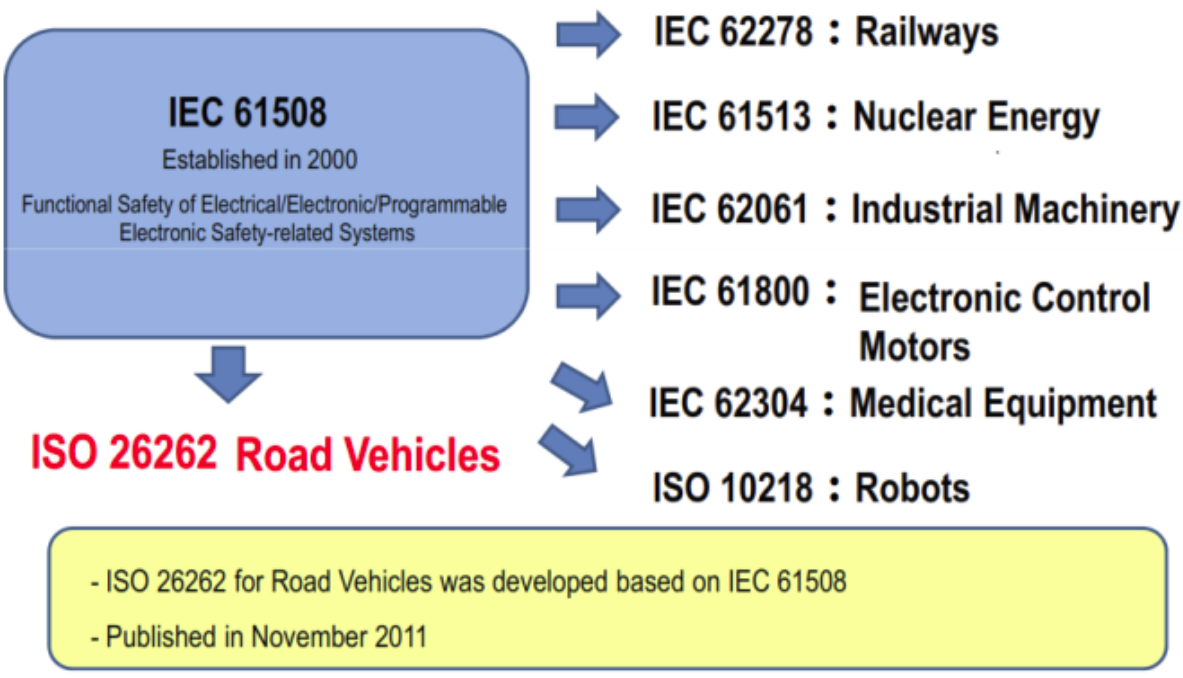
ISO26262

Automotive safety: An ISO 26262 perspective

Benefits of ISO 26262
Implementing ISO 26262 ensures that a high level of safety is built into car components right from the start. The standard can be used to establish a safety management system based on internationally recognized best practices and the latest approach to risk management, giving you a competitive edge. It is expected that car manufacturers will use compliance to ISO 26262 as a means to qualify components and potential suppliers of E/E components.

What is ISO 26262?

ISO 26262 is a multipart standard defining requirements and providing guidelines for achieving functional safety in E/E systems installed in road vehicles. The standard ISO 26262 is considered a best practice framework for achieving functional safety in road vehicles.



Scope of ISO26262

– Hardware/Software such as electric/electronic devices
– Parts or systems that may significantly impact on human lives in case of

malfunction/failure are considered.
– Equipment that consists only of machinery is out of its scope
– The entire Life-Cycle of automotive products
– Motor vehicles up to 3500kg
– The entire Life-Cycle of automotive products

The framework provided by ISO 26262 deals with the functional safety of:

- Products. The standard requires a safety case and a number of confirmation measures to be applied during the product lifecycle
- Processes. The standard requires specific life cycle processes to be implemented within a safety management system driven by a risk-based approach.

Safety has been a key aspect in the automotive industry even from its earliest stages, but the importance with which it is regarded has become far greater in recent times. Currently the biggest compound annual growth rate (CAGR) in automotive electronics revenue can be attributed to safety applications. Increasingly car manufacturers are making safety a key selling point with which to differentiate themselves from their competition. But with a growing amount of electronics content making up a car's bill of materials, there is now a necessity to switch from the long-established best practices approach to well-defined universal guidelines. As a result, industry protagonists have joined forces to develop a standard with far-reaching implications.

