spyrosoft

Guidebook to ISO 26262

Table of contents

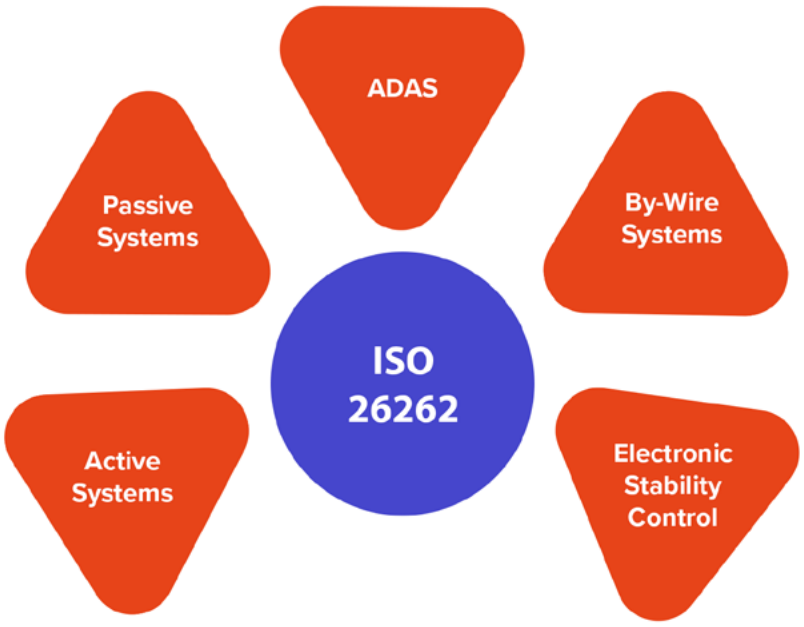
For more information on our Functional Safety (ISO 26262) competencies, visit our automotive training page.

The application of the appropriate standards, rules and best practices is essential from the perspective of any experienced manufacturer or supplier on the market. The story doesn’t differ in the automotive environment. This well developed and crucial industry branch cannot work effectively without the unification and the process support defined in the standards. Nowadays, it is obvious, but it was not always like that.

Currently, there are a few vital organisations that provide international industry standards. Some examples of these types of institutions include Internal Organisation of Standardisation (ISO) and International Electrotechnical Commission (IEC). ISO standards are developed by groups of experts from all over the world,and are part of larger groups called technical committees. These experts negotiate all aspects of the standard, including its scope, key definitions and content. These non-governmental institutions are doing their job in almost every area of human life. Since 1946, they approved about 20 000 standards.

