ptc

DIGITAL TRANSFORMS PHYSICAL

Automotive Functional Safety & ISO 26262 Compliance

Introduction

Automotive technology is developing at a breakneck speed, and market analysts agree that the mobility industry is ripe for disruption. This prompts regulators, OEMs, and automotive suppliers worldwide to step up their system safety engineering efforts in order to make sure that despite the pace of development, no necks are broken once these new technologies hit the road.

This guide provides fundamental information to help automotive development companies (OEMs, suppliers, and other stakeholders) ensure their products' functional safety and achieve compliance with both current and future regulations in the automotive industry.

Established carmakers understand both the need and the means to build hardware that functions as expected in all operational conditions and which ultimately helps keep our roads safe. But in addition to evolving hardware, the development of modern mobility solutions and vehicles is more and more reliant on electrical and/or electronic systems and especially software. Ensuring the functional safety of these constantly evolving software systems, and their safe operation with hardware components, is an ongoing challenge.

In addition, the processing of digital (visual data via cameras, radar, LiDAR data, etc) information, Artificial Intelligence, vehicle-to-vehicle connectivity, ADAS (Advanced Driver Assistant Systems), and fully autonomous driving all require new competences that traditional carmakers historically lack.

Building on their software competences, new and non-traditional technology companies (such as Google, Lyft, Uber, Baidu, etc) are entering the automotive market, whether they choose to partner or compete with established carmakers. This increases market competition and a drive for innovation in the automotive industry.

In this pre-disruption flurry of modern technologies and new automotive developers, governments and regulatory bodies are looking to tighten the standards governing the safety and reliability of tomorrow's vehicles. Ensuring functional safety is becoming a crucial aspect of the development of automotive embedded systems for both OEMs and their suppliers.

Market trends shaping the automotive industry

To grasp current and emerging challenges of ensuring functional safety in today's (and tomorrow's) vehicles, we must first understand the most important market trends that are shaping the mobility industry today.

Modularization, granularly segmented product lines

Market demand for product customization is growing. Increasing granularity in terms of target groups means that car manufacturers have to face the challenge of modularization and product variants management. Different user groups increasingly prefer vehicles geared towards their specific needs, creating niche market demands.

This, of course, brings the challenge of managing the development of diverse product lines with multiple product variants. Numerous modules may be built on the same platform (vehicle architecture) in various models. This results in increased product complexity, but also allows auto developers to reuse certain components in different models.

Carmakers need to equip themselves with adequate variants management capabilities and tools that enable them to ensure functional safety across multiple product variants with optimal effort.

Changes in consumer preferences & Shared mobility

Despite modularization allowing automotive developers to satisfy niche market needs, the signs of declining car ownership are already apparent. Technologies to support carsharing are hugely successful, sharing culture is on the rise, and a growing number of mobility providers aim to deliver on-demand car rental services. McKinsey forecasts that as soon as in 2030, 1 out of 10 cars sold could be a shared vehicle. As autonomous driving technology matures into everyday use, car ownership should dwindle further.

Shared mobility presents a host of new challenges in terms of functional safety that auto developers and mobility service providers need to prepare for.

Changing automotive value chains

In this shifting market landscape, carmakers will have to redefine their role in the auto industry. Players involved in the development of autonomous technology are now drawing closer, taking advantage of each other's strengths and capabilities.

Partnerships have already been established in recent years between tech companies with a solid proficiency in software engineering and traditional carmakers with an expertise in building high quality vehicles.

The multi-tier ecosystem that characterizes the auto industry is therefore getting more and more complex. In the race to delivering safe and reliable fully autonomous vehicles to the market, there is a growing need to facilitate the collaboration between internal and external stakeholders across the automotive value chain.

In addition to the business management aspects, this process also introduces a technical and tooling issue. Traceability across software and functional safety requirements, development, Quality Assurance & testing, bug management, and continuous improvement with OTA (over-the-air) updates will have to be ensured to enable compliance with increasingly stringent automotive standards.