The word "safety" is subject to various different interpretations. However, when applied to modern automobile design it can generally be categorized using the following structure:

1. Passive safety: Assuming that an accident is effectively inevitable, the aim of passive safety mechanisms is to minimize the severity of that accident. The passive safety elements found within a vehicle include seatbelts, crumple zones, etc.

2. Active safety: The systems that are concerned with active safety (based on the knowledge of the current state of the vehicle) will aim to avoid accidents altogether in addition to the minimization of its effects if an accident occurs. Seatbelt pre-tensioning, airbag deployment, predictive emergency braking, anti-lock braking systems and traction control are all examples of this.

3. Functional safety: This focuses on ensuring that all of the electrical and electronic systems (such as power supplies, sensors, communication networks, actuators, etc), including (but not limited to) all ;active safety related systems, function correctly. Functional safety is dealt with by the ISO-26262 standard (published in November 2011).

Reference Books:

Structure of ISO 26262:

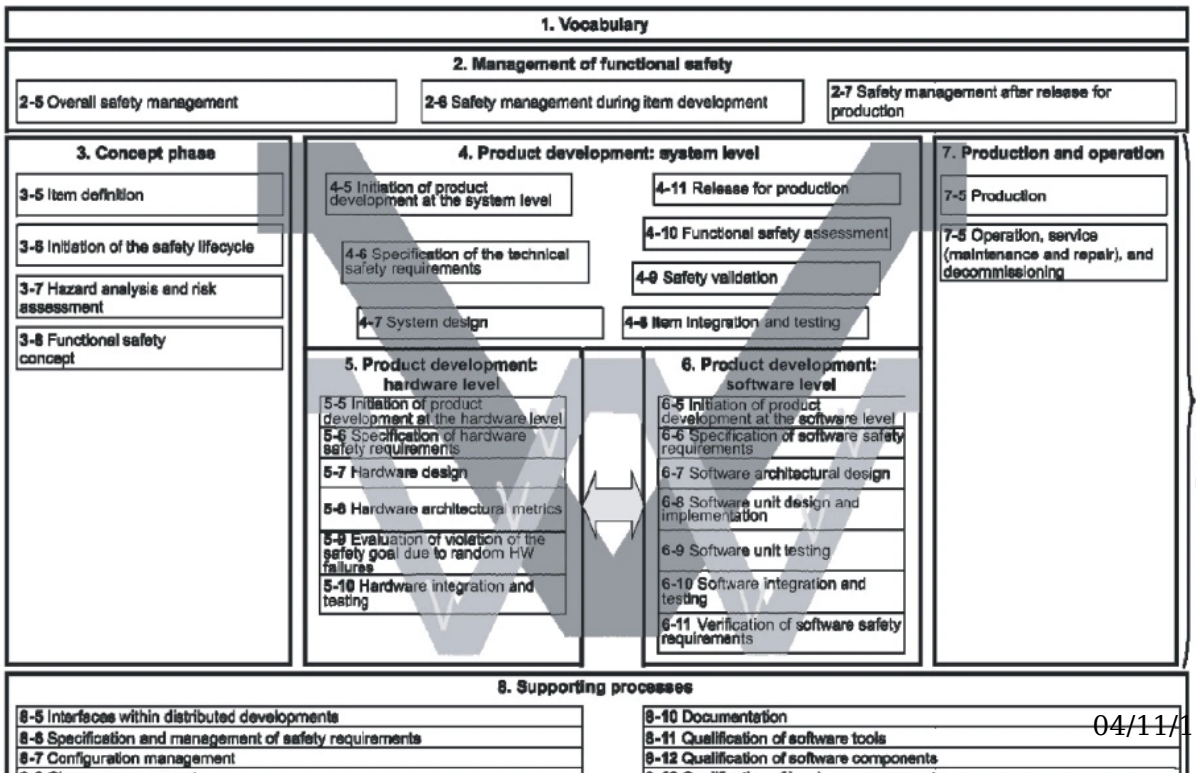
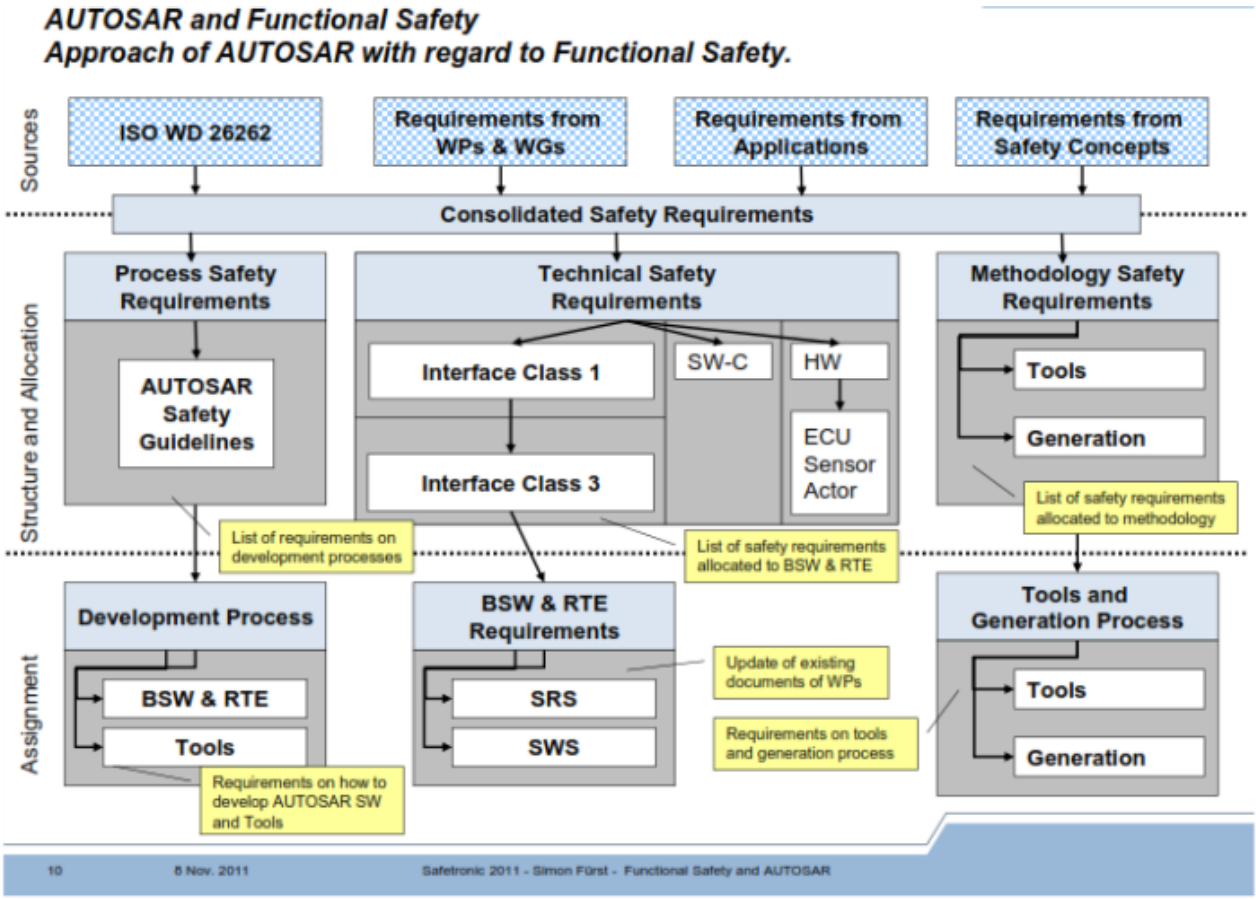


Figure 1 — Overview of ISO 26262

8-8 Change management	8-13 Qualification of hardware components
8-9 Verification	8-14 Proven in use argument
9. ASIL-oriented and safety-oriented analyses	
9-5 Requirements decomposition with respect to ASIL tailoring	9-7 Analysis of dependent failures
9-6 Criteria for coexistence of elements	9-8 Safety analyses
10. Guideline on ISO 26262 (informative)	

It is important to state from the beginning that functional safety does not mean that there is no risk of a malfunction taking place — instead, functional safety implies the absence of unacceptable risk due to hazards caused by malfunctioning behavior of electrical and electronic systems.



