Functional safety for a digital world

Smart solutions from chip design to whole system design

Add value.
Inspire trust.

White paper

Abstract

As digitalisation and automation progress, electrical, electronic or programmable electronic systems (E/E/PES) are used increasingly in the field of safety applications. Growing complexity and connectivity bring new requirements for the functional safety of systems and power plant technology, with previously separate applications growing closer together. Given this, interdisciplinary expertise is increasingly important to ensure safety and dependability of systems. As a result, new applications of functional safety are emerging, such as collaborative robots which work hand in hand with humans.

These trends are also reflected at standardisation level. Current standards provide starting-points for implementing the new demands when realising safety requirements. This TÜV SÜD white paper summarises the current trends and challenges and also provides an overview of the opportunities offered by functional safety. Third-party audits and testing throughout the design and development phases play a critical role across all applications. This topic will be of interest to the manufacturers of systems, components and machines and the owners or managers of industrial plants and infrastructure.

Contents

1 INTRODUCTION 3

2 TRENDS AND CHALLENGES IN FUNCTIONAL SAFETY 4

Modern semiconductors with safety features 4

Stricter requirements – an opportunity for the medical-device industry 5

Machine industry: A paradigm shift in protection strategy 6

Lifting devices for highest demands in nuclear engineering 7

Revised standards for combustion systems 8

Safety instrumented systems in the process industry 9

Continuously improved signalling systems for the rail industry 10

Industrial IT security in plant engineering 11

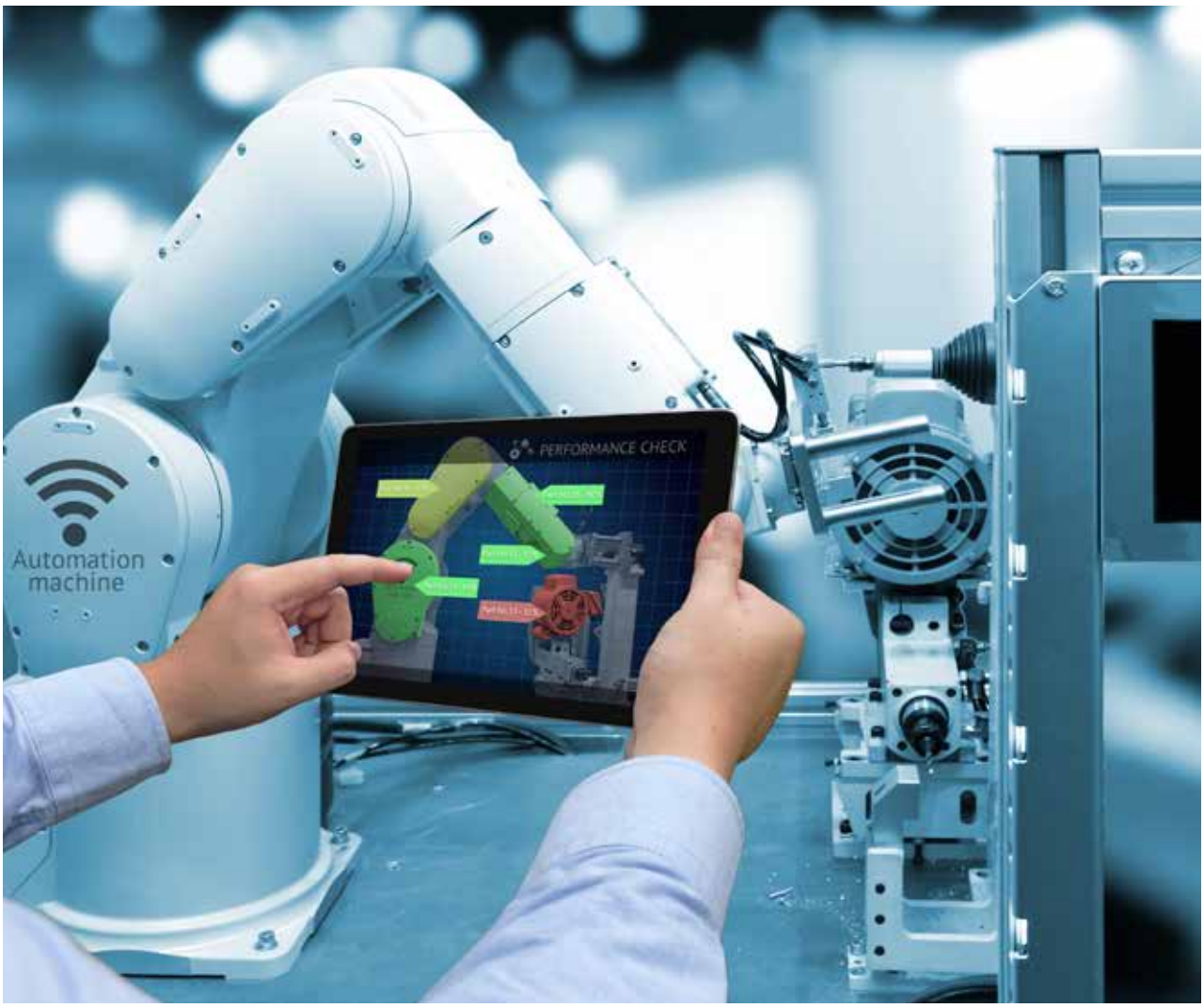
Functional safety as a management responsibility 12

