

FUNCTIONAL SAFETY & ISO 26262

Keeping up with design: ISO26262 time for an update

The proliferation of electronic systems in passenger cars has led to the steady development of new and existing automotive standards to ensure continued functional safety. One such standard, ISO 26262, is an adaptation of the more general International Electromechanical Commission (IEC) 61508 functional safety standard. ISO 26262 specifically defines functional safety for automotive Electric/ Electronic (E/E) equipment and addresses possible hazards caused by the malfunctioning of E/E systems in passenger vehicles.

Intrinsically ISO 26262 offers regulations and recommendations which can be applied throughout the product development process; from conceptual development to final decommissioning. By implementing the standard, practitioners are able to assign an acceptable risk level to a system or component and document the overall testing process.

In so doing, ISO 26262:

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

Importantly the standard also defines the entire production lifecycle process; including the need for a safety manager, the development of a safety plan, and the definition of confirmation measures including safety review, audit, and assessment.

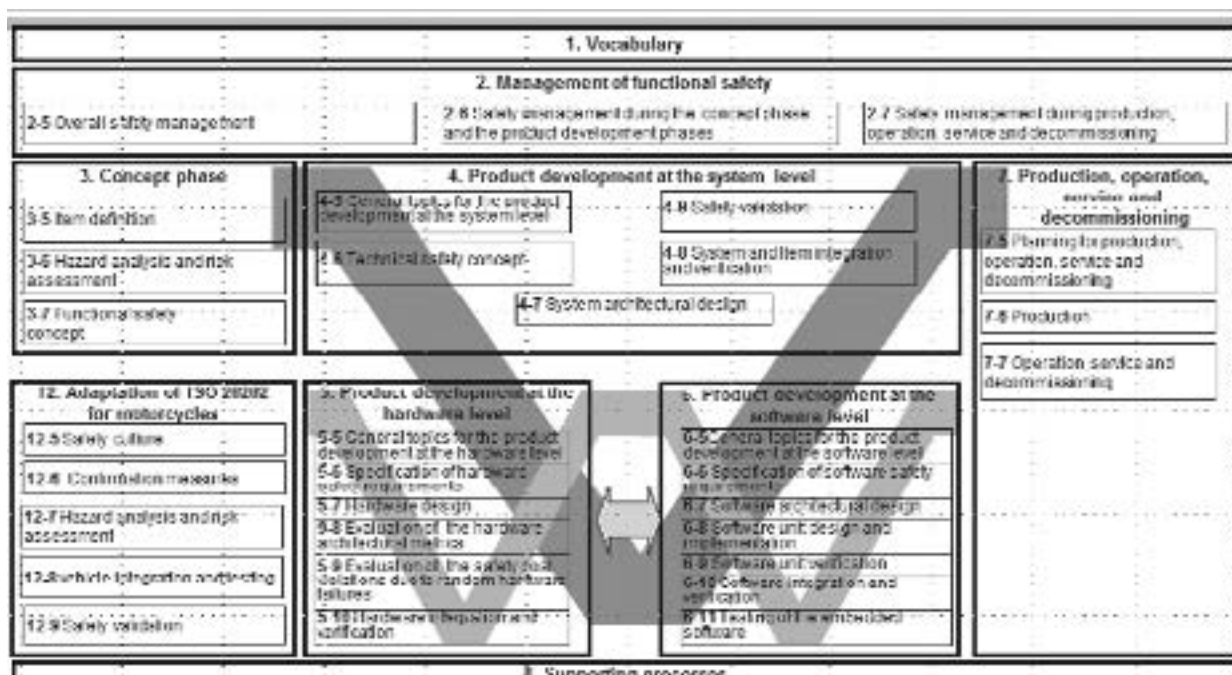
While manufacturers and safety practitioners look to the standard for guidance, lawyers also consider ISO 26262 to be the technical reference in any legal arbitration. According to German law, car producers are generally liable for injury to a person caused by the malfunction of a component or system. If the malfunction could not have been detected by the technical standard, in this case ISO 26262, the liability is set aside.



In order to address the functional safety requirements of the industry ISO 26262 currently comprises ten sections:

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. ASIL- and safety-oriented analysis
10. Guideline for ISO 26262

However, for the standard to remain relevant in an industry undergoing a radical revolution in electrical and electronic systems it is in need of a makeover.



© ISO 2016

ISO26262 (2016)

ISO 26262 edition two looms bright on the horizon

This makeover will come in the form of edition two which is due for publication in 2018. While the deadline is still more than a year away there is a lot of work to be completed, as per the timeline:



Already subcommittees (SC) such as SC 22/ SC38 have published Committee Drafts (CD) for comment. These drafts were finalized as Draft International Standards (DIS) in September 2016. This allows the SC twelve months to review the proposal in order to release the Final Draft International Standard which will eventually be published as the ISO 26262 Edition 2 in January 2018.