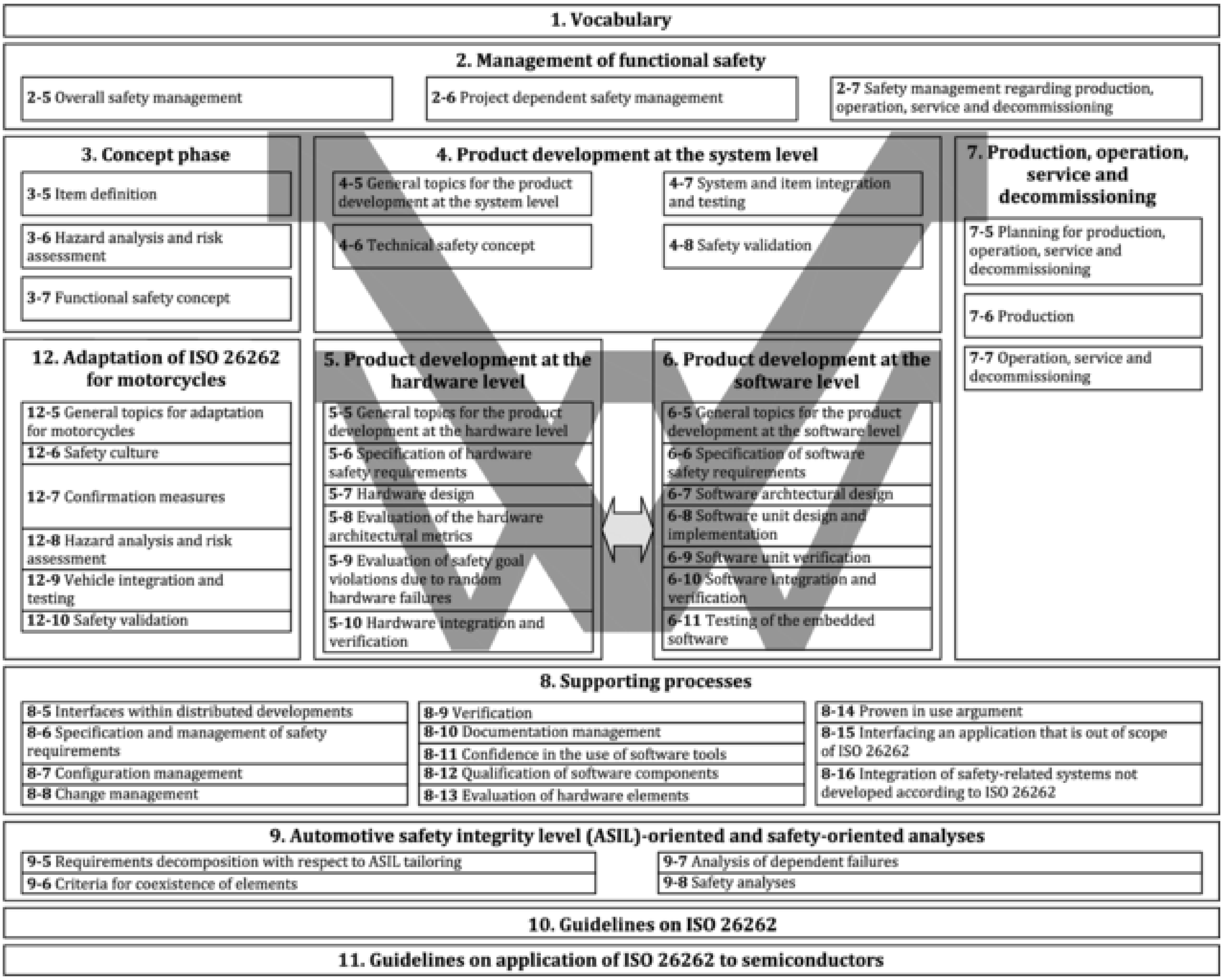
What is ISO 26262 01

"Road vehicles – Functional Safety" is the official title of the ISO 26262 standard. It is the international standard for functional safety of electrical and electronic systems in serial production road vehicles. The basics were derived from IEC 61508, which is often recognised as a master functional safety standard. IEC 61508 can be applied in various industries and it is related to any electronic or electrical system. From that point of view, ISO 26262 is an adaptation of the IEC 61508 for automotive needs.



The ISO 26262 maintains support for the whole product safety lifecycle, including management, development, production and service. During the development process, functional safety covers every safety related aspect of the product on a very detailed level, including such activities as requirements specification, design, implementation, integration, verification, validation, configuration, production, services, operation and decommissioning. The above-mentioned standard also describes the framework for functional safety to assist the development of the safety-related system.

The goal is to achieve acceptable residual risk. E/E System Safety Goals are derived from Hazard and Risk Assessment (HARA) and then the ASIL (Automotive Safety Integrity Level) can be defined. ASIL from A to D means that in the system there is some level of non-acceptable risk which means there are particular FUSA efforts needed to raise the controllability of unwanted situations. - an Automotive Safety Integrity Level (ASIL). Based on that series of activities, it could then be tailored to a particular application.