ISO 26262 Software Compliance: Achieving Functional Safety in the Automotive Industry

Introduction: Functional Safety In The Automotive Industry

Electronic systems carry out many functions in modern automobiles, including driver

assistance functions, vehicle dynamics control, and active/passive safety systems. The complexity of electronically-driven operations, especially safety functions, makes predicting safety performance extremely difficult. More action will be required, furthermore, to reduce the risks of systematic and random hardware failures as system complexity continues to increase.

ISO 26262 is a functional safety standard intended to be applied to the development of software for electrical and/or electronic (E/E) systems in automobiles. ISO 26262 is an adaptation of the broader IEC 61508 safety standard, which has been used to derive safety standards for the nuclear power, machinery, railway, and other industries. It is aimed at reducing risks associated with software for safety functions to a tolerable level by providing feasible requirements and processes.

About ISO 26262:

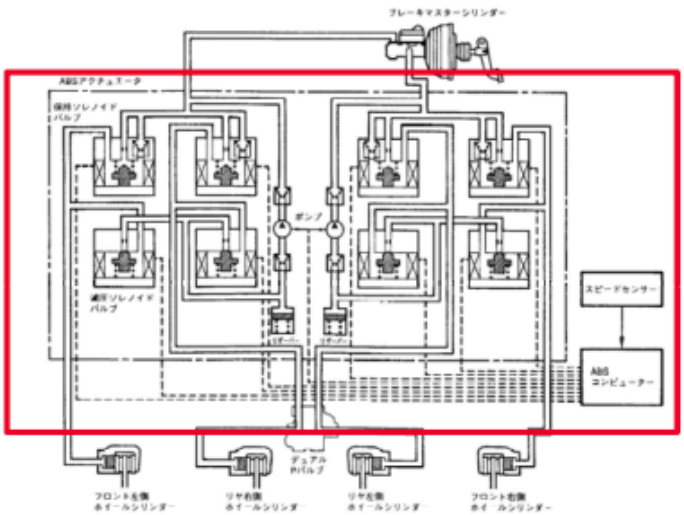
ISO/DIS 26262 is the adaptation of IEC 61508 to comply with needs specific to the application sector of E/E systems within road vehicles. ISO 26262 covers functional safety aspects of the entire development process (including such activities as requirements specification, design, implementation, integration, verification, validation, and configuration). The standard provides guidance on automotive safety lifecycle activities by specifying the following requirements:

- Functional safety management for automotive applications
- The concept phase for automotive applications
- Product development at the system level for automotive applications Software architectural design
- Product development at the hardware level for automotive applications Software unit testing
- Product development at the software level for automotive applications
- Production, operation, service and decommissioning
- Supporting processes: interfaces within distributed developments, safety management requirements, change and configuration management, verification, documentation, use of software tools, qualification of software components, qualification of hardware components, and proven-in-use argument.
- Automotive Safety Integrity Level (ASIL)-oriented and safety-oriented analyses

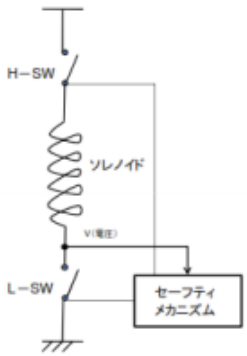
What ISO 26262 Does Not Cover

- Unique E/E systems in special purpose vehicles such as vehicles designed for drivers with disabilities
- Hazards related to electric shock, fire, smoke, heat, radiation, toxicity, flammability, reactivity, corrosion, release of energy and similar hazards, unless directly caused by malfunctioning behavior of E/E safety-related systems
- Nominal performance of E/E systems

Example for Functional Safety:



Structure of ABS



Safety mechanism of actuator

Specific Software Development Sections In ISO 26262

Part 6 of the standard specifically addresses product development at the software level. Requirements for the following development activities are specified:

- Initialization of product development
- Specification of software safety requirements
- Software architectural design
- Unit design and implementation

- Unit testing
- Software integration and testing
- Verification of software safety requirements.