One of the objectives of the update is to streamline and contextualize some of the more complex activities: Thus in order to simplify functional safety management many “planning” activities are being moved into Part 2 (Management of functional safety) so that most process-related requirements are grouped into this section.

Another new key requirement dictates that effective communication channels be created between functional safety and other related disciplines. This is aimed primarily at improving cybersecurity functional safety. Related to this, a new Annex showing example interfaces between functional safety and cybersecurity has also been included.

Lacking in the current version, the revised standard will contain important scope extensions to cover trucks, buses, and motorcycles as well as semiconductors, ADAS and autonomous systems.



© Fotolia 2016

ISO 26262 edition two, spreads it's wings to cover other classes of road transport

Although ISO 26262: 2011-2012 has demonstrated significant benefits when applied to the development of passenger cars; trucks, buses and motorcycles are not covered.

Even though truck and bus requirements are mostly integrated into the main sections of the standard a few minor changes specific to vehicles over 3.5tn are being considered:

- Specific requirements pertaining to hazard analysis and risk assessment are under review
 - Management of the variants when performing the analysis
 - Integration of truck and bus examples into Annex B
- New supporting processes for
 - Development of a base vehicle for an application out of scope of ISO 26262
 - Integration of safety elements developed out of scope of ISO 26262

While trucks and buses are mostly covered by the standard as it is applied to passenger cars, motorcycles have very specific requirements which cannot be addressed by the existing standard.



© Fotolia 2016

On the other hand, as many of the requirements specified in ISO 26262 are also applicable to E/E systems fitted to motorcycles, SC 22 has accepted that the E/E systems developed for motorcycles should also be incorporated into ISO 26262.

However, the adoption of an unabridged version of ISO 26262:2011 could lead to the incorrect evaluation of the risk when applied to a motorcycle. Thus, with the introduction of edition two of the standard, the Publicly Available Specification (PAS) will recommend certain motorcycle-specific changes. Thus ISO/PAS 19695:2015, specifically targeting motorcycles, will form the basis of a new Part 12 in the updated standard. ISO/PAS 19695:2015 is intended to be applied to safety-related systems that include one or more electrical and/or electronic systems that are fitted to series production two or three-wheeled motorcycles. As such the proposed standard is intended to address possible hazards caused by malfunctions in the E/E safety-related systems, including the interaction of these systems.

The worldwide established level of technology (“state-of-the-art”) in the motorcycle industry suggests that existing ASIL requirements are not appropriate when applied to motorcycles. However, this will be addressed through an alignment of the proposed MSIL to existing ASILs.

The committee also acknowledges that product development processes and technical solutions within the motorcycle industry are incompatible with those of the automobile industry; therefore, a MSIL has been created from the current ASIL to accommodate motorcycles.

Specifically in the motorcycle industry, external measures (for example, riding rules, training/qualification of riders, personal protective equipment, e.g. helmets and infrastructure features) play a significant role in reducing risks.

Other areas of the standard which would be affected by the inclusion of motorcycles have also been identified and the necessary changes recommended. The content of this PAS still requires consideration and acceptance by SC 32 in order to facilitate the inclusion of motorcycles within the scope of ISO 26262:2011 Edition 2.

It’s also important to note that the PAS is not intended to address the nominal performance of E/E systems, even if dedicated functional performance standards exist for these systems. Nor does it address hazards related to electric shock, fire, smoke, heat, radiation, toxicity, flammability, reactivity, corrosion, release of energy, and similar hazards, unless directly caused by malfunctioning behaviour of E/E safety-related systems.



© Fotolia 2016

Next time in our ISO 26262 report...

“Addressing concerns around emerging technologies”

- Update the hardware development standard
- Edition 2 addresses shortcomings of current software development standards
- Part 11 sets the standard for semiconductor functional safety
- Publicly available specification 19451:1 discusses intellectual property
- Addressing ADAS & fully autonomous safety

Until then, make sure to check out the upcoming 7th International Conference ISO 26262, taking place 27-30 March, 2017, in Frankfurt, Germany!

With the following confirmed companies

**Jaguar Land Rover • Bosch Engineering • Delphi • SP Technical
Research Center • Magna Powertrain • ZF TRW • Horiba Mira •
Siemens • Allegro Microsystems • Marquardt • HELLA**

and many more...

Our target is to understand and tackle the evolving challenges of safety and security engineers for safeguarding tomorrow's automotive innovation.

In 2017, we are bringing together, safety and security professionals of the automotive world for a one of a kind event; a deep dive event on the topics of ISO 26262, Cyber Security and Testing ADAS and self driving cars.

DOWNLOAD THE AGENDA