

ISO 26262 compliance

Addressing the compliance complexity of safety-relevant E/E systems



**Add value.
Inspire trust.**

White paper

Abstract

An increasing number of high profile recalls have proved that even industry leaders in automotive technology are not immune to functional safety issues. ISO 26262 provides an automotive safety lifecycle that covers management, development, production, operation, service and decommissioning. Automotive Original Equipment Manufacturers (OEMs) and their suppliers risk losing their competitive advantage if they fail to implement the requirements of ISO 26262. They also often approach functional safety as an afterthought following product development, rather than as an integral part of the design process, spending millions of dollars rectifying issues, rather than avoiding them from the start.

This whitepaper gives an overview of how the automotive industry can address this challenge to help minimise the risks of product liability and ensure continued profitability.

Contents

INTRODUCTION.....	3
OVERVIEW OF ISO 26262.....	4
STAFF COMPETENCE.....	7
CREATING A CULTURE OF FUNCTIONAL SAFETY.....	8
REAL-WORLD IMPLEMENTATION.....	9
CONCLUSION.....	10

About the TÜV SÜD expert



Andreas Bärwald

Business Line Manager Safety and Electronics at TÜV SÜD Auto Service GmbH

Andreas Barwald has global responsibility for TÜV SÜD's Automotive Functional Safety operation, which includes business units in Canada, China, Japan, Korea and the USA.

As head of TÜV SÜD's accredited test laboratory, and an appointed technical certifier, Andreas and his team deliver the Functional Safety Certification Programme (FSCP). This ensures that safety professionals are certified to the highest standards of quality and deliver a sound foundation for a company's compliance to ISO 26262.

Andreas first joined TÜV SÜD Automotive GmbH in 2004 as Group Manager Functional Safety and Semiconductor. He has a highly technical background, having studied Computer Science at university, and joined TÜV SÜD from BFI Peters, a vocational training institute, where he was an IT lecturer.

Introduction

ISO 26262 was published in 2011 to address the increasing complexity of safety-relevant electrical and electronic systems, and is now recognised as the state-of-the-art functional safety requirement. The standard covers safety-related systems that are installed in series production passenger cars, and include one or more electrical and/or electronic (E/E) system.



While ISO 26262 is a complex standard, it will help OEMs to improve the safety of their product, minimise risks of product liability and help them remain competitive.

The ISO 26262 framework deals with product related requirements that define properties which can be observed as specific safety-features in the final product, as well as process related requirements that reduce the probability of systematic faults (but cannot directly be observed as a feature of the product).

Following a number of functional safety related issues that have put lives at risk and cost the industry dear, few automotive OEMs and suppliers will dispute the importance of the standard. However, while the necessity to improve functional safety in the automotive industry has become widely accepted, many

will agree ISO 26262 is a challenging standard to interpret and implement due to its complexity and the lack of functional safety experts within the industry.

While ISO 26262 is a complex standard, it will help OEMs to improve the safety of their product, minimise risks of product liability and help

them remain competitive. It will also enhance a business's reputation as a premium quality manufacturer with a commitment to safety, thereby improving attractiveness to both consumer and corporate customers.

ISO 26262 contains 10 sections, which provide a system of stages to manage the development process:

THE 10 SECTIONS OF ISO 26262:

1. Vocabulary – a glossary of terms and abbreviations for application across all parts of the standard
2. Management of functional safety – outlines organisational aspects of functional safety management
3. Concept phase – a risk evaluation and safety concept
4. Product development at the system level – safety aspects of the system development
5. Product development at the hardware level – safety aspects of hardware development
6. Product development at the software Level – safety aspects of software development
7. Production and operation – safety aspects after Start of Production (SOP)
8. Supporting processes – quality ensuring processes
9. ASIL-oriented and safety oriented analyses – safety analysis
10. Guidelines on ISO 26262

Overview of ISO 26262

In general, ISO 26262:

Provides an automotive safety lifecycle (management, development, production, operation, service, decommissioning) and supports tailoring the necessary activities during these lifecycle phases.

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, verification and confirmation measures to ensure a sufficient and acceptable level of safety being achieved.

Figure 1 shows a useful diagrammatic representation of the various elements required to achieve compliance.

While it is not demanded by the standard, it would be best practice to initially perform a gap analysis. This is an assessment of your existing processes and products against the requirements of the standard.

Typically the process involves the internal and independent third-party functional safety experts investigating key issues of the development process and/or

technical product or system. These processes are outlined within ISO 26262 and include documentation, management processes, technical functions and risk analysis. In TÜV SÜD's experience, this can usually be accomplished over a week long workshop.