What is functional safety in accordance with ISO26262?

ISO 26262 focuses on the functional safety of electrical and electronic (E/E) systems in vehicles. Functional safety in accordance with ISO 26262 affects all systems containing electrical, electronic, or electromechanical components, i.e. systems from the fields of actuator and sensor technology as well as control electronics. Industrial systems in general are covered by IEC 61508, with additional sector-specific standards applying to railroad technology, aircraft technology, etc. ISO 26262 is the sector-specific extension of IEC 61508 for the automotive industry.

Functional safety is concerned with the absence of unreasonable risk to individuals caused by potential malfunctions in E/E systems. Functional safety is therefore considered a system property. Known active and passive safety systems differ in that active safety is primarily concerned with proactive accident prevention (through the vehicle driver's driving ability, but also electronic systems such as ACC, ABS, ESP, etc.), whereas passive safety relates to the reactive mitigation of the consequences when an accident has already occurred (e.g. safety belts, but also electronic systems such as airbags, belt tensioners, etc.). The electronic systems for active and passive safety must themselves be functionally secure since malfunctions in these systems could also cause personal injury. Functional safety focuses primarily on risks arising from random hardware faults as well as systematic faults in system design, in hardware or software development, or in production, through to the commissioning, repair, and withdrawal of the system.

To this end, ISO 26262 comprises 10 sections with around 750 clauses on approximately 450 pages, which deal with system design, hardware, software, and the associated development processes among other things. The safety lifecycle plays an important role in this regard. The safety lifecycle governs the identification, design, monitoring, and evaluation of the various elements involved in an industry-standard V- model in causal sequence. The term "functional safety" should not be confused with or, worse still, equated to product characteristics such as reliability, availability, and security 1 . Reliability describes the probability of a system performing its assigned function within a particular period of time. Availability describes the percentage of a system's entire service life during which it can be used to perform its assigned function2.

ISO 26262 itself is not a certification standard and therefore contains no clauses regulating certifications or the scope thereof. From the point of view of the standard, there is no requirement to certify systems, components or processes against it; neither is this standard directly relevant for vehicle registration. Experience in implementing ISO 26262 has shown that, for many of those that apply the standard, it is worth obtaining an external assessment as well as certification. The content of these checks are currently being finalized by the competent certifying bodies.

From a legal point of view, ISO 26262 does not bring about any direct change in the legal situation. The provisions of product liability and liability for material defects continue to apply. With regard to other legal aspects such as reversal of the burden of proof, reference is made to the relevant legal publications. In general, professional standards are deemed relevant when assessing the "state of the art," meaning that ISO 26262 is naturally of indirect legal importance.

To take account of the supply structure in the automotive industry, ISO 26262 contains requirements for regulating safety-relevant responsibilities in the case of split-site development. This is the purpose of the Development Interface Agreement (DIA), which covers the explicit detailed agreement between the companies involved at their interfaces. As explained in the following section, it is in no way sufficient for a customer simply to make a general request to his supplier to work in an "ISO 26262- compliant manner" or just to state a particular safety classification. An explicit agreement on a technical level of, in particular, safety objectives, the classification of safety goals, and the safety measures to be implemented, etc. is also essential to ensure the development of a safe product above and beyond supply boundaries.

How is functional safety in accordance with ISO26262 achieved?

The safety lifecycle starts with a definition of the system to be considered at vehicle level ("item"). For the purposes of illustration, let us take the example of an airbag system. The next step is to carry out a hazard analysis and risk assessment for the system to be considered. One potential hazard in an airbag system would be the airbag inflating unintentionally. A corresponding safety goal must now be determined for each hazard. In this example case, one safety goal would be to prevent the airbag from inflating unintentionally. Typically, a large number of safety goals are identified at this point. Each safety goal is then classified either in accordance with QM or in accordance with one of four possible safety classes, which are termed Automotive Safety Integrity Level (ASIL) in the standard, with the four levels being termed ASIL A to ASIL D. The rating "QM" indicates that a standard quality management system, e.g. in accordance with ISO/TS 16949, and the observance of established standards such as Automotive SPICE are sufficient to achieve the corresponding safety goal and that no additional requirements need to be taken from ISO 26262. The next-highest rating "ASIL A" in accordance with ISO 26262 indicates the lowest safety classification, "ASIL D" the highest. The ASIL is determined for each safety goal with the aid of an allocation table contained in the standard. Three parameters are evaluated in each case. These are:

Exposure, i.e. how often the vehicle is in a situation in which the people involved, e.g. driver, passengers or other road users, may be put at risk, Controllability, i.e. how well the individuals involved can handle an infringement of the safety goal, Severity, which quantifies the seriousness of the consequences that may arise from a breach of the safety goal.