1. Vocabulary

2. Management of functional safety

- **2-5** Overall safety management
- **2-6** Project dependent safety management
- **2-7** Safety management regarding production, operation, service and decommissioning

3. Concept phase

- **3-5** Item definition
- **3-6** Hazard analysis and risk assessment
- **3-7** Functional safety concept

4. Product development at the system level

- **4-5** General topics for the product development at the system level
- **4-6** Technical safety concept
- **4-7** System and item integration and testing
- **4-8** Safety validation

7. Production, operation, service and decommissioning

- **7-5** Planning for production, operation, service and decommissioning
- **7-6** Production
- **7-7** Operation, service and decommissioning

12. Adaptation of ISO 26262 for motorcycles

- **12-5** General topics for adaptation for motorcycles
- **12-6** Safety culture
- **12-7** Confirmation measures
- **12-8** Hazard analysis and risk assessment
- **12-9** Vehicle integration and testing
- **12-10** Safety validation

5. Product development at the hardware level

- **5-5** General topics for the 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 safety goal violations due to random hardware failures
- **5-10** Hardware integration and verification

6. Product development at the software level

- **6-5** General topics for the product development at the software level
- **6-6** Specification of software safety requirements
- **6-7** Software archtectural design
- **6-8** Software unit design and implementation
- **6-9** Software unit verification
- **6-10** Software integration and verification
- **6-11** Testing of the embedded software

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 management
- **8-11** Confidence in the use of software tools
- **8-12** Qualification of software components
- **8-13** Evaluation of hardware elements
- **8-14** Proven in use argument
- **8-15** Interfacing an application that is out of scope of ISO 26262
- **8-16** Integration of safety-related systems not developed according to ISO 26262

9. Automotive safety integrity level (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. Guidelines on ISO 26262

11. Guidelines on application of ISO 26262 to semiconductors

Source: ISO 26262-1:2011(en) https://www.iso.org/obp/ui/#iso:std:iso:26262:-1:ed-1:v1:en:term:1.120

The history of ISO 26262 02

The origins of the safety design date back to the 1960s, when for example, the product failure rate, reliability, dependability and availability were considered, but in those days, there was still a long way to go before the first functional safety standard in the automotive environment was created. It does not mean there weren't any safety features in cars before then. Despite mechanical improvements like safety belts which where mounted in the series car since 1958, the electronic/electrical features were also added long before the appearance of ISO 26262 . For example, Anti–lock braking systems (ABS) currently mandatory in the EU was released in late 1960s. It was the same story with the Electronic steering control (ESC), which was first introduced to the market in the 1980s.

The first draft of the ISO 26262 arrived in 2008, but the official release was in 2011. That version of the standard includes ten parts and was limited to electric or electronic devices in series production vehicles with a maximum gross weight of 3500 kg. The second and latest version of the ISO 26262 is from 2018. Two new chapters had been added to the standard. One of them was concerning semiconductors, the other describes adaptation for motorcycles.

Even though ISO 26262 is treated very seriously by mature producers it is not mandatory. Widespread compliance shows therefore that it is viewed as an essential standard. This is just half of the story. OEM's are aware that compliance with this standard is essential and will insist that their own suppliers adhere to it. Following the rules and best practice defined by ISO 26262 makes the development and production process more effective and structured. Based on Quality Assurance there are still gaps in the safety product related to design. and production, so the answer in that case is the ISO 26262. It introduces more effort and restriction in the workflow, but as a result, you receive well organised processes, and weak points will be identified and addressed. This lead to a safe, high quality product.

12 parts of ISO 26262 and how they help manufacturers comply with Functional Safety 03

As was mentioned before, ISO 26262 contains twelve separate parts. Each of them refers to a different level of the product lifecycle. Ten parts are normative and the remaining, are guidelines. All the parts constitute one combined form and furthermore it is common that one part refers to another.

