

FUNCTIONAL SAFETY & ISO 26262

Addressing concerns around emerging technologies

Since the original publication of ISO 26262 on 15 November 2011 the industry has undergone several significant changes. The rapid deployment of ADAS and fully autonomous connected technologies, together with the associated cybersecurity threat has seen growing inadequacies in the original iteration of ISO 26262. As a result, many manufacturers have raised concerns that ISO 26262:2011 no longer adequately addresses the functional safety of modern and emerging E/E architectures.

Updating the hardware development standard

Hardware qualification has two main objectives: to show how the part fits into the overall system and to assess failure modes.

Basic hardware components can be qualified with standard qualification, but more complex parts require evaluation through ASIL decomposition and testing. Hardware components are typically qualified by testing the part in a variety of environmental and operational conditions. The test results are then analyzed with various numerical methods and presented in a qualification report along with the testing procedure, assumptions, and input criteria.



© Fotolia 2016

Currently the ISO 26262 hardware development process starts with planning the hardware development. This plan should be a part of the overall safety plan for the complete product safety process, and should include the measures and methods to be used for hardware design.

After planning, the next step is to use the previous activities such as the technical safety concept and the system design specification to derive hardware safety requirements. These requirements typically specify the requirements and attributes of various safety mechanisms and are used when designing the hardware. However, they may also specify requirements not concerning safety mechanisms, such as requirements for target values for random hardware failures.

The hardware design process includes architectural design and hardware detailed design. The former represents all hardware components and their interactions, while the latter details the design at electrical schematic level by determining the interconnection and hardware elements that make up the hardware components.

Generally, safety requirements as well as non-safety requirements are included in this process to create a single integrated design.

In the creation of the hardware architecture, components are given the highest ASIL of the hardware safety requirements they implement. If a hardware element is made up of sub-elements with different or no ASILs, then each of these sub-elements should be treated with the highest ASIL among them, if criteria for coexistence can be proved.

These criteria are defined in ISO 26262 Part 9 and detail how coexistence is derived from the manner in which sub-elements interact with each other with regard to violation of safety goals.

In short, this means that if it can be proved that a lower-ASIL sub-element does not contribute to the violation of the safety goal of a higher-ASIL sub-element, then the sub-elements may keep their separate ASILs. Once the detailed hardware design has been created based on the architecture, the design should be analyzed regarding if it meets the requirements derived from its ASIL.

It is possible that this process has to be performed in an iterative manner in which the safety analysis of the design requires going back to modify the hardware architecture or component design.

These measures are then used for evaluation of hardware architectural metrics and evaluation of safety goal violations due to random hardware failures. Lastly, the results from the analysis are compared to various target values for the different ASILs.

Finally, the diagnostic coverage of each safety mechanisms must be evaluated in order to find the faults that retain the possibility of violating a safety goal after safety measures have been included in the system. The diagnostic coverage with respect to residual faults is defined as the part of the failure rate (of faults of a single-point origin) in an element that is covered by a certain safety mechanism.

A tribute to the existing hardware development standard is the fact that changes to section 5 (governing hardware development) of the standard are confined to:

The evaluation of safety goal violations due to random hardware failures has seen an update to the Probabilistic Metric for (Random) Hardware Failures, Method 1.

Currently this is defined as the sum of the single point, residual and multipoint fault metrics, expressed in Failure In Time (FITs) - The number of failures that can be expected in one billion (1×10^9) device-hours of operation: Method 1 requires that each cause of a safety goal violation due to random hardware failures is compared to a target failure rate class.

The update, recognising the impact of increasingly complex E/E systems on functional safety, seeks to increase target values by up to one order of magnitude for items composed of multiple systems. (Clause 13 of section 8 describes a new approach to defining complexity in the qualification of hardware components.) Related to the above update is the addition of a residual risk assessment, which will be applied if the target values for Method 1 are not met.

In another minor “update” the SC has suggested that an earlier proposal for a new “residual risk assessment method” be withdrawn.

The final addition to section 5 is the inclusion of example architectures for fault tolerant implementation.

Edition 2 addresses shortcomings of current software development standards

Presently ISO 26262-6 specifies what steps should be taken during the development of software components to ensure product safety. There are seven phases that govern software development:

- Clause 5 Initiation of software development.
- Clause 6 Safety requirements specification.
- Clause 7 Architectural design.
- Clause 8 Unit design and implementation.
- Clause 9 Unit testing.
- Clause 10 Integration testing.
- Clause 11 Safety requirements verification.

These clauses governing the development of software are critical in ensuring functional safety standards are clearly determined and adhered to.



© Fotolia 2016

Clause 5 describes the initiation of the software development. During this phase, the software development process to be used must be selected, as well as which tools will be used.

