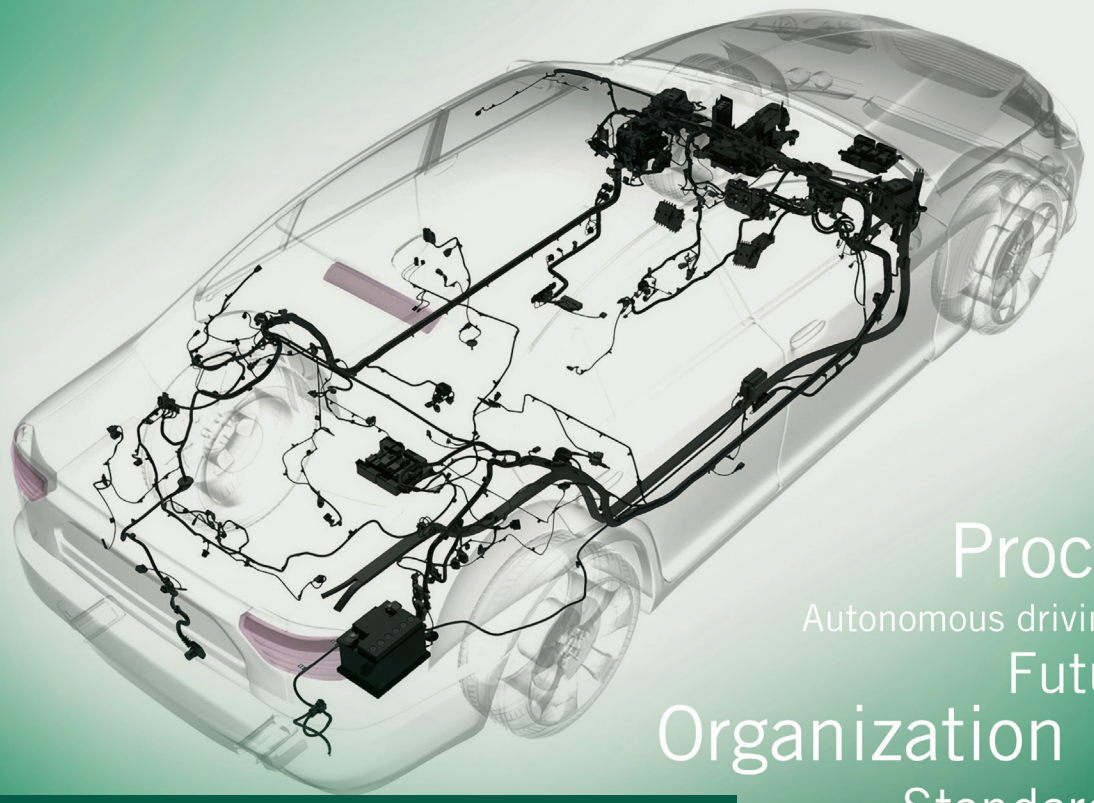


Processes
Autonomous driving
Future
Organization Efficiency
Standards

Rethinking
Functional Safety Requires Optimized Process Organization

Highly automated and autonomous driving is giving rise to new requirements in the automotive sector, particularly with regard to safety-relevant functions. But which means do we need to use to meet these challenges? One possible answer to this question lies in the non-trivial implementation of the ISO 26262 standard, as Dräxlmaier Dräxlmaier describes by the example of on-board electrical systems development.

EXPANDING ESTABLISHED STANDARDS

With the SAE level 3 "Conditional Automation", the next milestone in the field of autonomous driving is getting closer: so-called highly automated driving. This development step is accompanied by a major change in situational awareness while driving: Instead of the driver, this task is now taken over by a wide variety of sensors.

What this means for safety-related functions such as steering and braking is obvious: Here, the aspect of functional safety for the protection of passengers takes on even more importance. Bearing in mind that the SAE levels 4 and 5, which will soon follow, provide a still broader automation of driving features, safety is being pushed even further into focus, **FIGURE 1**.

In view of the complexity of today's on-board electrical systems, this leads to a significant increase of development expenses, because of the reduction in tolerance of any system errors. As good as today's quality and process management are, this is pushing them to their limits. For this reason, the standard ISO 26262:2011 was written, which will appear later this year in an updated version. It is essentially based on a V-model, which includes special requirements for implementation of the project, **FIGURE 2**.