3 CONCLUSION 13

1. Introduction

The tradition of functional safety dates back to the 1970s, when an uncontrolled reaction from over-heating caused a major dioxin leak at the Seveso chemical plant in the north of Italy. This event led to stricter industrial safety regulations that formed the basis for international standards. Functional safety has become a critically important issue across all areas of industry, from transportation, healthcare and medical devices to the design of power plants or amusement parks and rides. As a result, manufacturers and operators place top priority on the quality and safety of products and plants in order to protect people, property and the environment against technology-related risk.

As new applications develop and become increasingly interconnected, the landscape of standardisation is changing. An excellent example of this is the field of collaborative robotics, in which man and machine work hand in hand. This innovative field requires a holistic approach to functional safety, emphasising the need for expertise and years of experience in both application-specific and generic systems. Other projects require expertise in various application fields across all project phases, from design and development to manufacturing and installation, testing, certification, placing into service and decommissioning.
Given this, testing and certification organisations need to provide holistic and international services that enable them to offer owners, managers and manufacturers one-stop multi-disciplinary support and comprehensive assistance with international approval services.



2. Trends and challenges in functional safety

Modern semiconductors with safety features

"Challenges in the field of semiconductors are short innovation cycles and increasing integration density. Ensuring that standards reflect the state of the art is one of these challenges."

Matthias Ramold
Global Head Functional Safety
TÜV SÜD Rail

The main requirement for complex semiconductors to be used in functionally safe embedded systems is a high degree of miniaturisation with the goal of reducing area and cost. Furthermore, modern design requires compatibility, reusability and embedded safety features. This leads to µCs, FPGAs and ASICs with safety mechanisms already implemented on-chip like lockstep architectures or memory integrity measures. The challenges in this domain are short innovation cycles, high degree of design complexity and increasing integration density.

These aspects have a massive impact on the assessment of functional safety of such devices. For example, new fault models caused by new technologies have to be regarded. Especially for Systems-on-Chip (SoC), dependent faults have to be evaluated. Already known failure modes like transient failures take on increased relevance in the context of integration of smaller structures.

In addition, adequate verification approaches showing the effectiveness of safety measures have to be developed. Due to the massively increasing complexity, a high quality development and lifecycle process is required to ensure a low level of systematic faults. Finally, great care has to be taken when generating the user documentation with respect to completeness of system integration. Therefore, the generic normative requirements have to be interpreted and extended based on the current state of the art and the specific technology.

The assessment of design and manufacturing processes is another key factor in avoiding the consequences of systematic faults. In addition to the above, the users of semiconductor components need informative and complete documentation to realise safe and straightforward system design. All these demands require comprehensive expertise.

Stricter requirements – an opportunity for the medical-device industry

"Functional safety benefits not only patients and users. Manufacturers also avoid conformity-related problems and benefit from shorter time to market."