Electrification & connectivity in the mobility industry

After the emissions scandal, most major carmakers have announced increased focus on electric powertrains, and while they won't fully replace traditional combustion engines in the near future, EV technology is expected to grow further. The sale of fully electric cars was up 47% in 2017, and in Nov 2017, Bloomberg reported a 63% jump in global sales (mainly due to China's efforts to reduce pollution, with Europe being the second-biggest market).

Electric vehicles, connectivity, and autonomous driving work hand in hand to deliver the future of mobility, leading to synergies in the development of these technologies. EVs are easier for computers to drive, while, V2V (vehicle-to-vehicle) communication will be a crucial enabler of fully self-driving technology.

Electric powertrains and connected vehicles add to the functional safety (and data security) challenges awaiting carmakers in coming years.

Autonomous driving

As the most important automotive innovation in the last decade, autonomous technology is still the number one factor expected to shape the industry's future. Most innovative research & development in the auto industry today is already focused on enabling self-driving transport, which is expected to completely redefine the mobility sector.

New driver-assisting (ADAS) solutions are already gradually seeping down into everyday vehicles, and the fast development of Artificial Intelligence and related technologies is expected to make fully autonomous cars a reality by 2020.

The functional safety challenges of self-driving cars are many and can't all be foreseen, but are becoming the number one concern of automotive developers worldwide as the mobility industry evolves.

Tightening regulatory landscape

In addition to tech challenges, building confidence in autonomous technology also takes considerable time. Regulatory bodies and consumers alike are slowly adapting to the idea of driverless cars, regardless of assurances that autonomous vehicles communicating via the IoT will actually be much safer than human-driven ones. Regulation around self-driving vehicles remains unclear, and testing is still confined to specific areas and closed test tracks.

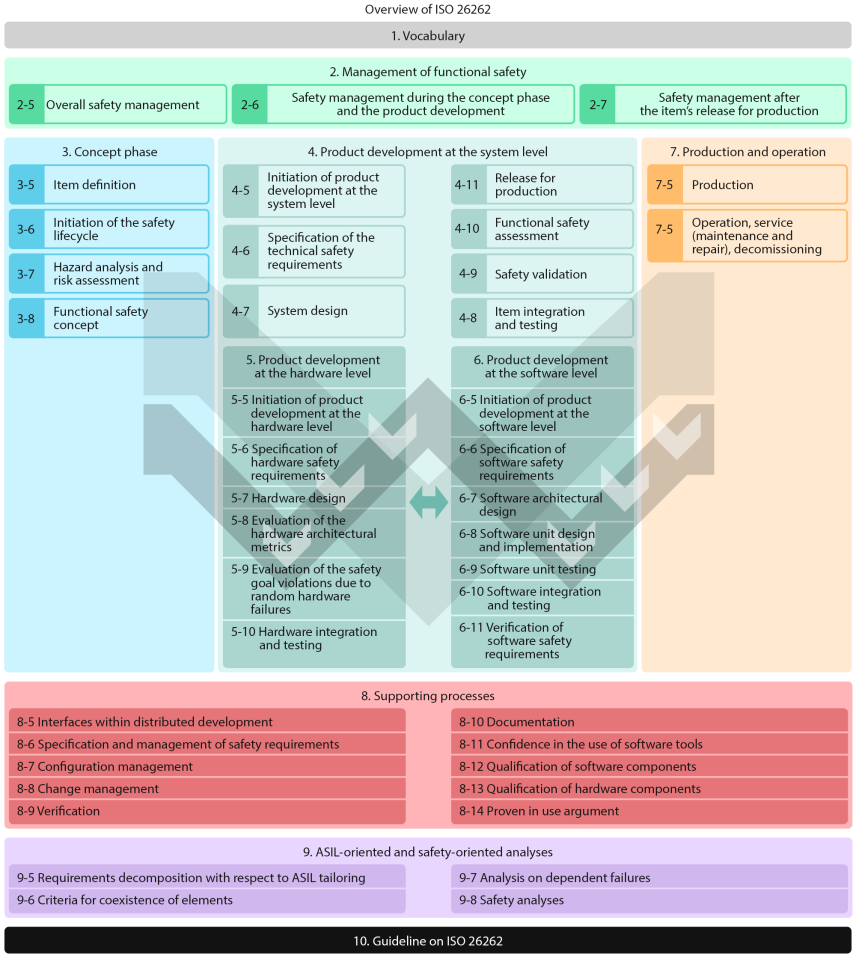
Regulators are hard at work to devise comprehensive standards to govern the functional safety requirements of modern automotive technology. Carmakers and suppliers have to prepare for increasingly stringent regulations that their products currently under development will have to comply with.