Stages 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.

The definition of the item is the first of these stages, which means identifying when it is necessary to achieve functional safety and what the required safety functions are. A risk assessment process, carried out according to accepted principles of risk assessment, is the best way of achieving this. This approach, for example, defines which actions of a product are defined as safety-relevant and which are not safety-relevant.

A safety goal can then be determined for every hazard identified. For example if one of the safety requirements identified is an airbag, a potential hazard may be the airbag initiating unintentionally and the safety goal would be to prevent this.

The result of the risk assessment is the Automotive Safety Integrity

Level (ASIL), which is a measure of the potential risk and determines the activities and methods required to address the risk in an appropriate manner. The ASIL is defined by the level of risk based on a combination of the probability of exposure, the possible controllability by a driver, and the possible severity if a critical event occurs.

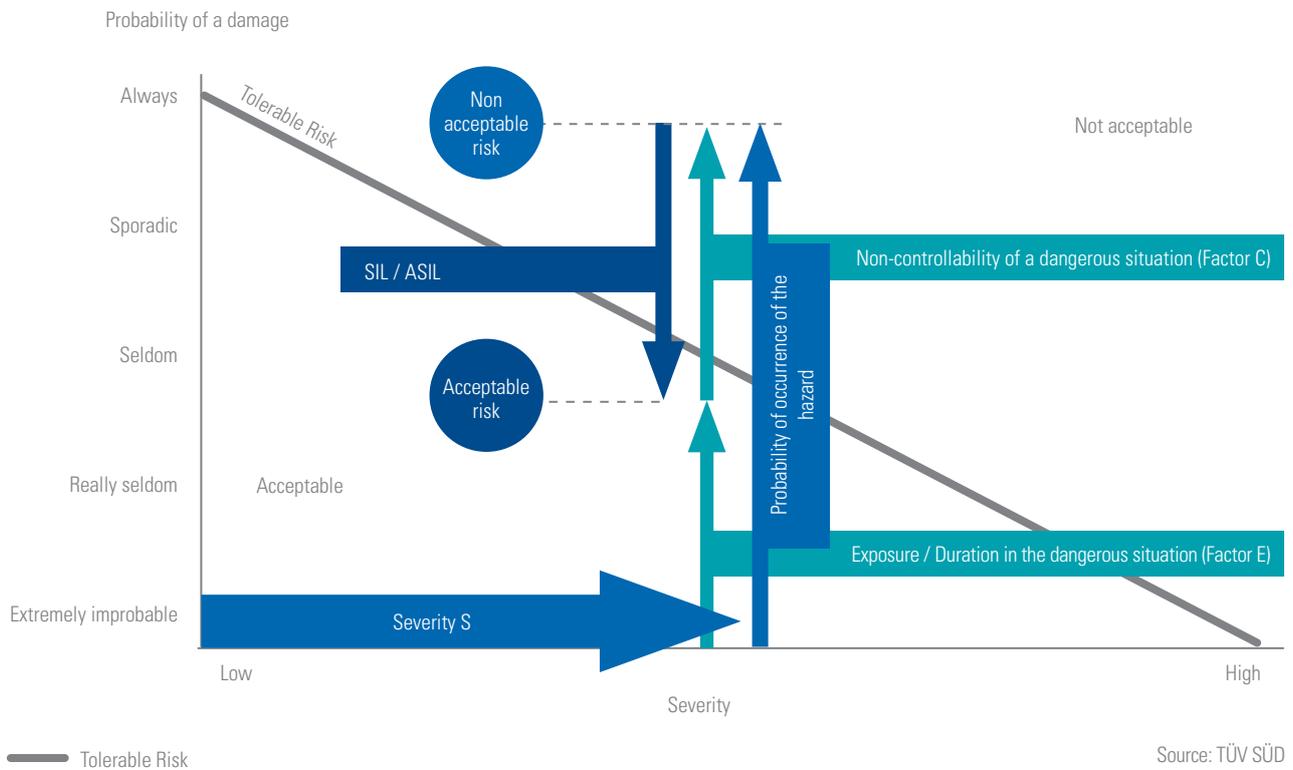
The ASIL is defined in four steps, from ASIL A (the lowest amount of risk reduction) to ASIL D (the highest amount of risk reduction), with the standard detailing the minimum requirements according to the assigned ASIL. This is a key component for ISO 26262 compliance, as the ASIL, and therefore the hazard level, is determined at the beginning of the development process, and the intended functions of the safety system are then analysed with respect to those possible hazards (Figure 2).