01. VOCABULARY

The title speaks for itself. The role of the first part is to specify vocabulary, definitions, and abbreviations. It is crucial to be on the same page and in terms of definitions, understand each other. A brilliant example is an explanation of these words:

Fault - Abnormal condition that can cause an element or an item to fail.

Error - Discrepancy between a computed, observed, or measured value or condition, and the true, specified or theoretically correct value or condition.

Failure - Termination of an intended behavior of an element or an item due to a fault manifestation.

02. MANAGEMENT OF FUNCTIONAL SAFETY

This section describes the appropriate functional safety management methodology for automotive applications, including overall safety management and project-specific information related to management activities during the safety lifecycle's various phases.

03. CONCEPT PHASE

The third part is applied during the early phase of product development. The third part is applied during the early phase of product development. This section requires you to perform a Hazard and Risk Assessment (HARA) based on Item Definition. Later on, Functional Safety Requirements will be defined then all of Functional Safety Requirements will be given to the System Team. meeting the definition of the item. This section requires you to perform Hazard Analysis and Risk Assessment (HARA), so from this point onwards, the Safety Goals in the project should be defined.

04. PRODUCT DEVELOPMENT AT THE SYSTEM LEVEL

This section covers a range of issues from development on the system level. On the stage are specifications that need to be initiated for technical safety, such as the technical safety concept, system architectural design, item integration and testing.

05. PRODUCT DEVELOPMENT AT THE HARDWARE LEVEL

Part five defines requirements for product development on the hardware level. It includes basic topics like hardware design, or evaluation of architectural hardware metrics. In the range of that section, it is also required to evaluate safety goal violation due to random failures.

06. PRODUCT DEVELOPMENT AT THE SOFTWARE LEVEL

This section addresses a range of topics concerned with product development on the software level. This includes specifications for software safety, software architectural design, software unit design and verification, software integration and testing embedded software. At this stage qualitative analyses, like Failure Tree Analysis (FTA) and Failure Mode and Effect Analysis (FMEA) are often used.

07. PRODUCTION, OPERATION, SERVICE AND DECOMMISSIONING

The objective of this part is to develop and maintain a production process for safety related elements or items that are intended to be installed in road vehicles, as well as gather information about operations, services and decommissioning for users which interface with safety-related items.

08. SUPPORTING PROCESSES

The goal of this part is to integrate the whole process and support Safety Life Cycle. It is continuously active throughout all phases. Part eight describes among others how to correctly proceed to verification, how to perform tool qualification, or how introduce proven in-use arguments.

09. AUTOMOTIVE SAFETY INTEGRITY LEVEL (ASIL)-ORIENTED AND SAFETY-ORIENTED ANALYSES

In specifying Automotive Safety Integrity Level (ASIL)-oriented and safety-oriented analyses, this part covers decomposition with respect to ASIL tailoring, criteria for coexistence of elements, analysis of dependent failures, and safety analyses.