Functional Safety in Automotive Development & ISO 26262

All these changes shaping the mobility industry have a significant impact on functional safety. As automotive systems get more and more sophisticated, addressing the requirements of evolving functional safety standards is becoming more and more challenging. There is a growing need for safe systems development processes, and automotive companies (OEMs and suppliers alike) will need to find ways to provide evidence that they took all reasonable measures to satisfy system safety objectives during the development of their products.

In the automotive industry, the most important safety standard is ISO/DIS 26262. Titled Road vehicles – Functional safety, this regulation is the international ISO standard governing the functional safety requirements of electrical, electronic, and programmable electronic systems in production vehicles.

ISO 26262 covers the product (E/E hardware and software) lifecycle processes to be implemented to ensure functional safety. The standard defines functional safety as "The absence of unreasonable risk due to hazards caused by malfunctioning behaviour of electrical / electronic (E/E) systems". ►



Source: ISO 26262-1:2011(en) https://www.iso.org/obp/ui/#iso:std:iso:26262:-1:ed-1:v1:en:term:1.120

ISO 26262 provides terminology to remove ambiguity, a set of target metrics, and guidance on making sure that automotive (E/E and software) systems operate safely even in situations when a system component fails.

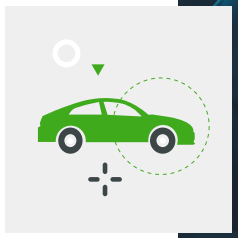
As the most widely applied international standard on automotive functional safety, ISO 26262 largely determines how automotive products are designed, developed, integrated and validated for safety in 2018.

ISO 26262 is in fact an adaptation of the general standard IEC 61508 and therefore applies a similar risk-based approach to functional safety. The standard calls for the assessment of risks of any hazardous situation, and requires its users to plan, document, and take safety measures that help avoid, detect, control, or mitigate the effects of both systematic and random hardware failures.

The standard defines an automotive safety lifecycle that encompasses the engineering/development, production, management, operation, service, and decommissioning of automotive products. Its risk-based concept helps users determine integrity levels (ASIL – Automotive Safety Integrity Levels) which in turn define what parts of ISO 26262 are applicable.

In addition to specifying the requirements to help avoid unreasonable (and therefore unacceptable) residual risk, the standard provides requirements for the documentation, validation and confirmation measures to prove that acceptable safety levels have been achieved. Finally, ISO 26262 also provides guidance on managing supplier relations.

Part 2 of ISO 26262 specifies requirements for the management of functional safety in the organization. It defines functional safety rules and processes, but also the means to determine and prove the competence and qualification of those team members carrying out functional safety activities. It also covers the evidence of a sound quality management system that helps achieve functional safety of the end product.