Dr Royth von Hahn
TÜV SÜD
Product Service

Medical devices are among the most heavily regulated products in the world. Faults can have serious consequences for patients and users. In contrast to most other safety-relevant sectors of industry, there is no explicit definition of functional safety for medical devices. Nevertheless, regulations and standards lay down a number of requirements that can only be fulfilled by applying the principles and methods of functional safety. These can be found in the relevant standards on electrical safety and software, including IEC 60601-1 "Medical electrical equipment – Part 1: General requirements for basic safety and essential performance" and application-specific particular standards and software standard IEC 62304 "Medical device software – Software life cycle processes".

The standards require hazards to be assessed with patients and users in mind. This concerns the function of a medical device or the software that controls the medical device respectively. For high-risk devices, the regulations and standards require specific safety systems that keep the probability of a fault or the severity of its consequences to a minimum. These systems are protected against faults with the help of functional safety methods. Medical engineering also increasingly relies on systems controlled and monitored by microprocessors and software. Digitalisation and connectivity not only raise the significance of functional safety; they also offer economic opportunities. Safe product design, early avoidance of conformity-related problems, fewer product recalls and shorter time to market are only some of the examples of the potential offered.

Machine industry: A paradigm shift in protection strategy

"Mechanical engineering is undergoing a paradigm shift: Where machines used to be operated behind safety fences in the past, collaboration is now possible."

Christian Eberle
TÜV SÜD
Industrie Service

In the machine industry, the significance of functional safety has increased continuously. In this sector, the focus of interest has always been the safety of operating and maintenance staff. The other goal has been to minimise the costs of operation and servicing or maintenance. Consequently, machine manufacturing and operation are subject to a host of regulations and requirements. Machinery manufacturers must show compliance with the European Machinery Directive 2006/42/EC. The harmonised standards EN ISO 13849, Parts 1 and 2 and EN 62061 can be used to reach this compliance in the field of functional safety.

In recent years, the requirements imposed on machines and machine systems have grown more comprehensive and complex, a trend that is again the result of advancing digitalisation and the increased use of electrical, electronic or programmable electronic systems (E/E/PES). These technologies have contributed significantly to more efficiency and a higher degree of automation – also in terms of improved operability and profitability. The safety systems must be aligned to these more versatile and more complex applications. In the past, dangerous movements of machines for example were reliably stopped on opening of one of the monitored access doors in the safety fence. The paradigm shift away from prevention of access and the reliable shutdown of machines to the reliable identification of people and continued operation is underway. Due to this trend both possible damage events and the safety-related parts of control systems have become more complex. One example is the collaboration of man and machine, which offers enormous potential for improving efficiency.

Lifting devices for highest demands in nuclear engineering

"Deterministic design principles in nuclear engineering require dissimilar redundant systems and various principles of measurement."

Cornelia Bühler
TÜV SÜD Industrie Service

The demands that functional safety makes on lifting and material-handling equipment depends on various factors including their specific use. In conventional sectors of industry, safety-related requirements follow from the EU Machinery Directive 2006/42/EC. These requirements are complemented by the standards of the German Institutions for Statutory Accident Insurance and Prevention, in particular DGUV standard 52 Cranes (previously BGV D 6).

Lifting equipment used for safety-relevant material handling in nuclear power stations are based on nuclear safety standards, such as KTA 3902 "Design of lifting equipment in nuclear power plants". In principle, the requirements of this standard build on conventional standards, in particular ISO 13849. KTA standard 3902 includes requirements that go beyond the provisions of this conventional standard, including a list of all necessary safety functions of a lifting device and the required performance level (PL) according to ISO 13849-1. In this context, the PLs established for the individual safety functions depend on the risk involved and the potential extent of radioactive release in case of an assumed functional failure. ISO 13849 thus defines the basically applicable requirements to be used in nuclear engineering for actions taken to identify and control random faults. However, the actions to prevent systematic errors or common cause failure required in ISO 13849 only refer to quality assurance and aim at preventing certain faults in design and development and manufacturing. They do not in all cases satisfy the deterministic design principles of nuclear engineering. There, individual safety functions may have higher safety-related significance, as their failure may result in violation of nuclear safety targets.

According to KTA 3902, these functions require two redundant and dissimilar safety devices to ensure reliable control of systematic faults. In this context, at least one of the two safety devices must comply with PL e (or SIL 3 as applicable). For the second safety device, PL c will be sufficient. In practice, this requirement is fulfilled by using two control systems made by different manufacturers. In addition, different principles of measurement are used for determining the conditions of the lifting equipment that are subject to monitoring.