If model-based development forms part of the development, then the development plan will need to include, among other things, the development of one or more models, the implementation of software based on those models, and plans to confirm that the implementation behaves the same as the model.

The primary objective of the safety requirements specification phase is to identify all software-based functions which could potentially impact safety by either: Directly producing an unsafe state, such as a software module which controls traction while braking, or failing to correctly handle a hardware or software fault.

The requirements for each software component that is identified in the standard must be determined, including such things as timing requirements and the interface between the software component and other system components.

During the architectural design phase, a high-level design for each software component must be developed. The conformance of this architectural design must be verified against measurable safety objectives.

Thereafter each subsystem is designed and implemented as prescribed in the design and implementation phase.

ISO 26262 requires extensive testing to verify both the individual elements as well as complete and integrated systems:

- Unit testing is covered in clause 9. The goal of unit testing is to individually test the correctness of each low-level software module.
- Clause 10 covers integration testing. The purpose of integration testing is to validate the safety of software systems comprising multiple units.

Finally, clause 11 describes the safety-requirements verification process to be completed in order to ensure that the embedded software works correctly in its target environment.

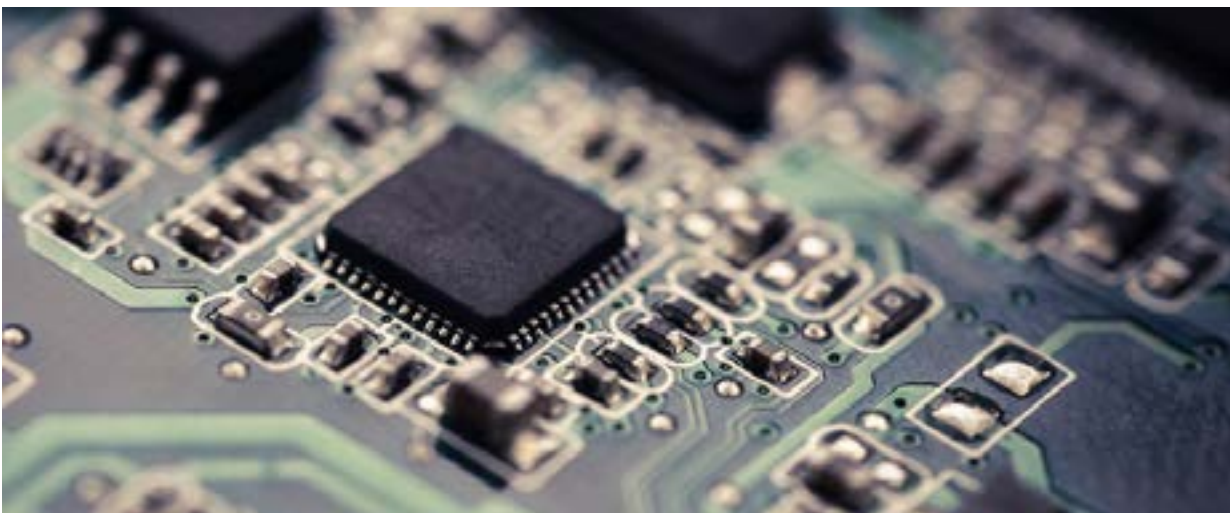
Once again, section 6 covering software development has only undergone a few minor updates in Edition 2:

- The requirements defining properties are to be modified to include a safety analysis to confirm the properties
- The requirements defining functions will call for the inclusion of a safety analysis identifying safety mechanisms to detect and react to software failures.

Whilst semiconductors are recognized as playing a pivotal role in E/E technologies, under ISO 26262:2011 these are not covered as separate, unique entities: Instead manufacturers have to rely on ISO 26262-10 Annex A to define functional safety pertaining to microcontrollers. In this form the standard describes:

- How to apply ISO 26262 definitions to semiconductor devices
- Component, part, sub-part
- MCU development example
- Qualitative and quantitative safety analyses for microcontrollers
- Failure rates for microcontrollers
- Example quantitative analysis
- FMEA based
- Example dependent failure analysis
- Examples of methods for systematic fault detection and avoidance measures
- Hardware design verification
- Supporting documentation

The upcoming Part 11 in the next edition of ISO 26262 will strengthen the focus on semiconductor requirements and ensure the standard remains relevant when applied to systems commonly used in ADAS and fully autonomous driving architectures.