ISO 26262 Vocabulary

ISO 26262 specifies a set of terms and definitions to remove ambiguity in the management of functional safety. Some of the key items of terminology as provided in the standard are the following:

Item
System or array of systems to implement a function at the vehicle level, to which ISO 26262 is applied

Functional safety
Absence of unreasonable risk due to hazards caused by malfunctioning behaviour of E/E systems

Risk
Combination of the probability of occurrence of harm and the severity of that harm

Harm
Physical injury or damage to the health of persons

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

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

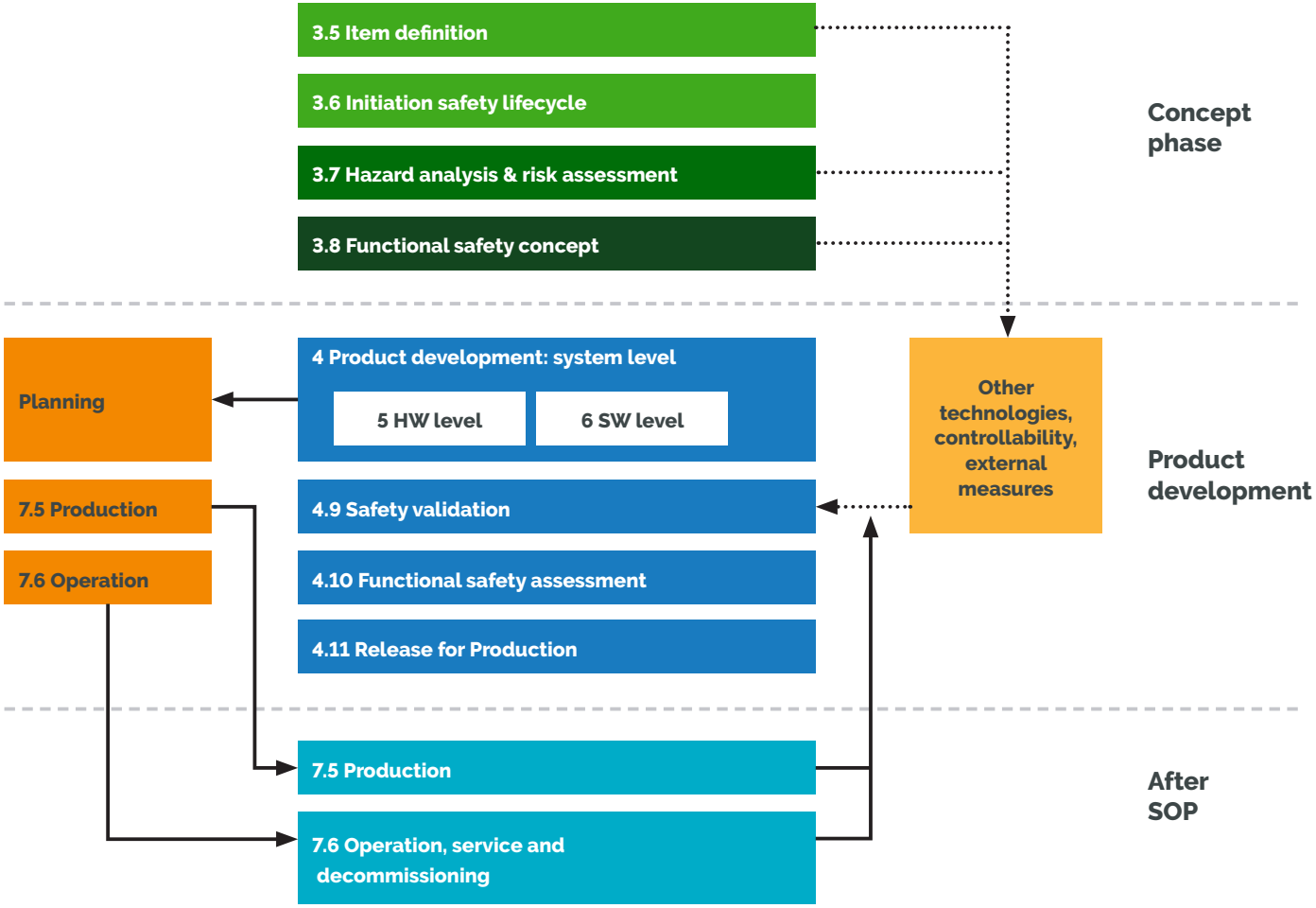
Safety measure
Activity or technical solution to avoid or control systematic failures and to detect random hardware failures or control random hardware failures, or mitigate their harmful effects