10. GUIDELINES ON ISO 26262

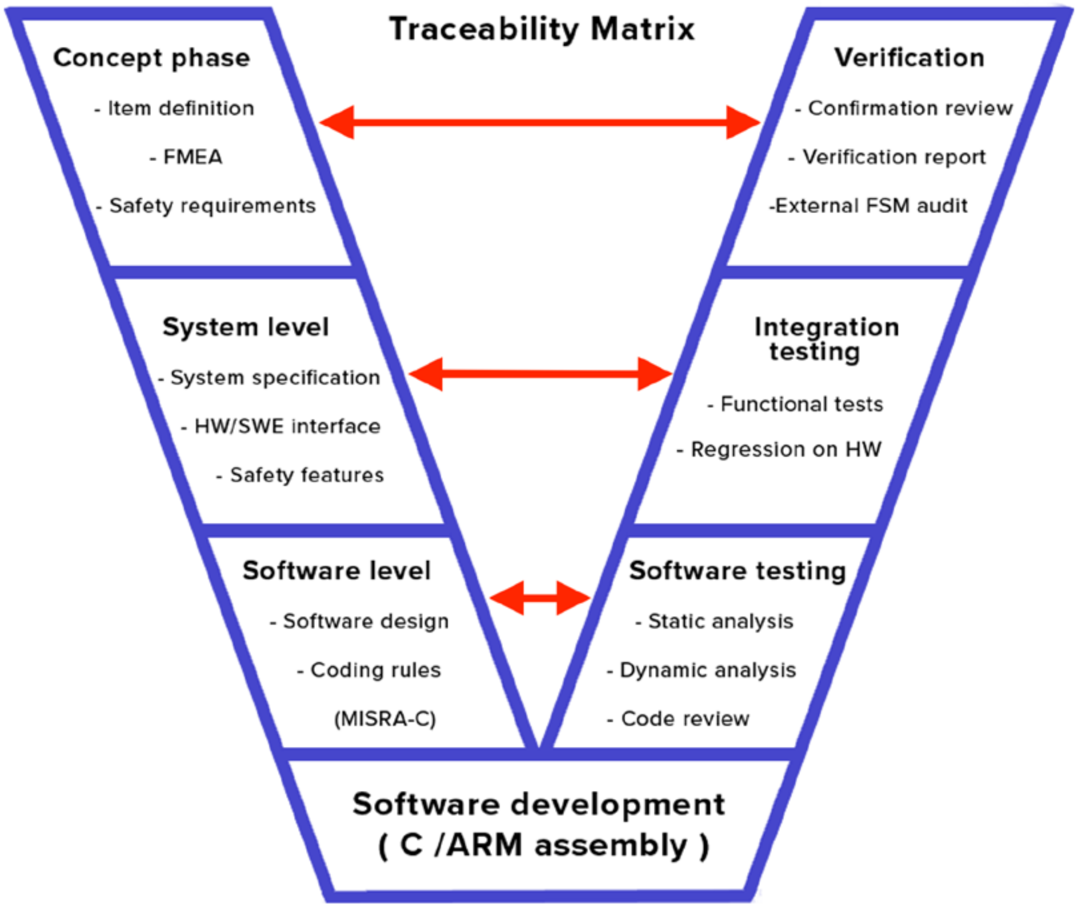
This is one of two informative ISO 26262 parts which provides an overview and extends information by adding additional explanations. The objective of this part is to improve the understanding of other parts and the general concept of the ISO 26262

11. GUIDELINES ON APPLYING THE STANDARD TO SEMICONDUCTORS

Part 11 was added in the second release of the standard. It provides detailed information to support semiconductor manufacturers and silicon intellectual property (IP). Its goal is to address how IP suppliers and integrators should work together.

12. ADAPTATION OF ISO 26262 TO MOTORCYCLES

The objective of this clause is to give an overview of the adaptation of the ISO 26262 series of standards for motorcycles. It covers general topics for the adaptation of motorcycles, safety culture, confirmation measures, hazard analysis and risk assessment, vehicle integration and testing, and safety validation.