Stages 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.

FIGURE 1: OVERVIEW OF THE STRUCTURE OF ISO 26262

1. VOCABULARY		
2. MANAGEMENT OF FUNCTIONAL SAFETY		
2-5 Overall safety management	2-6 Safety management during the concept phase and the product development	2-7 Safety management after the item's release from production
3. CONCEPT PHASE	4. PRODUCT DEVELOPMENT AT THE SYSTEM LEVEL	7. PRODUCTION AND OPERATION
3-5 Item definition	4-5 Initiation of product development at the system level	4-11 Release for production
3-6 Initiation of the safety lifecycle	4-6 Specification of the technical safety requirements	4-10 Functional safety assessment
3-7 Hazard analysis and risk assessment	4-7 System design	4-9 Safety validation
3-8 Functional safety concept		4-8 Item intergration and testing
	5. PRODUCT DEVELOPMENT AT THE HARWARE LEVEL	6. PRODUCT DEVELOPMENT AT THE SOFTWARE LEVEL
	5-5 Initiation of product development at the hardware level	6-5 Initiation of product development at the software level
	5-6 Specification of hardware safety requirements	6-7 Software architectural design
	5-7 Hardware design	6-8 Software unit design and implementation
	5-8 Evaluation of the hardware architectural metrics	6-9 Software unit testing
	5-9 Evaluation of the safety goal violations due to random hardware failures	6-10 Software integration and testing
	5-10 Hardware integration and testing	6-11 Verification of software safety requirements
8. SUPPORTING PROCESSES		
8-5 Interfaces within the distributed developments		8-10 Documentation
8-6 Specification and management of safety requirements		8-11 Confidence in the use of software tools
8-7 Configuration management		8-12 Qualification of software components
8-8 Change management		8-13 Qualification of hardware components
8-9 Verification		8-14 Proven in use argument
9. ASIL-ORIENTATED AND SAFETY-ORIENTATED ANALYSES		
9-5 Requirements decomposition with respect to ASIL tailoring		9-7 Analysis of dependent failures
9-6 Criteria for coexistence of elements		9-8 Safety analyses
10. GUIDELINE ON ISO 26262		

FIGURE 2: APPROACH TO HAZARD ANALYSIS



The next stage is to ensure that the defined safety requirement performs as its design intended, which must include accounting for failures of the underlying hardware and the prevention of systematic faults. The identified safety goals, which define the safety requirements, must also be implemented as specified by the appropriate ASIL, with suitable processes and methods implemented.

This is achieved by defining a functional safety concept, with the technical aspects detailed in a technical safety concept, together with a safety design (or safety

architecture), that determines the hardware and software safety requirements. Using the airbag example, a safety architecture could be defined that stops the airbag inflating unintentionally, but ensures it protects the driver in a crash.

It is also necessary to formulate a plan that closes any conformity gaps. Should, for example, the hardware layout of a safety relevant electronic system leave a high risk of malfunction when there is a short circuit, the plan would outline how the layout (design) needs to be changed to prevent this. It would also describe how the design will be

technically modified, the still safe interaction of the modification with other systems and the supporting documentation required. This will ensure all activity is documented correctly so, if there is an incident, it can be re-assessed at a later date. This is also required even if no change to the layout or concept was necessary. It is crucial for such measures to be taken early in the process as changes become more costly and time-consuming in later stages.

Verification that the system meets the assigned ASIL is also a vital stage. This is achieved by a specialist, either in-house or

a qualified third-party, running appropriate tests and analysis to determine the safety function's mean time between failures.

Many that have experienced the implementation of ISO 26262 fully understand the value of obtaining an external assessment, as well as certification. This final step

involves attaining a technical report or certificate from an independent assessor as a proof of conformity to the latest standard. For example, TÜV SÜD provides testing based on your development documentation and on-site assessments. The result is a technical report that evaluates your systems, hardware, software and tools, which is especially

important for suppliers as leading automotive manufacturers in markets such as France, Germany, Japan, Korea and the United States will often only accept reports or certificates endorsed by reputable third parties.

Staff competence

While ISO 26262 sets out the complex 'functional' steps that must be taken towards compliance, you must first ensure that your business has the expertise required to understand how ISO 26262 relates to your products and, if required, how to implement any changes towards conformity. This can either be achieved through training existing staff, hiring functional safety

specialists to become part of your staff, or outsourcing the work to an independent third-party.

It is vital that relevant staff fully understand the content of ISO 26262, the required documentation and the key issues in each of its ten sections.