Systematic failure
Failure related in a deterministic way to a certain cause, that can only be eliminated by a change of the design or of the manufacturing process, operational procedures, documentation or other relevant factors

Random hardware failure
Failure that can occur unpredictably during the lifetime of a hardware element and that follows a probability distribution

ISO 26262 Functional Safety Lifecycle – Concept Phase

ISO 26262 is composed of 10 parts that provide a vocabulary, guidance on the management on functional safety, information on supporting processes, and guidelines on ASIL as well as the whole of the standard. Parts 3 through 7 break down the functional safety lifecycle into a Concept phase, a Product Development phase, and a post-SOP phase (this latter one basically translates to production and operation).



Source: https://www.kuglermaag.com/improvement-concepts/functional-safety-and-security.html

1. Item Definition

A functional safety lifecycle as defined by ISO 26262 begins with the identification of a product and the definition of its requirements. Of primary importance are the product's functional requirements, but their non-functional requirements, known safety requirements, relevant operating and environmental constraints are also defined. During this phase, functional analysis helps identify functional failures. All this information serves as input for the next step of the process, where a comprehensive list of hazards (potential hazardous events) is identified.

2. Hazard Analysis and Risk Assessment (HARA)

During HARA, conditions such as potential vehicle states (engine off, wheels rolling, etc), driving situations (city ride, parking, etc), environmental conditions (dry or wet road, etc), but also road surface conditions (tunnel, slope, deep water, etc) are taken into account to identify failures that could lead to hazardous situations.

Each combination of the above is analyzed and documented. Then, all hazards are evaluated and are assigned an ASIL (Automotive Safety Integrity Level) based on their Severity, Exposure and Controllability values. ISO 26262 provides an allocation table to help define the right ASIL value for each hazard.

Automotive Safety Integrity Levels (ASIL)

ASIL is ISO 26262's risk classification scheme which helps understand which safety requirements apply to specific hazards. Each hazard will be assigned one of four ASIL levels based on the Severity, Exposure and Controllability of the vehicle operating scenario. In ISO 26262, D represents the most stringent while A the least stringent level of safety integrity.

ASIL = Severity x (Exposure x Controllability)

Severity

Estimate of the extent of harm to one or more individuals that can occur in a potentially hazardous situation

Exposure

State of being in an operational situation that can be hazardous if coincident with the failure mode under analysis

Controllability

Ability to avoid a specified harm or damage through the timely reactions of the persons involved, possibly with support from external measures

Source: ISO 26262-1:2011(en) https://www.iso.org/obp/ui/#iso:std:iso:26262:-1:ed-1:v1:en:term:1.120

3. Safety Goals & Functional Safety Concept

Next, a safety goal will be determined for each hazardous event. These safety goals will inherit the underlying hazard's ASIL value, and will be used as an input for the Functional Safety Concept stage.

For each Safety Goal a Fault Tolerant Time Interval will be determined using, for instance, fault injection tests. FTTI refers to the timespan in which a fault can be present in a system before a hazardous event occurs. The system has to first detect and confirm the existence of the fault, then react to that fault to achieve safe state, all of which takes time. FTTI is used to describe the maximum duration within which the system has to achieve a safe state so as not to jeopardize safety goals.

Safety Goals will generate Functional Safety Requirements based on architectural assumptions. One system element can receive Functional Safety Requirements from more Safety Goals, in this case the highest ASIL shall apply. On this level safety mechanisms and safe states on system level are already defined so the first Functional Safety Concept is known.