While ISO 26262 is already applied in ECU development, the established processes currently provide no adequate solutions for responding to the challenges at the overall vehicle level and in terms of the entire electrical system. Automotive Spice, the standard com-

AUTHORS

Oliver Druhm
is Concept Development Team Leader for On-board Electrical Systems at the Dräxlmaier Group in Vilsbiburg (Germany).

Dr. Martin Gall
is CTO of the Dräxlmaier Group in Vilsbiburg (Germany).

Georg Scheidhammer
is Leader of the Ressort Strategy and Innovations in the Development Department of the Dräxlmaier Group in Vilsbiburg (Germany).

monly used in development, is essential for ensuring the functional safety of products. However, its requirements are not strict enough. The provisions of IATF 16949 go one step further – but only ISO 26262 ensures that the entire safety life cycle related to safety-relevant functions is taken into account. These include the development and production of downstream processes during the operating life; for example, in the areas of operation, service and decommissioning of the vehicle, **FIGURE 3**.

RELIABILITY IN FOCUS

To achieve a functional secure system at the end of the development process, it is of particular importance to identify possible sources of error in advance. For this purpose, two fault categories are distinguished: random errors and systematic errors.

Random errors are analyzed according to ISO 26262 based on their Failure-in-Time (FIT) rates and then evaluated. They basically serve to select the right materials and components. FIT rates were and are determined and set under predefined conditions. In addition, the corresponding use case is to be defined for usage in every project. Only then, and under the condition that the corresponding processes are respected for the custom FIT rates, this is valid for the overall system.

Systematic errors, however, can occur when designing, manufacturing or operating a system and are nearly always predictable. This distinguishes them from random errors.

Based on use cases, a hazard and risk assessment according to ISO 26262 reveals potential hazards and determines where risks must necessarily be reduced. To achieve the defined objectives, there are special instructions with which systematic errors and also random errors can be avoided. At the end of this process, a classification in the Automotive Safety Integrity Level (ASIL) is made. This assigns an FIT rates budget to the system under development and, at the same time, determines what action is to be taken.

PROCEDURAL TOOL BOXES

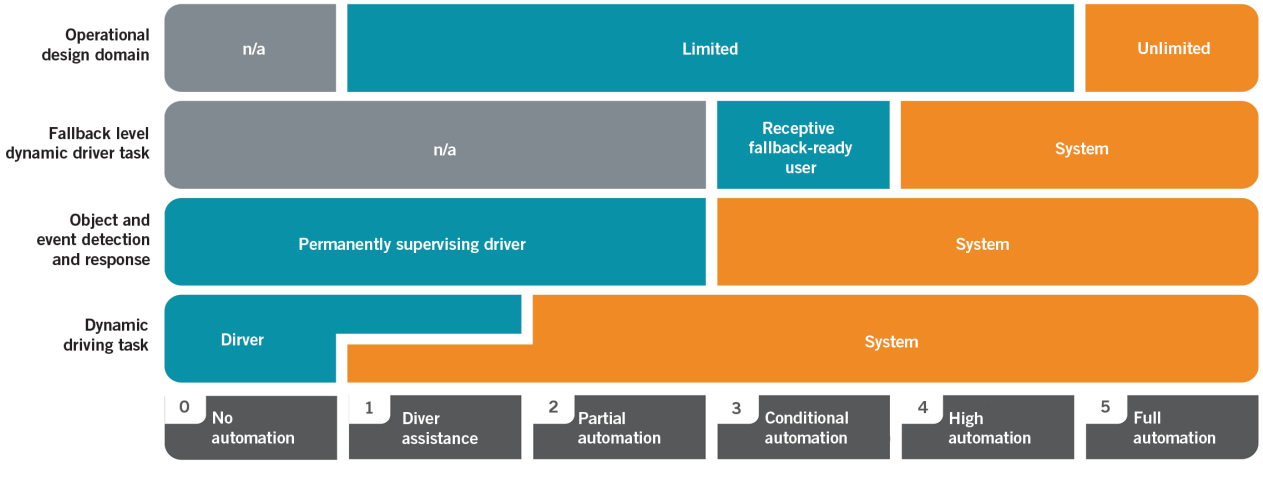
ISO 26262 provides a procedural tool box, to develop, produce and operate the necessary systems. This includes, among other things, requirements for the development process, such as the establishment of a safety life cycle, error control and request management. Therefore, safety management in the sense of ISO 26262 cannot be viewed in isolation from normal engineering, test, and production processes.