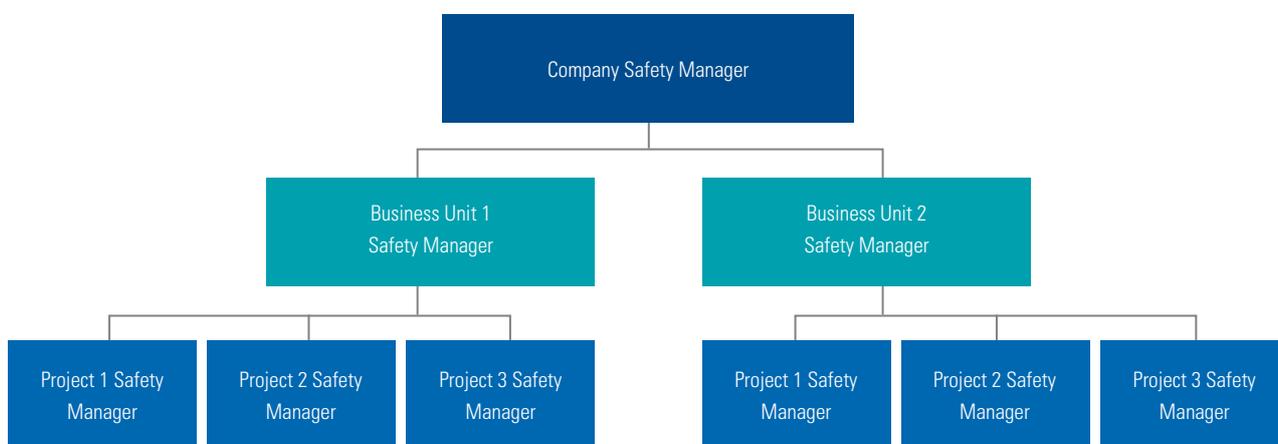
Within larger organisations there are often three key task personnel

profiles that could support successful functional safety management within the organisation:

1. Company Safety Manager
2. Business Unit Safety Manager
3. Project Safety Manager - the only role required by the standard

This hierarchy is shown in Figure 3.

FIGURE 3: THREE KEY TASK PROFILES FOR SUCCESSFUL FUNCTIONAL SAFETY MANAGEMENT



Source: TÜV SÜD

It is vital that relevant staff fully understand the content of ISO 26262, the required documentation and the key issues in each of its ten sections.

The Company Safety Manager is the custodian of an organisation's safety culture, ensuring consistent communication amongst all staff, the company's management team and external service providers. They are also responsible for the further

development of functional safety within the business, ensuring that company specific guidelines and staff training are updated according to compliance changes.

They should also instigate regular audits of departments to ensure consistent compliance with company-wide guidelines for functional safety, including regular adjustment meetings with the safety managers of each separate business unit.

The Business Unit Safety Manager is not a role specified within the standard, but is common within larger organisations. They are the central point of contact within the business unit for all questions relating to functional safety, and should also be responsible for the maintenance of

basic data and ensure the appropriate training of staff.

The Project Safety Manager is the most important role, and the only one that is required by the standard. They work with the Business Unit Safety Manager to coordinate specific functional safety projects. The Project Safety Manager typically has the responsibility for the creation and maintenance of a project safety plan, which includes the execution of assessments, the application of measures to avoid systematic faults, as well as the execution of verification and validation measures. They also have responsibility for the coordination of all internal and external interfaces (business units, suppliers, customers etc.).



Creating a culture of functional safety



Achieving functional safety requires more than just an understanding of the technical requirements of ISO 26262. For successful implementation there must be a culture where employees at all levels 'live and breathe' its mantra.

Functional safety is an extension of quality management that can only work if all employees adhere to high standards. For example, a major

safety issue can be caused if just one out of the hundreds of engineers involved in the development process misses an activity or uses the wrong method.

To help OEMs and suppliers achieve this cultural consistency, appropriate management processes must be in place, including the strict execution of safety rules and tools.

Functional safety is an extension of quality management that can only work if all employees adhere to high standards.

Real world implementation

TÜV SÜD's functional safety team was established more than 30 years ago and works with OEMs and automotive suppliers globally, including:



The team at GAIO receive the ISO 26262 certificates from TÜV SÜD

Toshiba*

Toshiba develops and manufactures a wide range of automotive components, including motors, inverters, batteries, microcomputers, ADAS and their related software. In March 2012 it received the highest level of ISO 26262 certification for software development process from TÜV SÜD. The process is now capable of supporting product developments up to the highest Automotive Safety Integrity Level (ASIL D).