ISO 26262 Functional Safety Lifecycle – Product Development Phase

Chapter 4 of ISO 26262 deals with product development at the system level, including the identification and planning of safety activities throughout the development lifecycle. It covers both the methods to be used and supporting activities, as well as the identification and refinement of technical safety requirements.

The input for these technical safety requirements are the functional safety requirements which in turn take into account the preliminary analysis of the product's architecture. Therefore, they help develop a safe system design and a define technical safety concept which should then be verified.

The terms "verification" and "validation" are often used interchangeably, but ISO 26262 makes a clear distinction. During item integration and testing, ISO 26262 requires developers to integrate and test an item for compliance, verifying that it correctly implements the system design considered functionally safe. Validation, on the other hand, is the next step of the process that takes safety goals as its basis.

In the context of ISO 26262, validation refers to the activities that aim to provide evidence that the defined safety goals are correct, complete, and fully achieved (not on the item but on the vehicle level). In other words, validation takes a step back and examines whether the safety objectives that were set are fit for purpose, whereas the goal of verification is simply to make sure the product actually adheres to those objectives.

Part 4 also covers the assessment of functional safety on the item level, and makes this the responsibility of the OEM (vehicle manufacturer). Finally, it requires adequate documentation of the vehicle's functional safety before it goes into production and is released.
Parts 5 and 6 specify requirements for product development on the hardware level and on the software level, respectively. These chapters follow a similar logic and describe a similar high-level process for HW and SW development.

First, they require the user of ISO 26262 to determine and plan functional safety activities with regards to HW/SW design, and to specify safety requirements based on these. After verifying that these requirements conform to those outlined by the technical safety concept, a hardware and software architectural design is created.

In both cases, the standards calls for the creation of a safety analysis report and a design verification report to analyze if the product conforms to the plan and the requirements specified by ISO 26262. Integration and (unit) testing should be carried out to prove the correct implementation of requirements, the product's robustness (or, in the case of hardware, an analysis of random failures), and the verification of design and safety requirements.

ISO 26262 Functional Safety Lifecycle – Production and Operation & Supporting Processes

Part 7 of the standard governs the production, operation, service, and decommissioning of the product.

In the case of hardware elements, this section defines requirements for the handling (production, transport and storage conditions) of the product. With regards to operations, ISO 26262 specifies objectives for the servicing (maintenance and repair), as well as the decommissioning of the product. This includes repair instructions and a maintenance plan, which of course can greatly impact the product's functional safety. The standard explicitly calls for the specification of requirements to maintain the product's functional safety over its lifecycle.

Supporting processes (covered by Chapter 8) include collaborative processes between the OEM and its suppliers. This section of ISO 26262 allocates responsibilities, and requires parties carrying out distributed development activities to specify a Development Interface Agreement (DIA).

DIA is vital to achieving the functional safety goals of a product where multiple parties are involved in its development. In essence, the Development Interface Agreement specifies not only what is expected of each party with regards to the product's development, but also how exactly to complete those requirements. ►

The DIA document should be created collaboratively so that all parties agree to it before development starts. It should be tailored to the needs of the project at hand, and should cover its scope in unambiguous and clear terms, with defined target values. In addition, the Development Interface Agreement should also be used as a basis to guide the creation of a safety plan and reviewed continuously throughout the development project.

Part 8 also specifies requirements on Configuration Management (including the traceability of relationships and differences between different versions of a product), and Change Management (a lifecycle-wide activity that aims to manage all changes to safety-related work items). This is also the chapter dealing with ISO 26262 compliance verification, including adequate documentation across the entire lifecycle, and the creation of a compliance report.

Chapter 9 provides further support on ASIL-oriented and safety-oriented analyses, including guidance on the coexistence of non-safety related and safety-related elements, their dependences, and the calculation of ASIL levels in such a scenario.

ISO 26262 Qualification of Software Tools & Components

ISO 26262 requires its users to qualify the software tools used during the product's development lifecycle for suitability.

