ISO 26262

ISO 26262 is a Functional Safety standard, titled "Road vehicles – Functional safety".

1 Overview

Functional safety features form an integral part of each automotive product development phase, ranging from the specification, to design, implementation, integration, verification, validation, and production release. The standard ISO 26262 is an adaptation of the Functional Safety standard IEC 61508 for Automotive Electric/Electronic Systems. ISO 26262 defines functional safety for automotive equipment applicable throughout the lifecycle of all automotive electronic and electrical safety-related systems.

The first edition, published on 11 November 2011, is intended to be applied to electrical and/or electronic systems installed in "series production passenger cars" with a maximum gross weight of 3500 kg. It aims to address possible hazards caused by the malfunctioning behaviour of electronic and electrical systems.

Although entitled "Road vehicles – Functional safety" the standard relates to the functional safety of Electrical and Electronic systems, not to that of systems as a whole or of their mechanical subsystems.

The standard consists of 9 normative parts and a guideline for the ISO 26262 as the 10th part.

Like its parent standard, IEC 61508, ISO 26262 is a risk-based safety standard, where the risk of hazardous operational situations is qualitatively assessed and safety measures are defined to avoid or control systematic failures and to detect or control random hardware failures, or mitigate their effects.

- Provides an automotive safety lifecycle (management, development, production, operation, service, decommissioning) and supports tailoring the necessary activities during these lifecycle phases.
- Covers functional safety aspects of the entire development process (including such activities as requirements specification, design, implementation, integration, verification, validation, and configuration).
- Provides an automotive-specific risk-based approach for determining risk classes (Automotive Safety Integrity Levels, ASILs).
- Uses ASILs for specifying the item's necessary safety requirements for achieving an acceptable residual risk.
- Provides requirements for validation and confirmation measures to ensure a sufficient and acceptable level of safety is being achieved.[1]

VDC Research reports that adherence to ISO 26262 and AUTOSAR is expected to increase significantly in the next two years.[2] Therefore, many functional safety service providers have created training programs to help understand the various safety processes as well as legal responsibilities and what is involved to achieve compliance.

The ten parts of ISO 26262:

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

2 Vocabulary

ISO 26262 specifies a vocabulary (a Project Glossary) of terms, definitions, and abbreviations for application in all parts of the standard.[3] Of particular importance is the careful definition of *fault*, *error*, and *failure* as these terms are key to the standard's definitions of functional safety processes,[4] particularly in the consideration that "A *fault* can manifest itself as an *error* ... and the *error* can ultimately cause a *failure*".[3]

Item Within this standard, *item* is a key term. *Item* is used to refer to a specific system or array of systems that implements a function at the vehicle level

to which the ISO 26262 Safety Life Cycle is applied. That is, the *item* is the highest identified object in the process and is thereby the starting point for product-specific safety development under this standard.

Element System or part of a system, including components, hardware, software, hardware parts, and software units -- effectively, anything in a system that can be distinctly identified and manipulated.

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 the ability of an *element* to perform a function as required.

Note: Since an element's specification defines its required function, the standard recognizes incorrect specification as a potential source of failure.

Malfunctioning Behaviour *Failure* or unintended behaviour of an item with respect to its design intent.

Hazard Potential source of harm caused by malfunctioning behaviour of the *item*.

Functional Safety Absence of unreasonable risk due to *hazards* caused by malfunctioning behaviour of Electrical/Electronic systems.

Note: In contrast to the formal vocabularies defined for other Functional Safety standards, Fault Tolerance is not explicitly defined within this standard -- it is assumed impossible to comprehend all possible faults in a system.[5] Functional Safety *rather than Fault Tolerance is the objective of the standard. ISO 26262 does not use the (IEC 61508) terms SFF and hardware fault tolerance. The terms* single point faults metric *and* latent faults metric *are used instead.*[6]

3 Functional Safety Management

ISO 26262 provides a standard for functional safety management for automotive applications, defining standards for overall organizational safety management as well as standards for a safety life cycle for the development and production of individual automotive products.[7][8][9][10] The ISO 26262 safety life cycle described in the next section operates on the following safety management concepts:[3]

Hazardous Event A *hazardous event* is a relevant combination of a vehicle-level *hazard* and an operational situation of the vehicle with potential to lead to an accident if not controlled by timely driver action.

Safety Goal A *safety goal* is a top-level safety requirement that is assigned to a system, with the purpose of reducing the risk of one or more *hazardous events* to a tolerable level.

Automotive Safety Integrity Level An *Automotive Safety Integrity Level* (ASIL) represents an automotive-specific risk-based classification of a *safety goal* as well as the validation and confirmation measures required by the standard to ensure accomplishment of that goal.

