ISO 26262

01 WHAT IS ISO 26262?

An increasing number of today's electrical/electronic (E/E) systems are now significantly relevant to safety certifications. Such systems can include steering, brakes, engine management or light controls. A malfunction of the underlying hardware or software can put lives at risk.
The safety standard ISO 26262 takes risk as the starting point for defining safety measures in order to avoid or control systematic failures. It also aims to detect or control random hardware failures or mitigate their effects.
ISO 26262 defines functional safety throughout the life-cycle of all automotive E/E safety-related systems. It addresses all development phases along the V-model: from specification to design, implementation, integration, verification, validation, and production.

More and more OEMs require ISO 26262 compliance from their suppliers. Thus the standard continues to get a wider distribution and meanwhile defines the "state-of-the-art". This is important since nothing less would be accepted in a liability case.
This poster introduces ISO 26262, the underlying ideas that shape the standard and how it is used. It focuses on the software related aspects of ISO 26262.

Who is this poster for? The intended audience is anybody who is familiar with the basics of software development (like the V-model) and who seeks a comprehensive introduction to ISO 26262.

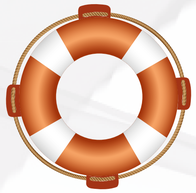
02 STRUCTURE OF THE STANDARD

The ISO 26262:2011 [2] standard consists of 9 parts and a guideline:

Part 1: Vocabulary
Part 2: Management of functional safety
Part 3: Concept phase
Part 4: Product development at the system level
Part 5: Product development at the hardware level
Part 6: Product development at the software level
Part 7: Production and operation
Part 8: Supporting processes
Part 9: Automotive Safety Integrity Level (ASIL)-oriented and safety-oriented analysis
Part 10: Guidelines on ISO 26262

A certification according to ISO 26262 does not necessarily require all parts of the standard to be fully considered.

For example: the T1-TARGET-SW (see section 4) was essentially certified according to parts 6 and 8.
The upcoming version of the standard is expected to add two more parts: part 11: guidelines for semiconductors and part 12 for motorcycles.



03 ITEMS, SYTEMS, ETC.

The figure below shows the different development levels where ISO 26262 applies. The figure also helps to clarify the terms "unit", "part", "component", "system", "element", "function" and "item", giving examples.

Item level Each item represents a certain safety relevant function at the vehicle level and is associated with all the systems and sub-systems through which this function is implemented. ISO 26262 is applied to an item.

Functional level Each function represents a particular functionality in the vehicle and is designed and developed in the vehicle's context.

System level Systems are usually an ECU with internal and/or external sensors and actuators. A system may include sub-systems. Complex ("intelligent") sensors or actuators can be individual systems.

Component level A component is comprised of more than one hardware part or of one or more software units at the atomic level.

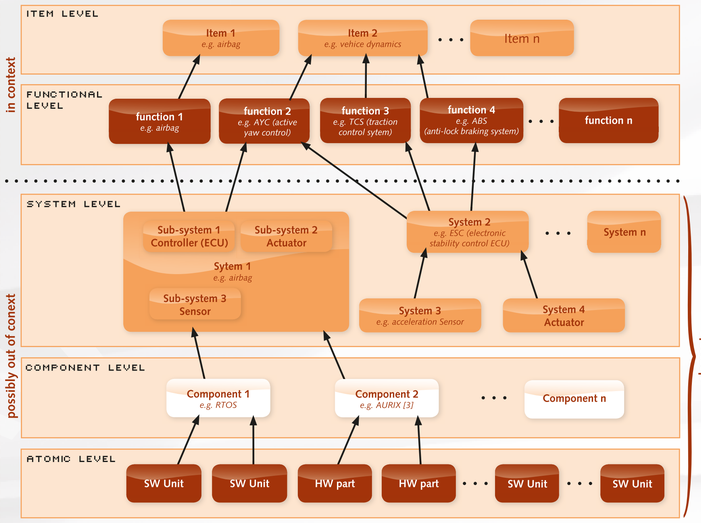
Atomic level Elements at the atomic level represent hardware parts or software units that are subject to stand-alone testing.