The unintentional inflation of the airbag is typically classified as "ASIL D."

Safety goals must be implemented in accordance with the classified ASILs. In other words, suitable processes and methods must be implemented to avoid systematic faults and corresponding additional requirements must be applied to the product to rectify technical faults. This is done initially by defining a functional safety concept. In the example case, this could be a redundancy concept comprising a control channel and an independent monitoring channel. The airbag would only inflate if both channels were in accordance with each other.

The technical aspects are then fleshed out in a technical safety concept. In the example case, a safety architecture could be defined with a sufficient number of independent sensors, with each channel having to enable the trigger circuit independently for the functional safety concept to be realized. The architecture could also include safety measures implemented outside the E/E system (e.g. using mechanical preventive measures). The implementation of such measures does not, however, fall within the scope of ISO 26262. The corresponding standards must be taken into account in this regard.

The hardware safety requirements and software safety requirements are now determined based on the technical safety concept. The following objectives are particularly important: achieving or maintaining sufficient independence in redundant system structures ("dependent failure avoidance"), achieving specific metrics in the evaluation of hardware ("single point fault metric," "latent fault metric") The system integration is followed by the safety validation, the functional safety assessment and the release for production, with the specific requirements of ISO 26262 being based on the relevant ASIL classification of the safety goals.

The scope of the standard also covers production and operation of the system through to its decommissioning in the field. The airbag is a particularly good example of how the unintentional inflation of the airbag must be avoided even at the end of a product's lifecycle.

Need for internal expertise

- Functional safety is a complex topic
- Functional safety standards are difficult to master

Further challenges

- ISO26262 can lead to multiple interpretations
- Many companies/consultants were (and still are) very much IEC61508 focused
- But automotive has different constraints to consider
- Often concept of safety, availability and reliability are mixed up – "It must always work. Then needs to comply to ISO26262!"
- ISO26262 terminology is still often read with IEC61508 "eyes" leading to many misunderstanding.

Example – IEC61508: Item is an element of the final Control System –ISO26262: Item is the final system at vehicle level

Based on the functional safety concept,the technical safety concepts are derived.
– The technical safety requirements are mapped to system elements which are hardware or software based.

- **If a system component fails:**

1. means need to be specified which will detect the failure (self control) and
2. a reaction needs to be present which wil ltransition the system into a safe state.
3. After hardware and software development,there is hardware and software integration, followed by system integration and vehicle integration.

- **Item integration:**

1. Experimentaltesting (time and costintensive)
2. Reconfiguration of HW and SW
3. Timing behavior(Analytics)
4. Independence and Interference

Please refer the following documents for autosar safety information:

1. AUTOSAR_Methodology

2.AUTOSAR and functional safety

3. FUNCTIONAL_SAFETY

[youtube http://www.youtube.com/watch?v=fSlmGib0oRM]

6 thoughts on “ISO26262”

1. **Jyoti**

   says:
   July 6, 2017 at 9:47 am
   Great information 🙂

2. **$ushil**

   says:
   October 15, 2017 at 4:52 pm
   Thanks for detail info along with examples.

3. **Neil Valero**

   says:
   November 23, 2017 at 7:35 am
   Thanks Mr. Nuyts for sharing this link , very informative for a beginner like me.

4. **Naveen Yashwanth**

   says:
   November 30, 2017 at 3:17 am
   Thanks for the info

5. **Prakash**

   says:
   December 15, 2017 at 8:58 am
   What is the role ASIL (A, B , C , D) in Secure storage & secure boot for Embedded systems . Are there any standards/guidelines defined

6. **shreya bhave**

says:
February 1, 2018 at 7:25 am
very useful compilation of information.

BLOG AT WORDPRESS.COM.

UP ↑