Revised standards for combustion systems

"There are various ways of implementing functional safety requirements for manufacturers, owners and managers of industrial combustion systems."

Johannes Steiglechner
TÜV SÜD
Industrie Service

Industrial combustion systems, such as thermal process plants, are designed and manufactured to match their specific applications. Functional safety systems are used to monitor combustion processes and prevent critical plant conditions. Decades of experience in the realisation of safety functions by means of hard-wired circuits combined with qualified safety devices and equipment is available, ensuring sufficient control of the fault models defined in the relevant technical standards.

There has been a rise in the percentage of combustion systems using both sensors and actuators which are approved for SIL- or PL-classified safety functions and circuitry via a freely programmable safety controller. The design of these safety systems requires a systematic approach in order to reach and verify the safety integrity level of this specific application. This requires expertise in functional safety, but also familiarity with process-engineering processes and their behaviour, in particular with respect to existing operating conditions and fault tolerant time.

Current standards pursue the approach of evaluating the application-specific design of a safety function under consideration of the strategy used. Examples include EN 746-2 for combustion and fuel-handling systems and its counterpart, the recently published ISO 13577-2 international standard in conjunction with ISO 13577-4. EN 50156-1 on the electrical equipment for furnaces provides for a similar approach, in which safety devices and subsystems must comply to EN 50156-2.

This gives plant manufacturers, owners and managers the possibility to design safety functions with hard-wired safety devices and equipment that are approved and qualified according to technical standards. However, they can also choose to use freely programmable safety instrumented systems with sensors and actuators. Within the scope of the framework defined by the relevant specialist standards, these two options allow stakeholders to find the best possible solution for the realisation of safety functions.

Safety instrumented systems in the process industry

"The impartiality and independence of the teams designing and assessing the functional safety of the SIS are key."

Christian Zauner
TÜV SÜD Industrie Service

The process industry frequently uses gases and fluids which may pose significant risks to people and the environment if they are discharged. Safety instrumented systems (SIS) help to prevent these damage events and limit their consequences. Compliance with the requirements of the relevant standards is critical for ensuring SIS reliability.
It is fundamentally based on the safety life cycle as defined in EN 61508, Parts 1-4 and EN 61511, Parts 1-3.

Chemical reactions in the process industry frequently run under high pressure and high temperatures. Examples include vessels such as separating reactors or distillation columns. Pressures that exceed the design pressure of these vessels will activate any mechanical overpressure valves to avoid bursting of the vessel. However, this causes some of the hazardous gases and acids in the vessel to be discharged. Given this, measures must be taken to ensure that such a discharge can be realised safely. Apart from this, the loss of some of the contents of the vessel also means a loss in sellable product plus plant downtime. SIS can reduce the probability of overpressure in the vessel to an acceptable level, thereby significantly reducing the technical efforts and costs of ensuring safe discharge of vessel contents.

In step one of this improvement, the experts define possible damage events and their probability of occurrence. They also determine which process parameters must be monitored and at which quality, and how to respond when certain defined limits are reached. This is done within the framework of hazard and risk assessment, which includes relevant safety goals. When the maximum permissible pressure is reached in the vessel, the SIS will shut off filling or heating of the vessels and thus reduce the probability of overpressure to a tolerable residual risk. SIS comprise sensors, a logic unit and actuators, which must be aligned to the specific fault-prevention and fault-control measures on hand. This applies to both individual components and their interactions.

One basic requirement of the relevant standards is the establishment of a functional safety management system. This applies to all stakeholders in the safety life cycle, including plant owners, managers, plant builders and component suppliers. The impartiality and independence of the teams designing and assessing the functional safety of the SIS are key. Suppliers, operators and plant builders who work with third-party expert teams not only fulfil their responsibilities; they also document impartiality in the design and testing of new plants and the modification of existing ones, establishing their compliance with all legal requirements and thereby minimising the costs and efforts of possible follow-up measures.

Continuously improved signalling systems for the rail industry

"By focusing on effective action to prevent systematic faults, we are significantly improving the safety of signalling systems."