Rather, it complements and improves the already existing processes. For this purpose, ISO 26262 defines required activities and results, so-called work products, specific methods for the areas of engineering, testing and production, as well as acquisition and supplier processes. Similar to realization in standard requirements management, ISO 26262 pays a great deal of attention to traceability and consistency in particular. Furthermore, the ISO 26262 process model fits very well with the already established methods that are defined, for example, in the standard Automotive Spice.

INTRODUCTION OF A SAFETY CULTURE

ISO 26262 is, however, much more than a pure toolbox for dealing with future

FIGURE 1 Autonomy levels 0 to 5 according to SAE J3016 (© ATZelektronik)



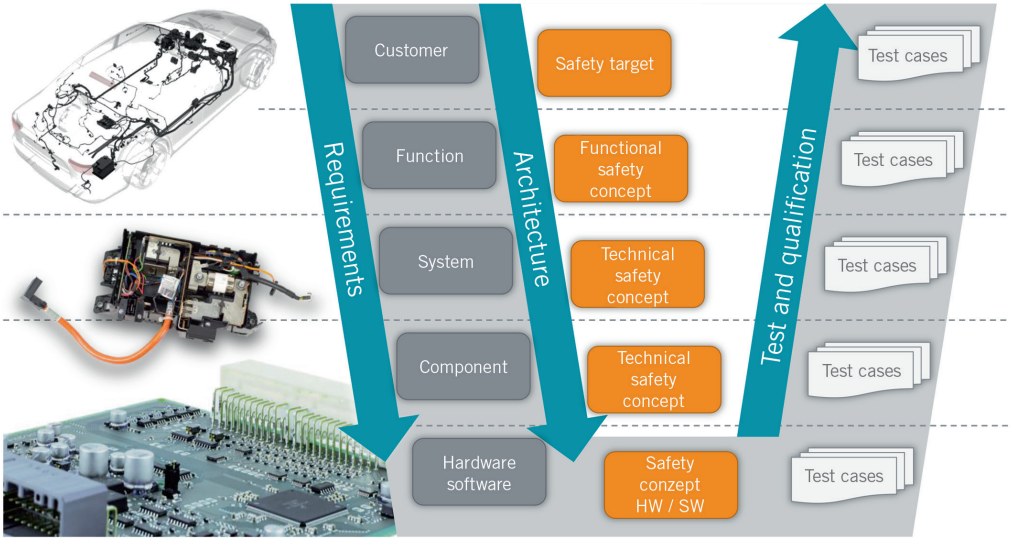


FIGURE 2 ISO 26262 cannot be considered as segregated from the normal engineering, test and production processes, but rather as being an enhancement of these processes (© Dräxlmaier)

requirements: It is also linked to the requirement to establish a safety culture within the company and the involved project partners. The success of the project depends not only on a purely formal adaptation of ISO 26262. In the process, this safety culture may not be put on the same level as the safety management that is also required.

The new processes and roles required by ISO 26262, such as the functional safety manager or the safety coordinator, impinge more or less severely in the structural and process organization as well as in the processes of an organization. The standard defines the specific activities and methods that must be used. Success, however, is highly dependent on the acceptance and understanding of those involved in the project. ISO 26262, namely, contains an additional challenge: While safety management – like any management process – can be written down and learnt, the establishment of a safety culture always requires a change in the way that those involved think; a change that goes beyond a common understanding and corresponding behaviour pattern.

It is noteworthy that a complex requirement is specified by a standard like ISO 26262. In this way, a special challenge arises when adapting ISO 26262. Because even if all process requirements have been established, the development of safety-critical functions hinges on the establishment of a safety culture.

To guarantee a successful introduction of ISO 26262, early involvement of all project participants is extremely important. It is necessary to communicate clearly and transparently to every employee which changes can be expected. It is also important that all those involved have an understanding of the overall process. Finally, when it comes to a safety culture, every employee must be able to identify with his or her role. This also provides the management with a major task during the introduction of ISO 26262.