Receiving ISO 26262 certification allows Toshiba to promote the continued expansion of its automotive systems business and provide secure, reliable products that meet the highest international safety standards.

Panasonic Corporation

Panasonic's development process has also been certified for ISO 26262 by TÜV SÜD. Its automotive equipment and device software development processes are now recognized as being capable up to the highest Automotive Safety Integrity Level (ASIL D).

The certification by TÜV SÜD demonstrates that Panasonic's software development processes comply with these safety requirements. This helps the company to manufacture safer products and contribute to the creation of a secure, safe, environmentally friendly, convenient, and comfortable automobile society.

GAIO Technology Co., Ltd

GAIO was the first company in the Asia-Pacific region to obtain tool ISO 26262 certification for its embedded software verification tools. Normally ISO 26262 requires users to create development tool qualification reports according to a Tool Confidence Level (TCL) for each software tool used. However, the tool certification granted by TÜV SÜD to GAIO's tools is applicable for even the highest-demanding tool confidence level (TCL3). Thus, end-users of GAIO's certified tools are not required to perform tool qualification of their own.

*Includes Toshiba Corporation Semiconductor & Storage Products Company and Toshiba Corporation Social Infrastructure Systems Company.

Conclusion

While ISO 26262 is complex, it is imperative for OEMs and suppliers as it helps them to improve product safety and minimise liability risks. However, not only does ISO 26262 help to ensure vehicles, systems and components are safe, it will also enhance your reputation as a premium quality OEM or supplier, improving the appeal of your

products and helping you to remain competitive.

TÜV SÜD has a global network of automotive functional safety experts with extensive industry experience who are ready to support your business with ISO 26262 activities. As an internationally accredited ISO 26262 testing body, TÜV SÜD is

one of the world's leading experts on functional safety and a founding participant in the establishment of the ISO 26262 standard. We can provide a comprehensive range of knowledge services, functional safety assessment, testing, certification and training services throughout the entire automotive value chain.

COPYRIGHT NOTICE

The information contained in this document represents the current view of TÜV SÜD on the issues discussed as of the date of publication. Because TÜV SÜD must respond to changing market conditions, it should not be interpreted to be a commitment on the part of TÜV SÜD, and TÜV SÜD cannot guarantee the accuracy of any information presented after the date of publication.

This White Paper is for informational purposes only. TÜV SÜD makes no warranties, express, implied or statutory, as to the information in this document. Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of TÜV SÜD. TÜV SÜD may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from TÜV SÜD, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property. ANY REPRODUCTION, ADAPTATION OR TRANSLATION OF THIS DOCUMENT WITHOUT PRIOR WRITTEN PERMISSION IS PROHIBITED, EXCEPT AS ALLOWED UNDER THE COPYRIGHT LAWS. © TÜV SÜD Group – 2019 – All rights reserved - TÜV SÜD is a registered trademark of TÜV SÜD Group

DISCLAIMER

All reasonable measures have been taken to ensure the quality, reliability, and accuracy of the information in the content. However, TÜV SÜD is not responsible for the third-party content contained in this publication. TÜV SÜD makes no warranties or representations, expressed or implied, as to the accuracy or completeness of information contained in this publication. This publication is intended to provide general information on a particular subject or subjects and is not an exhaustive treatment of such subject(s). Accordingly, the information in this publication is not intended to constitute consulting or professional advice or services. If you are seeking advice on any matters relating to information in this publication, you should – where appropriate – contact us directly with your specific query or seek advice from qualified professional people. TÜV SÜD ensures that the provision of its services meets independence, impartiality and objectivity requirements. The information contained in this publication may not be copied, quoted, or referred to in any other publication or materials without the prior written consent of TÜV SÜD. All rights reserved © 2019 TÜV SÜD.



Find out more about TÜV SÜD's automotive solutions

www.tuvsud.com/automotive

automotive@tuvsud.com

Add value. Inspire trust.

TÜV SÜD is a trusted partner of choice for safety, security and sustainability solutions. It specialises in testing, certification, auditing and advisory services. Since 1866, the company has remained committed to its purpose of enabling progress by protecting people, the environment and assets from technology-related risks. Through more than 24,000 employees across over 1,000 locations, it adds value to customers and partners by enabling market access and managing risks. By anticipating technological developments and facilitating change, TÜV SÜD inspires trust in a physical and digital world to create a safer and more sustainable future.

TÜV SÜD AG
Westendstr. 199
80686 Munich Germany
+49 89 5791 0
www.tuvsud.com