Sven Nowak
TÜV SÜD Rail

Technological progress does not stop at rail signalling systems. This means that traditional mechanical and electromechanical systems are gradually being modernised and replaced by modern microelectronics. The increasing complexity of the systems generally results in a higher probability of faults. In conventional mechanical and electromechanical systems, failures and failure effects are generally deterministic. The systems can be fully tested. However, due to the introduction of modern microelectronics and the increasingly widespread dependence on software this is now only possible to a limited extent. In case of faults in particular, the behaviour of signalling systems is more difficult to control. Reliable use of these modern systems requires the development of suitable actions that can be described with the help of standards.

The key standards on functional safety in the EN 5012X series address the problem by taking a risk-based approach. They define tolerable hazard rates for systematic and random faults as a benchmark of failure safety. Qualitative targets in the form of safety integrity levels (SILs) provide a classification value, which determines the technologies and actions that must be used to limit systematic faults. Quantitative targets, by contrast, cover failure probability for random faults in the form of a numeric fault rate. Random hardware faults must be analysed to prove that qualitative safety goals will be reached even in case of a fault. Systematic faults should be prevented to the degree required by the relevant safety integrity level (SIL).

This is done by a pronounced process focus combined with selected measures and methods.

To reach the safety goal, the actions taken should be well balanced. This applies to both prevention of failure causes and management of possible effects. Studies prove that the majority of risks in signalling systems result from systematic faults which safety analyses failed to identify, examine in detail or assess correctly.

This also applies to the consequences of these risks and any counteractions taken. Random hardware failures, by contrast, are in the one-digit percentage range.

To significantly improve the safety of a signalling system, the focus has to be on the effectiveness of actions that prevent systematic faults throughout the signalling systems' life cycle.

Industrial IT security in plant engineering

"As automation and connectivity grow, we face an increasing need to consider issues of industrial IT security in functional safety."

Karsten Klingler
TÜV SÜD
Industrie Service

For many years, power stations have applied a deterministic approach to functional safety. This approach has been included in the Technical Rules for Steam Boilers 411, 412, 413 and the pertinent technical rules of the 604 series as well as DDA 1001 recommendations. The codes describe in detail the system redundancies that must be realised to reduce the initial risk based on different modes of operation. The currently valid standard for furnaces in power stations or steam generators and similar systems, EN 50156, adopted the defined redundancies directly and merely aligned them to the new terminology (hardware fault tolerance, HFT).
The most informative example in this context is probably the structural requirements for non-type-approved limiting devices. These requirements were adopted practically unchanged from the TRDs. The key changes concern the addition of further combinations and detailed information (test cycles and level of diagnostic cover) which have been made more relevant by the probabilistic approach of the fundamental standards of functional safety (EN 61508 and EN 61511 with the German sub-standard VDE/VDI 2180).

As Germany and other countries pursue the energy transition, connectivity of power stations will become significantly more important in the future. One of the results will be a higher level of automation in power stations to allow for their remote control and monitoring.
The significance of functional safety for these functions of direct surveillance will continue to rise. However, remote monitoring and control raises another safety-relevant problem. As control systems are connected to the Internet, they must be protected against access by unauthorised third parties.
The significance of these new challenges will rise over the coming years. The new IEC standard 62443 faces these challenges at both the system and management level and at device level. The standard offers an integrated approach to ensuring the IT security of systems, network security and system integrity. It allows organisations to comb their control and process systems for potential vulnerabilities and develop effective actions to protect them.
The standard focuses on the IT security of industrial automation and control systems (IACS). These systems are needed to ensure the reliable and secure operation of automated systems and infrastructures.

Functional safety as a management responsibility

"Responsibility for functional safety does not rest with the suppliers alone; the owners share in this responsibility. Management is responsible for establishing effective processes."