3.1 IN CONTEXT/OUT OF CONTEXT

The usage of the term **in context** expresses that an element is related to or embedded into its final environment (typically the vehicle). In contrast, the term **out of context** indicates that something is created independently of a certain vehicle. For example microcontrollers, operating systems, etc.

3.2 AN EXAMPLE: ELECTRONIC STABILITY CONTROL (ESC) ECU

The ESC ECU shown uses the acceleration data provided by the airbag ECU, therefore the airbag ECU with all its subsystems and components which might have an impact on the acceleration data are related to the item "vehicle dynamics" by implication.



04 T1 CERTIFICATION: TOOLING AND VERIFICATION

T1 is a timing analysis and stack analysis suite by GLIWA embedded systems. In June 2016, GLIWA embedded systems received ISO 26262 ASIL-D certification for the embedded software component of T1, known as the T1-TARGET-SW. The figure below shows how the tests required for certification are integrated into a regression test environment.

4.1 TEST EXECUTION

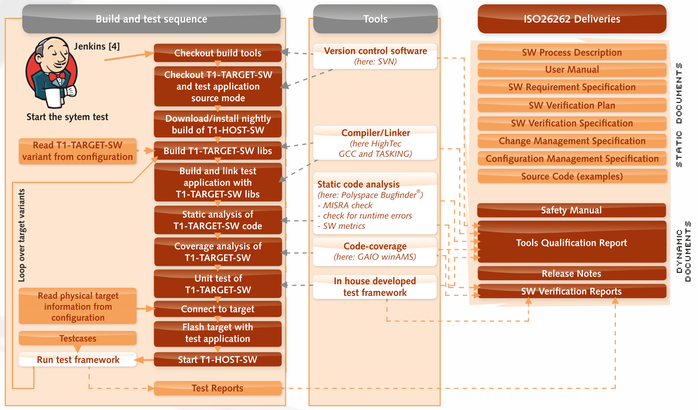
The testing regimen for T1 consists of end to end functional and non-functional testing and unit-testing the T1-TARGET-SW on a test server alongside a variety of embedded targets.

4.2 CERTIFICATION DELIVERIES

The set of deliverables for ISO26262 certification consists of a set of specifications and a set of reports which are subject to frequent updates. These cannot be released prior to an official release of the T1-TARGET-SW. The tests are considered "passed" when the criteria defined in the software verification plan are met.

4.3 TOOL QUALIFICATION

The tools to develop and test the T1-TARGET-SW are subject to a so-called "tool qualification". Tool qualification must be completed regardless of the origin of the tool, be it open source software, "common off the shelf" (COTS) software or a tool developed in-house. The process of tool qualification ensures that any tool malfunctions have been determined and their effect and detectability have been assessed. Measures must be taken to avoid or mitigate potential risks accordingly based on the intended ASIL level of the certification.



05 ASIL (AUTOMOTIVE SAFETY INTEGRITY LEVEL)

Automotive Safety Integrity Level is one of four levels ranging from A, the least stringent, to D, the most stringent level. Below level A lies the QM level which indicates that there is no need to apply ISO 26262.

5.1 ASIL DETERMINATION

The item or element's ASIL is **determined** by assessing its potential safety risks. An ASIL level is determined based on the severity, probability, detectability and ability to control a potentially hazardous event.
For example: ASIL D is assigned to an item if the following conditions are met:

- **Severity Level S3**: Life-threatening injuries (survival uncertain), fatal injuries.
- **Exposure Level E4**: High probability.
- **Controllability Level C3**: Diffcult to control or uncontrollable.

