Executive Summary

Functional Safety in accordance with ISO 26262

ZVEI UG2 ad hoc working group,
"Functional Safety in accordance with ISO 26262"

Electronic Components and Systems (ECS) Division

Impressum

Executive Summary

Funktionale Sicherheit ISO 26262

ZVEI UG2 ad hoc working group, "Functional Safety in accordance with ISO 26262"

Published by:

ZVEI–German Electrical and Electronic Manufacturers‘ Association e.V.

Electronic Components and Systems (ECS) Division

Lyoner Straße 9

60528 Frankfurt am Main, Germany

Phone: 069 6302 - 276

Fax: 069 6302 - 407

E-mail: zvei-be@zvei.org

www.zvei.org/ecs

contact person:

Dr. Stefan Gutschling

Authors:

Stefan Kriso	Robert Bosch GmbH
Christopher Temple	Freescale Halbleiter Deutschland GmbH
Berthold Arends	Marquardt GmbH
Pierre Metz	Brose Fahrzeugteile GmbH Co. KG
Bernd Enser	SANMINA-SCI Germany GmbH

Foto:

ZVEI–German Electrical and

Electronic Manufacturers‘ Association e.V.

Juni 2012

Contents

What is functional safety in accordance with ISO 26262?

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 function[2].

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.

---

[1] The German word "Sicherheit" is used to translate both the English "security" and "safety," unfortunately making it very difficult to differentiate between the two attributes in German. For this reason, the English terms are mainly used in German-speaking professional circles.

[2] This is considered in detail as part of the ZVEI's "Robustness Validation" working group.

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 ISO 26262 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.

Comments on ISO 26262

One frequently misunderstood aspect of ISO 26262 is the ASIL classification. A fundamental principle of the ASIL classification is that it is the safety goals, not the system, that are evaluated! It must also be borne in mind that a system usually has to fulfill a whole host of safety goals.

Unfortunately, in practice even experts have adopted an interpretation whereby the most important ASIL classification is transferred to the system. It is therefore common to talk of an "ASIL-D system" in the case of an airbag system, for example, ignoring the fact that an airbag system must also fulfill many other safety goals under various different ASIL classifications. If reference is simply made to ASIL classification, it is impossible - without knowledge of the functional and technical safety concept - to obtain detailed information on the requirements made of specific components within the system. The frequently heard term "ASIL-X component" is therefore misleading.

As the ASIL classification for any safety goals is typically calculated at whole-vehicle level and separately from the actual implementation of the system, it makes sense for the vehicle manufacturer to specify the safety goals to his suppliers together with the corresponding ASIL classifications. This can be regulated under a DIA. If this is not the case, e.g. in the case of platform development on the part of the supplier, then the supplier must make assumptions regarding the safety goals and associated ASIL

classifications, which the customer (OEM) must then validate on system integration. In this case, the standard represents the concept of "Safety Element out of Context" (SEooC) in the information volume 10.

The authors of the standard have gone out of their way to keep it as generic as possible. For example, the standard itself prescribes certain properties and criteria that must be fulfilled as part of the functional and technical safety concept within the framework of the ASIL classification but does not cover the selection of a specific safety concept. One strength of this approach is that it does not impose any unnecessary or potentially indiscriminate restrictions and thus ensures the standard's longevity. As a consequence, the information regarding the definition of a suitable safety concept must be acquired in another manner and, naturally, many different safety concepts are suitable for achieving the same safety goals.

One much-discussed aspect of ISO 26262 is the additional time and effort believed to be required by the standard. In this regard, it should be pointed out that the standard expects the purpose underlying the requirements to be met in an auditable manner. The standard is thus flexible with regard to justified deviations provided that the justification is adequate in each case. In principle, it can be expected that extra time and effort may be required in the introductory phase for integrating the safety lifecycle in the development workflow. By and large, technical demands are due to the functional safety of the system and not the standard. The demands made on safety-related validation should not be underestimated. Although these too are due more so to the functional safety of the system rather than the standard, they are made more significant by the standard's strict verification requirements.

Following approval of the normative sections of ISO 26262 as an international standard in November 2011, there are now no obstacles to successful implementation.

Published by:

ZVEI–German Electrical and Electronic Manufacturers‘ Association e.V.
Electronic Components and Systems (ECS) Division
Lyoner Straße 9
60528 Frankfurt am Main, Germany

Phone: 069 6302 - 276
Fax: 069 6302 - 407
E-mail: zvei-be@zvei.org
www.zvei.org/ecs