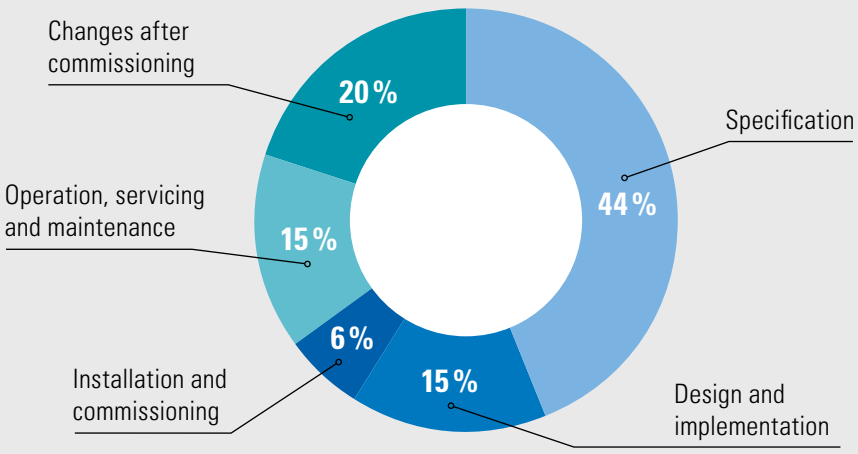
Dr Rolf Zöllner
TÜV SÜD Industrie Service

Organisations and people have the responsibility of realising functionally safe products and systems. Implementation of the many different requirements of functional safety thus requires a management framework which regulates the processes and organisation of the activities to be performed. Given this, functional safety management (FSM) is a key element of relevant functional safety standards.

This includes the definition of the roles and tasks of the individuals involved, proof of their competence and the qualification measures necessary to ensure up-to-date knowledge. Further elements that must be defined within the scope of the safety life cycle include the type and scope of the required documentation and quality assurance. This spans the preparation of documented procedures, work instructions and checklists as well as official signature authorisations. Recording of field experience must also be regulated, as must modification and configuration management.

FSM has numerous interfaces with the higher-level quality management system which is typically in place. These interfaces must be given special attention. It has proved good practice, for example, to define the responsibilities of the individual parties clearly and early in the quotation phase. The reason is that functional safety is not the responsibility of the component or system supplier alone but also that of the future owner of these systems.

WHAT IS THE CAUSE OF A FAULT?



The pie chart shows the various phases of the safety-life cycle in clockwise order. Faults causing accidents or incidents are allocated to these phases based on their frequency.

3. Conclusion

Growing digitalisation and automation across all areas of life and industry not only increase the significance of functional safety and industrial IT security; it also offers economic opportunities. Safe product design, early prevention of conformity-related problems, fewer product recalls and shorter time to market are some examples. Manufacturers and owners can best use these opportunities by establishing a systematic process focus, including consideration of the entire system life cycle, and by calling in the support of a third-party partner at an early stage, ideally in the development phase.

TÜV SÜD experts develop methods which can be used to verify the effectiveness of safety and security measures. Thereby the robustness of components as well as the complete life cycle, including the development process are taken into account in the assessment. These actions are aimed at ensuring maximum prevention of systematic faults. In addition, TÜV SÜD experts pay special attention to user documentation, which enables easy and safe system integration. TÜV SÜD also supports manufacturers and operators when placing their products on the market, during operation and when changing machines and machine systems. By working together with TÜV SÜD's functional safety experts to perform the assessment, manufacturers and owners fulfil their responsibility of verifying impartial and independent design and testing when building new plants and changing existing plants.

The increasing connectivity of systems and plants plus the growing possibilities of remote control further require suitable approaches to protect systems against unauthorised access and safety-relevant manipulation of the safety functions embedded in hardware and software. TÜV SÜD provides the relevant tests and certifications for manufacturers according to IEC 62443-4-1 and for system integrators according to IEC 62443-2-4.

TÜV SÜD offers long-standing experience and an excellent international reputation in functional safety. Building on this, the multi-disciplinary team of experts pursue an integrated approach – from chip design to inspection of entire plants. This enables comprehensive cross-industry assessment and assurance of the complex functional safety requirements.

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 – 2018 – 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 © 2018 TÜV SÜD.

Find out more about TÜV SÜD's functional safety services

www.tuvsud.com/functional-safety
functional-safety@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 founding principle of enabling progress by protecting people, the environment and assets from technology-related risks. Through 24,000 employees across 1,000 locations, it adds tangible value to customers and partners by enabling market access and managing risks. By anticipating technological developments and facilitating change, TÜV SÜD inspires trust in the 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

2018 © TÜV SÜD AG | MKG/RL/18.1/en/DE