Section 8-11 provides guidance on tool classification based on tool impact and tool detection. Based on these two values, a Tool Confidence Level (TCL 1-4) is calculated for each software tool that has possible functional safety implications.

The standard calls for the documentation of these tools and the creation of a tool qualification report, making this a difficult task for developers of automotive system components and end products.

Additionally, ISO 26262 contains requirements on the qualification of software components with the objective to facilitate the reuse of these items of development. Adhering to the requirements of the standard, certain software components that have already been engineered and developed in compliance with ISO 26262 may be re-used for increased efficiency. Adequate documentation and a qualification report permits the re-use of system software components while maintaining the already established compliance with the standard.

The standard also allows the use of the "proven in use" argumentation, essentially enabling developers to use this as an alternate means of compliance with ISO 26262. For instance when reusing a component of a product that is already compliant with the standard's requirements, a Proven in use analysis report (with adequate Proven in use credits) may be sufficient to establish compliance in the item's new environment, permitting the resource-efficient reuse of that specific component.

Codebeamer and its Templates

The growing complexity of today's automotive products and of their development processes necessitates the use of modern tools in automotive engineering.

With the growing reliance on software, traditional PLM tools that support the development of automotive hardware components seem to take a back seat. The importance of integrated Application Lifecycle Management tools is becoming evident as focus shifts to software-heavy embedded electronics architectures in automotive end products.

The necessity to analyze, manage, and document functional safety throughout the process of development introduces previously unheard of complexity to the automotive value stream. Smart software platforms are inevitable in order to ensure consistency, the traceability of functional safety efforts and other lifecycle data, and the use of mature development and functional safety processes throughout the automotive software lifecycle.

Due to its holistically integrated architecture and collaborative features, Codebeamer serves as a single source of truth to bridge the gaps in automotive development. The platform is TÜV-certified for compliance with IEC 61058 and ISO 26262, and supports the efficient alignment of engineering disciplines.

With rigorous process control and approval management features, versatile Quality Assurance & Testing functionality, and out-of-the-box capabilities to support risk management, Codebeamer is the go-to ALM tool for automotive innovators worldwide. It offers advanced analytics & reporting features to accelerate compliance audits, and provides baked-in best practices from global leaders in automotive technology.

References
https://www.mckinsey.com/industries/automotive-and-assembly/our-insights/disruptive-trends-that-will-transform-the-auto-industry / https://www.iso.org/obp/ui/#iso:std:iso:26262:-1:ed-1:v1:en / https://www.arm.com/files/pdf/The_Functional_Safety_Imperative_in_Automotive_Design.pdf / https://es.cs.uni-kl.de/publications/data/Kolh15.pdf / https://www.kuglermaag.com/improvement-concepts/functional-safety-and-security.html

Codebeamer's Automotive ISO 26262 & ASPICE Template

Our Automotive ISO 26262 & ASPICE Template leverages the advanced capabilities of Codebeamer to support the product development processes of automotive OEMs and suppliers. The template comes preconfigured with artifacts and workflows to enable its users to develop automotive end products in compliance with IEC 61508 and ISO 26262 up to ASIL D or SIL 3. It greatly simplifies adherence to the requirements of the Automotive SPICE and CMMI models.

Learn more

For developers using Codebeamer to accelerate the innovation of automotive technology, our Tool Validation Kits provide invaluable help in tackling the tool qualification requirements of ISO 26262. They contain all the assets relevant and necessary for qualifying Codebeamer for use in automotive development as per ISO 26262 specifications.

Learn more about the Tool Validation Kits by visiting our website.

TÜV NORD
TÜV NORD Systems GmbH & Co. KG
Trusted Tool

DIGITAL TRANSFORMS PHYSICAL

121 Seaport Blvd, Boston, MA 02210 : ptc.com

008-automotive-functional-safety-iso-26262-compliance–02-08