Safety Requirement *Safety requirements* include all *safety goals* and all levels of requirements decomposed from the safety goals down to and including the lowest level of functional and technical safety requirements allocated to hardware and software components.

4 Safety Life Cycle

Processes within the ISO 26262 *safety life cycle* identify and assess hazards (safety risks), establish specific safety requirements to reduce those risks to acceptable levels, and manage and track those safety requirements to produce reasonable assurance that they are accomplished in the delivered product. These safety-relevant processes may be viewed as being integrated or running in parallel with a managed requirements life cycle of a conventional Quality Management System:[11][12]

- An *item* (a particular automotive system product) is identified and its top level system functional requirements are defined.
- A comprehensive set of *hazardous events* are identified for the *item*.
- An *ASIL* is assigned to each *hazardous event*.
- A *safety goal* is determined for each *hazardous event*, inheriting the ASIL of the hazard.
- A vehicle level *functional safety concept* defines a *system architecture* to ensure the *safety goals*.
- *Safety goals* are refined into lower-level *safety requirements*.

  (In general, each safety requirement inherits the ASIL of its parent safety requirement/goal. However, subject to constraints, the inherited ASIL may be lowered by decomposition of a requirement into redundant requirements implemented by sufficiently independent redundant components.)

- "Safety requirements" are allocated to *architectural components* (subsystems, hardware components, software components)

(In general, each component should be developed in compliance with standards and processes suggested/required for the highest ASIL of the safety requirements allocated to it.)

- The architectural components are then developed and validated in accord with the allocated safety (and functional) requirements.

5 Automotive Safety Integrity Level (ASIL)

Main article: Automotive Safety Integrity Level
See also: Comparison of ASIL with Other Hazard Level Standards

Automotive Safety Integrity Level refers to an abstract classification of inherent safety risk in an automotive system or elements of such a system. ASIL classifications are used within ISO 26262 to express the level of risk reduction required to prevent a specific hazard, with ASIL D representing the highest and ASIL A the lowest. The ASIL assessed for a given hazard is then assigned to the safety goal set to address that hazard and is then inherited by the safety requirements derived from that goal.[13]

5.1 ASIL Assessment Overview

The determination of ASIL is the result of *hazard analysis and risk assessment*.[14] In the context of ISO 26262, a hazard is assessed based on the relative impact of hazardous effects related to a system, as adjusted for relative likelihoods of the hazard manifesting those effects. That is, each hazardous event is assessed in terms of severity of possible injuries within the context of the relative amount of time a vehicle is exposed to the possibility of the hazard happening as well as the relative likelihood that a typical driver can act to prevent the injury.[15]

5.2 ASIL Assessment Process

At the beginning of the safety life cycle, hazard analysis and risk assessment is performed, resulting in assessment of ASIL to all identified hazardous events and safety goals.

Each *hazardous event* is classified according to the *severity* (S) of *injuries* it can be expected 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 recognizes that consideration of the severity of a possible injury is modified by how likely the injury is to happen; that is, for a given hazard, a hazardous event is considered a lower risk if it is less likely to happen. Within the *hazard analysis and risk assessment* process of this standard, the likelihood of an injurious hazard is further classified according to a combination of

exposure (E) (the relative expected frequency of the operational conditions in which the injury can possibly happen) and

control (C) (the relative likelihood that the driver can act to prevent the injury).

Exposure Classifications (E): **E0** Incredibly unlikely

E1 Very low probability (injury could happen only in rare operating conditions)

E2 Low probability

E3 Medium probability

E4 High probability (injury could happen under most operating conditions)

Controllability Classifications (C): **C0** Controllable in general

C1 Simply controllable

C2 Normally controllable (most drivers could act to prevent injury)

C3 Difficult to control or uncontrollable

In terms of these classifications, an "Automotive Safety Integrity Level D" hazardous event (abbreviated "ASIL D") is defined as an event having reasonable possibility of causing a life-threatening (survival uncertain) or fatal injury, with the injury being physically possible in most operating conditions, and with little chance the driver can do something to prevent the injury. That is, *ASIL D* is the combination of S3, E4, and C3 classifications. For each single reduction in any one classification from its maximum value (excluding reduction of C1 to C0), there is a single level reduction in the ASIL from *D*. [For example, a hypothetical uncontrollable (C3) fatal injury (S3) hazard could be classified as ASIL A if the hazard has a very low probability (E1).] The ASIL level below *A* is the lowest level, *QM*. *QM* refers to the standard's consideration that below ASIL A, there is no safety relevance and only standard Quality Management processes are required.[14]