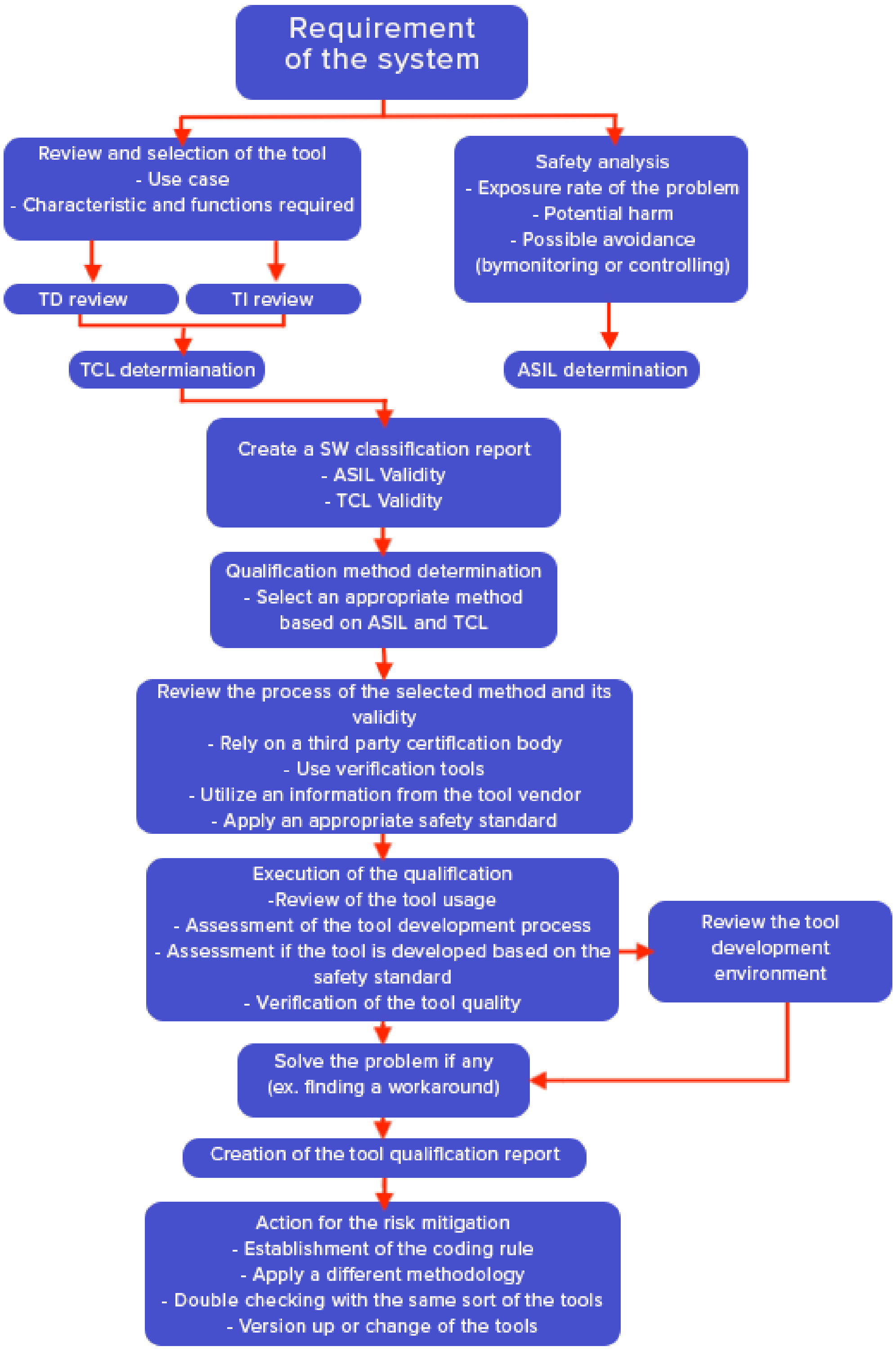
Criticism of ISO 26262 (mentioning SOTIF) 04

Despite the significant improvement to the electronic and electrical environment in the second release of the ISO 26262, there are still some gaps in the functional safety field. Places where the standard falls short are for example missuses, or automated driving. The solution is ISO PAS 21448 (SOTIF). Previously there was a plan to include that standard in ISO 26262 as a fourteenth section, but it was released as a separate document.

The purpose of SOTIF is to start to address some of the aspects of autonomous driving, where safety is not violated by the failure itself but by the unspecified behavior of the vehicle. SOTIF is taking a more holistic look on the usage of the product. Bright lights, dust, smoke and snowstorms all affect the sensor data, and the “brain” of the car is processing and making decisions based on probability.