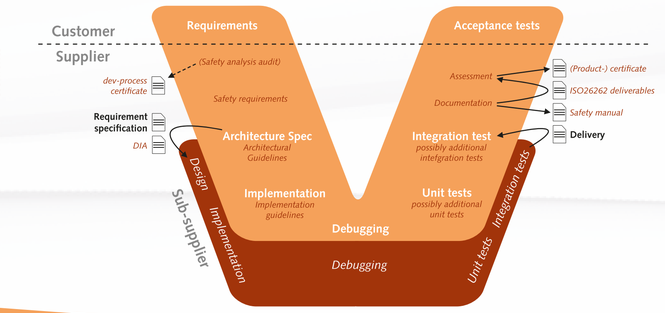
5.2 ASIL DECOMPOSITION

The mechanism of **ASIL decomposition** allows the combination of architecturally independent safety elements with a lower ASIL to meet a safety requirement with a higher ASIL (typically by implementing redundancy).
For example: The developer of an MCU can achieve ASIL D for timer reliability by providing several independent timers each at ASIL B.

06 ISO 26262 STEPS ALONG THE V-MODEL

What are the additionally required actions and documents when certifying software according to ISO 26262?
The answer depends on what type of certification is required (product, COTS, SEooC, etc.) and also on the current state of the development process and all related documentation. However, the figure below gives an idea of what to add to an existing development process based on the standard V-model.

Some components are developed by a sub-supplier as shown by the dark red V in the figure below. Additional actions and documents required by ISO 26262 are indicated in light red. Completing a safety analysis audit is optional but strongly recommended, as it captures the state of the development process and can aid in discovering missing documentation or processes.



07 DISTRIBUTED DEVELOPMENT

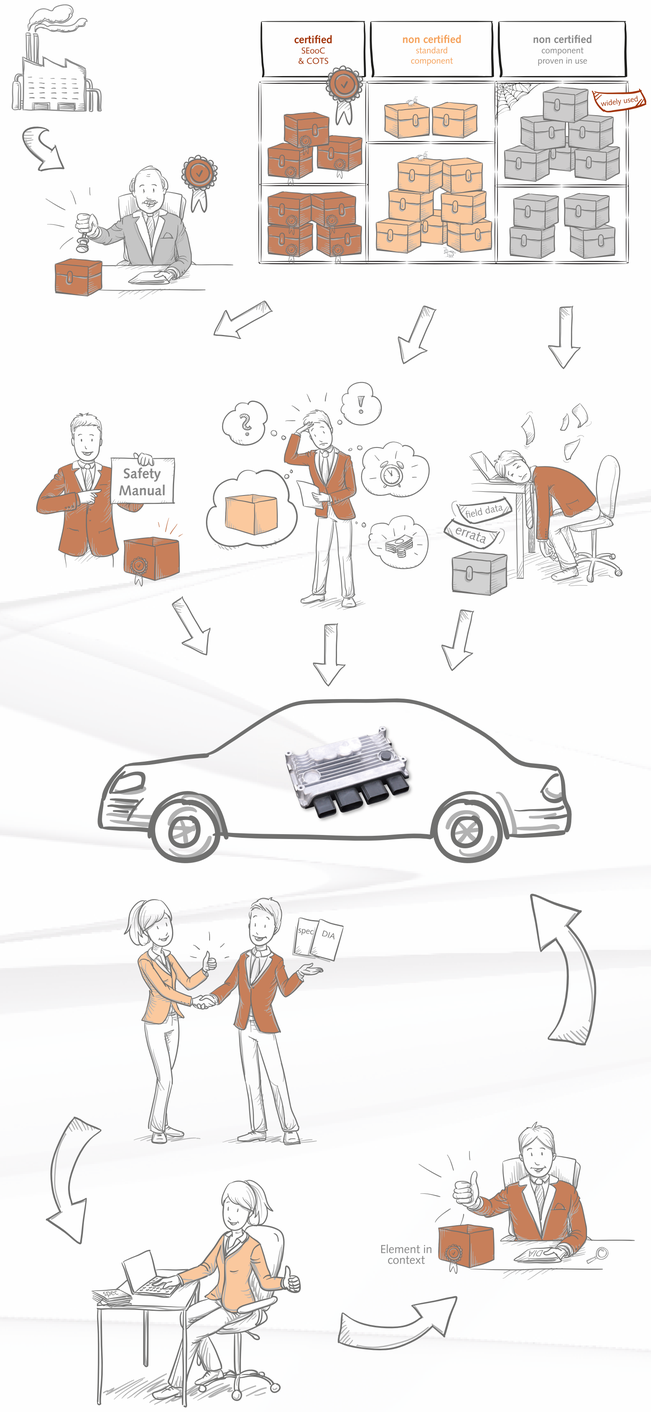
The figure below illustrates the shared development of software for a safety relevant ECU. Several components are used and part of the development is out-sourced:

Certified SEooC or COTS components typically require the least integration effort. However, the limitations and requirements of the safety manual provided with the component *must* be respected.
All documents required for a qualification are usually available and can be provided.

Non-certified standard components often require high integration effort as the component must be qualified. The documents required to qualify these components are often not available (e.g. design specifications or verification results).

Standard components proven in use usually require medium levels of effort due to their need to be qualified. Field data must be collected and possible erratas need to be analyzed with respect to their potential safety impact.

Elements in context are developed by a supplier which is specifically given the specification of the element.
A development interface agreement (DIA) defines the responsibilities regarding the safety aspects and must be negotiated with the chosen supplier.



08 GLOSSARY

TERM	DEFINITION
Assessment	*The examination of a characteristic of an item or element.*
Audit	*The examination of an implemented process.*
ASIL	*Automotive Safety Integrity Level. See section 5*
Component	*See section 3*
COTS	*Commercial off-the-shelf; see section 7 and section 4*
Controller	*This typically refers to an ECU which is part of a system. See section 3*
DIA	*Development Interface Agreement. An agreement between a customer and a supplier in which the responsibilities for activities, evidence or work products to be exchanged by each party are specified. See section 7*
ECU	*An Electronic Control Unit; in the context of ISO 26262 also refered to as "controller"*
E/E Systems	*A system that consists of electrical and/or electronic elements, including programmable devices*
Element	*See section 3*
Freedom From Interference	*No element interferes with any another element in a way that a safety requirement is violated. In this context the resource related aspects "timing", "stack" and "memory" become very important because here, functionally independent elements share resources.*
Functional Safety	*The absence of unreasonable risk due to hazards caused by the malfunctioning behaviour of E/E systems.*
Functional Safety Requirement	*The specification of implementation-independent safety behaviours, or implementation-independent safety measures, (including its safety-related attributes).*
Hardware Part	*See section 3*
Hazard	*A potential source of harm caused by malfunctioning behaviour of an element.*
Item	*See section 3*
OEM	*Here: automobile manufacturer*
Risk	*The combination of the probability of occurrence of harm and the severity of that harm.*
Safety	*The absence of unreasonable risk.*
Severity	*An estimate of the extent (S1=low, S2=medium, S3=high) of harm to one or more individuals that can occur in a potentially hazardous situation.*
Software Component	*See section 3*
Software Unit	*See section 3*
System	*A set of elements that relates (at least) a sensor, controller and an actuator with one another. Note 1: The related sensor or actuator can be included in the system, or can be external to the system. Note 2: An element of a system can also be another system. See section 3.*
SEooC	*A "System element out of context"; see section 7*

09 REFERENCES

1. WIKIPEDIA
https://en.wikipedia.org/wiki/ISO_26262

2. ISO
http://www.iso.org/iso/home/search.htm?qt=iso+26262&sort=rel&type=simple&published=on

3. Infineon
http://www.infineon.com

4. Jenkins Server
https://www.jenkins.io

GLIWA engineering
gliwa-engineering.com
GLIWA engineering GmbH | Pollinger Str. 1 | 82362 Weilheim | Germany