These Severity, Exposure, and Control definitions are informative, not prescriptive, and effectively leave some room for subjective variation or discretion between various automakers and component suppliers.[15][16] In response, the Society for Automotive Safety Engineers (SAE) is drafting J2980 – *Considerations for ISO26262 ASIL Hazard Classification* to provide more explicit guidance for assessing Exposure, Severity and Controllability for a given hazard.[17]

6 See also

- Automotive Safety Integrity Level, comparison with other safety level systems
- ARP4754
- IEC 61508 (Related safety standard)
- Time-triggered system (Related software architecture)

7 References

[1] "ISO 26262 Software Compliance: Achieving Functional Safety in the Automotive Industry" white paper by Parasoft

[2] "Automated Defect Prevention for Embedded Software Quality" white paper by VDC Research

[3] *ISO 26262-1:2011(en) Road vehicles — Functional safety — Part 1: Vocabulary*. International Standardization Organization.

[4] *ISO 26262-1:2011(en) Road vehicles — Functional safety — Part 10: Guideline on ISO 26262*. International Standardization Organization. pp. 5–6.

[5] Greb, Karl; Seely, Anthony (2009), "Design of Microcontrollers for Safety Critical Operation (ISO 26262 Key Differences from IEC 61508)", *ARMtechcon*[3] (PDF)

[6] "High-Availability Controller Concept for Steering Systems: The Degradable Safety Controller" (PDF), Recent Researches in Circuits, Systems, Communications and Computers, WSEAS, 2011, pp. 222–228 Missing or empty |title= (help)

[7] ISO 26262-2:2011, "Management of functional safety" (Abstract)

[8] Greb, Karl (2012), "Functional Safety and ISO 26262" (PDF), The Applied Power Electronics Conference and Exposition, Industry Sessions, APEC (www.apec-conf.org), p. 9 Missing or empty |title= (help)

[9] Blanquart, Jean-Paul; et al. (2012), "Criticality categories across safety standards in different domains" (PDF), ERTS2 Congress, Embedded Real Time Software and Systems (www.erts2012.org), pp. 3–4 Missing or empty |title= (help)

[10] ISO 26262-10:2012(E), "Guideline on ISO 26262", pp. 2-3.

[11] Min Koo Lee; Sung-Hoon Hong; Dong-Chun Kim; Hyuck Moo Kwon (2012). "Incorporating ISO 26262 Development Process in DFSS" (PDF). *Proceedings of the Asia Pacific Industrial Engineering & Management Systems Conference*: 1128 (Figure 2). Retrieved 2013-08-01.

[12] Juergen Belz (2011-07-28). *The ISO 26262 Safety Lifecycle*. http://www.mks.com. External link in |publisher= (help)

[13] *Glossary, V2.5.0* (PDF). AUTOSAR. p. 19.

[14] *ISO 26262-3:2011(en) Road vehicles — Functional safety — Part 3: Concept phase*. International Standardization Organization.

[15] Hobbs, Chris; Lee, Patrick (2013-07-09). *Understanding ISO 26262 ASILs*. *Electronic Design*. Embedded Technologies (Penton Electronics Group).

[16] Dr. Qi Van Eikema Hommes, "Assessment of the ISO 26262 Standard, "Road Vehicles – Functional Safety"" (PDF), SAE 2012 Government/Industry Meeting, John A. Volpe National Transportation System Center: SAE, p. 9 Missing or empty |title= (help)

[17] *J2980 - Considerations for ISO 26262 ASIL Hazard Classification*. SAE International.

8 External links

ISO 26262-1:2011(en) (Road vehicles — Functional safety — Part 1: Vocabulary) at ISO Online Browsing Platform (OBP)

ISO 26262 Template

9 Text and image sources, contributors, and licenses

9.1 Text

- **ISO 26262** *Source:* https://en.wikipedia.org/wiki/ISO_26262?oldid=711197119 *Contributors:* Kku, Kri, SMcCandlish, Attilios, Stephowrs, CmdrObot, Towopedia, Nick Number, April's Fool, Cubidoo, WereSpielChequers, Fuddle, WurmWoode, Swtechwr, Addbot, Kmiki87, FrescoBot, ManojMohamed, Trappist the monk, EmausBot, WikitanvirBot, BG19bot, FuSi Experte, IveGoneAway, Sylda31, Bouxetuv, ChrisGualtieri, Higham100, Nclarkmit, Rk.prashan, Glen Eyre Hall and Anonymous: 15

9.2 Images

9.3 Content license

- Creative Commons Attribution-Share Alike 3.0