ISO 26262 Tool Qualification 05

The tool qualification is a one of the activities deemed essential for compliance with ISO 26262. In general, the purpose is to ensure that all tools used in the project are reliable, or malfunctions are known, and any issues that arise can be handled. It is important to take into consideration all tools used even those indirectly involved in the development process.


Requirement of the system
Review and selection of the tool - Use case - Characteristic and functions required
Safety analysis - Exposure rate of the problem - Potential harm - Possible avoidance (bymonitoring or controlling)
TD review
TI review
TCL determianation
ASIL determination
Create a SW classification report - ASIL Validity - TCL Validity
Qualification method determination - Select an appropriate method based on ASIL and TCL
Review the process of the selected method and its validity - Rely on a third party certification body - Use verification tools - Utilize an information from the tool vendor - Apply an appropriate safety standard
Execution of the qualification -Review of the tool usage - Assessment of the tool development process - Assessment if the tool is developed based on the safety standard - Verification of the tool quality
Review the tool development environment
Solve the problem if any (ex. finding a workaround)
Creation of the tool qualification report
Action for the risk mitigation - Establishment of the coding rule - Apply a different methodology - Double checking with the same sort of the tools - Version up or change of the tools

Over to you 06

The tool qualification is a one of the activities deemed essential for compliance with ISO 26262. In general, the purpose is to ensure that all tools used in the project are reliable, or malfunctions are known, and any issues that arise can be handled. It is important to take into consideration all tools used even those indirectly involved in the development process.

Book a Free Consultation

Let's talk about how our experts can help your team build automotive skills. Free and without obligation.

Adam Pietraszek

DIRECTOR OF AUTOMOTIVE

tel: +48 728 869 155

email: apietraszek@spyro-soft.com

Automotive risk management and safety requirements call for complex solutions and deep-rooted knowledge of how they work. We offer Functional Safety ISO26262 training for any role and at any level.

FuSa Awareness Training	The training includes an overview of safety standards; ISO26262 basic definitions, terminology, and concepts. Mandatory for each project member. (Prerequisite for in-depth roles training).	regular / online	2.5h
FuSa SW Requirements Training	How-to on managing requirements in safety-rated projects. It also includes modules on what are safety requirements and how to handle them. Safety Requirements traceability; verification; relation to safety analysis; exercises.	regular / online	3h
FuSa SW Architecture Training	The training includes analysing safety concept impact on SW architecture, as well as key Safety Architecture concepts; verification; tooling; best practices. There's also a module on how to justify SW architecture implements safety, exercises.	regular / online	3h

FuSa SW Dev & Devops Training

The core of this training is the module on what makes your code safety-rated. We will also teach your team the SW Unit Design principles, SW Unit Verification methods and we will go through course exercises together.

regular / online

4h

FuSa Testing Training

How-to on executing testing processes to be compliant with ISO26262 and what criteria must be met to test ASIL rated components. Testing prerequisities; test environment; main goals and strategies; Integration and Verification methods required by ISO26262; exercises.

regular / online

4h

FuSa for Management Training

The topics of this training include: what is the role of management in the ISO26262 process? How the implementation of ISO26262 can impact your organisation? Is it possible to combine ISO and ASPICE? How much effort more must be added to a "typical" non-ASIL project to make it ISO26262 rated? There are also modules on FuSa vs. ASPICE, FuSa in projects, FuSa early adoption advantages, Non-FuSa product development risks, and successful FuSa implementation.

regular / online

2h

Fusa Concept/System Training

There are modules on functional safety concept, system architectural design, technical safety concept, system and integration testing and safety validation, plus exercises.

regular / online

7h

FuSa HW Training

The modules include how-to on preparing hardware compliant with ISO26262, how-to on making sure that hardware and software are complementary to achieve project safety goals. HW Development Lifecycle; HW requirements; HW Architecture and Design; HW Analysis; Hardware Testing; exercises.

regular / online

7h

spyrosoft