© Fotolia 2016

Part 11 sets the standard for semiconductor functional safety

Part 11, which is currently in the CD stage, has been developed from ISO/PAS 19451-1 (which addresses semiconductors) and elements from the current ISO 26262-10. This section of the update will, for the first time, offer guidance on:

- Fault injection
- Sensors and transducers
- Production and operation
- Confirmation measures and audits

Highlighting the focus on semiconductors the introduction to this section defines key concepts, such as:

- The meaning of component, part and sub-part
- Fault, error and failure in semiconductors
- Semiconductor safety analysis

Because semiconductors are found in a wide variety of modern electronic systems, covering everything from EV motor controllers to sophisticated ADAS it's been deemed important to describe specific semiconductor use cases that cover:

- Multi-core components
- Digital components, memories
- Analogue and mixed signal devices
- Programmable logic devices
- Sensors, transducers

Moreover, to eliminate any ambiguity surrounding the use cases section 11 also contains six annexes of clearly laid out examples.



© Fotolia 2016

During the development of this section, the subcommittee has given careful consideration to the application of the standard to various stages of operation, thereby addressing the following issues:

- Intellectual property
- Dependent failure analysis
- Fault injection for semiconductors
- Interfaces within distributed developments
- Confirmation measures
- HW integration and testing
- Base failure rate estimation
- Production and operation

Publicly Available Specification 19451:1 discusses Intellectual Property

The aforementioned PAS document (ISO/PAS 19451) has recently been approved for publication later this year. Based on ISO 26262-10:2012, Annex A, “ISO 26262 and microcontrollers,” the update has been expanded to include additional types of semiconductor technologies and topics surrounding these.

Importantly the new Publicly Available Specification 19451:1, addresses the following issues relating to the application of concepts within the broader framework of semi-conductors:

- Clarification of ISO 26262 application to semiconductor devices
- Includes a section on Intellectual Property (IP) designs
- General considerations for Intellectual Property designs
- Safety requirements for IP designs
- IP lifecycle
- Work products for IP designs
- Integration of black-box IP designs

With Intellectual Property designs now commonplace the following higher level issues have undergone considerable scrutiny:

- Safety Element out of Context (SEooC)
- In-context
- Use through hardware qualification
- Use through proven in use argument

What's more, the PAS describes the following IP work products in great detail:

- Safety plan
- Safety requirements and verification review
- Safety analysis report
- Analysis of dependent failures
- Confirmation measure report
- Development interface agreement
- Integration documentation set

Addressing ADAS and fully autonomous safety

Greater automation brings with it many challenges: For example the risk model of ISO 26262 assumes that the driver is a part of the control loop. The driver's ability to maintain control is a fundamental consideration when determining a risk. Obviously, greater automation has the potential to take the driver out of the control loop, and as such the demands on functional safety will be significantly impacted upon.

Although not yet ready for publication, ISO/PAS 21448, will focus on the functional safety of ADAS-related hazards caused by "normal operation" of the sensors. Timing for this is as yet undefined.



© Fotolia 2016

As ADAS and connected functions increase, so do concerns around cybersecurity. And although many manufacturers have ad-hoc systems in-place to try and identify functional safety risks, these are largely ineffective in addressing systemic risks.

Information security has focused for too long on just the technical elements, but it is people that develop systems; people who may make mistakes, fail to follow policies and sometimes use the power they have at their keyboard for malicious purposes.

Ed Savage, Cyber Security expert, PA Consulting Group says, "To date, most cyber security related best practice has focused almost exclusively on methods and the controls. Whereas instead, the newly proposed PAS 555 focuses on the outcomes – the aims and impacts of security processes – and helps organisations identify the areas that need protecting the most."

While getting the basics of cyber security right would help significantly, good practice needs to address all dimensions, PAS 555 defines all the dimensions of the cyber security challenge through the complete lifecycle, including risk assessment, protection and mitigation, detection and response, and recovery. This is the first time that this has been achieved and no other standard is as comprehensive.

Setting the standard for cyber security – introducing PAS 555

BSI, the UK's National Standards Body, has created a new specification, PAS 555 Cyber Security Risk Governance and Management, to help organisations manage cyber security. In a domain where there are already a large number of standards and schemes, is there really a need for another?

In fact, it is that very thinking that has led to the creation of PAS 555. The truth is that there are so many different pieces of good practice, it can be confusing to choose between them and potentially very expensive for any organisation to demonstrate its security credentials.

Moreover, despite nearly £3Bn a year spent on information security technology in the UK alone, the volume and scale of cyber security incidents has continued to increase.

The creation of PAS 555 arose from a need recognised by industry and also articulated in the UK Government's 2011 Cyber Security Strategy. It is intended to help organisations of all sizes better understand the risks they face and to take an outcome-based approach to improving cyber security.

PAS 555 is simple. Its non-technical outcomes focused language makes it accessible beyond the IT department; to boards, suppliers and the other business functions who have a part to play in effective cyber security.

Similar to IEC 61508, PAS 555 is proposed as a generic standard meant to be applied across industries. However, as connected technologies in the automotive industry spreads so the cyber security threat increases; thus the interest in this standard.

The PAS is sponsored and supported collaboratively by Cisco, Control Risks, G4S, PA Consulting Group and Symantec, with other key stakeholders involved in its development.



© Fotolia 2016

PAS 555 offers a framework that defines the outcomes of good cyber security practice. It extends beyond the technical aspects of cyber security to encompass physical and people security aspects as well. It can work on a stand-alone basis or can be integrated with existing protocols or standards.

Therefore, the PAS works with other existing standards and good practice, but for the first time allows them to be mapped into a comprehensive framework that can be readily understood. In so doing, it aims to add something truly valuable to what is a minefield of overlapping and sometimes conflicting information. Central to the framework is the requirement for a cyber security risk assessment. This allows an organisation to understand its cyber security risk exposure and develop a robust approach to managing that risk, according to its business context.

However, notwithstanding the impressive strides planned in ISO 26262 Edition 2 the speed at which new technologies are being introduced in the automotive industry is such that, already Edition 2 may be outpaced: And in some instances commentators are predicting that the update has not addressed some lingering issues.

What functional safety challenges remain?

With ISO 26262 designed as a standard meant to be applied by manufacturers across the world differing approaches to interpreting and applying the standard still exist. Although much improved this is an area that requires further refinement.

Furthermore, discussions on cybersecurity highlight the narrow focus of ISO 26262 compared to system safety and wider issues of system dependability. Although PAS555 is seen as a breakthrough in improving cybersecurity functional safety, there are still issues related to the wide scope of the problem.

Similarly, several issues associated with autonomous vehicles have been acknowledged but it is unlikely the updated standard will fully address autonomy in the timescales being discussed for their deployment

And looking forward to 2025 when the majority of cars on the road will have at least one SAE Level 1 (or above) application, one needs to ask the question: Is there a ISO 26262, Edition 3, already in the pipeline?

Sources:

- www.iso.org, Draft 26262 edition 2, <http://www.iso.org/iso/home/>
- Christian Esposito, Università di Napoli Federico II., Hands on the ISO 26262 Standard, June 2016 (Whitepaper)
- Helen Monkhouse, Protean Electric, Can the ISO standard handle the speed of research in the car industry, March 2016 (Whitepaper)
- PA Consulting, Setting the standard for cyber security; introducing PAS 555, June 2016, <http://www.paconsulting.com/our-thinking/setting-the-standard-for-cyber-security-introducing-pas-555/>
- Lauri Ora, ARM, Functional safety for semiconductor IP, February 2016, <https://nmi.org.uk/wp.../ARM-NMI-ISO-26262-practitioners-workshop-2016-v4.pdf>
- ISO, ISO/PAS 19695:2015(E), Motorcycles — Functional safety, Dec 2015, Whitepaper
- Euroforum interview with Stefan Kriso, Robert Bosch, ISO 26262 part 11, Sept 2016, <http://www.euroforum.de/interview/>
- Dr. Christof Eber, Vector consulting Services, Functional Safety with ISO 26262, June 2016, http://vector.com/portal/medien/vector_consulting/publications/Webinar_Safety.pdf
- John Blyle, JB Systems, What makes Automotive Electronics ISO 26262 Different from other Standards?, February 2016, <http://jbsystech.com/what-makes-automotive-electronics-iso-26262-different-from-other-standards/>

27-30 March 2017
Dorint Hotel Oberursel,
Frankfurt, Germany

ISO 26262

Improving safety of advanced mobility

ISO 26262 Conference Advisory Board



Prof. Dr. Stefan Leue,
Chair of Software Engineering
Computer Information Science,
University of Konstanz, Germany



Dr. Ing. Rafał Dorociak,
Head of Safety Platform, **HELLA KGaA**
Hueck & Co., Germany



Dr. Tomislav Lovric,
Safety Assesor, **TRW Automotive**
Lucas Varity GmbH, Germany



Dr.-Ing. Florian Leitner-Fischer,
Team Lead Software, **ZF TRW**
Automotive, Germany



Roger Rivett,
Functional Safety Technical Specialist,
Jaguar Land Rover Limited, MISRA
Chairman, UK



Dr. Pierre Metz,
Organisational Safety Manager,
Brose Fahrzeugteile GmbH & Co. KG



Johannes Schild,
Expert Functional Safety Manager,
Bosch Engineering GmbH, Germany



Adam Schnellbach,
Functional Safety Leader, **MAGNA**
Powertrain AG & Co KG, Germany

ISO 26262 Conference - 2017 Focus:

- Understanding the ISO/DIS 26262 and explanation of the changes and newest additions
- Applying ISO 26262 to highly complex architectures and autonomous systems
- How to implement a lean functional safety process with minimum business disruption

**DOWNLOAD
THE AGENDA**