POTENTIAL OF IMPLEMENTATION

The implementation of ISO 26262 harbours great potential. For instance, the relatively high effort involved in introducing a process system can be quickly offset by its specific benefits. What is particularly relevant is that the resulting systems can achieve a much higher level of quality and therefore cause less consequential costs. It is also possible to extend the findings to related processes throughout the enterprise. Project participants will quickly see that the newly introduced processes result in greater transparency due to the two

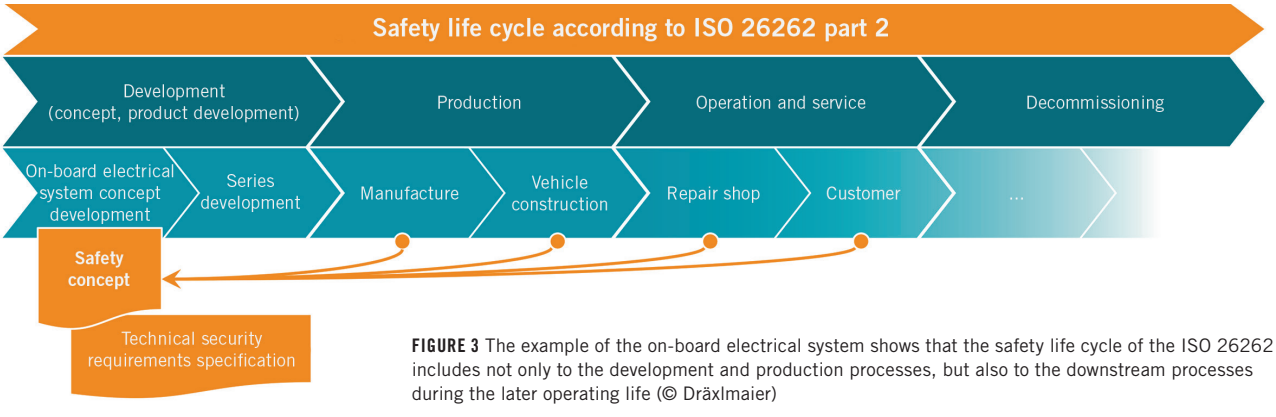


FIGURE 3 The example of the on-board electrical system shows that the safety life cycle of the ISO 26262 includes not only to the development and production processes, but also to the downstream processes during the later operating life (© Dräxlmaier)

factors of traceability and consistency. This supports efficient process design. It can therefore be noted: even though the initial implementation of ISO 26262 in- volves quite an overhead, this inevitably goes hand in hand with the process of transformation and can, for the most part, be compensated. This is achieved, in particular, by the fact that all processes can benefit – not only those relating to safety-related systems. This potential can be increased even faster, the tighter the affected organizations in all phases of work together – from process analysis to design and implementation to end use. Especially with regard to the developments in the automotive market, which are arising due to highly and fully automated driving, it will be interesting to observe how different companies deal with this challenge.

EXAMPLE: ON-BOARD ELECTRICAL SYSTEM DEVELOPMENT

The outlined procedures to ensure the functional safety of vehicles lead to very special demands on the wiring harness as the connecting element between a variety of components and sub-systems. It is, in the truest sense of the word, the physical embodiment of all process interfaces in vehicle development and production.

If the requirements in one place change, this already has effects on other components of the on-board circuit – however, these must now be documented as part of a continuous change management when ISO 26262 is applied. Since it is also necessary to take into account all downstream processes when a change is implemented, the requirements of the specific architecture of the vehicle must be fully known.

Here, in particular, the requirements for traceability and consistency laid down in ISO 26262 come into play, because it is the only way that the changes occurring in complex vehicle projects can be handled reliably. Thereby, the following questions must be always in focus: "What needs testing?", "How is testing to be done?", "Which production process is to be chosen?" and "Can continuous ISO 26262 conformity be guaranteed?". The aim must always be to integrate changes seamlessly into the overall vehicle concept.

The working group "ASIL metrics in on-board electrical systems", an initiative run by the Automotive Cluster at Bayern Innovativ, has been busy looking into this overall topic since the spring of 2015. The working group is currently composed of approximately 20 companies from the automotive industry, including the Dräxlmaier Group.

The objective of the working group is an overall system analysis of the on-board electrical system as well as the respective components, and to derive binding metrics on the FIT rate analysis as well as recommendations for action. The thematic focus is on the consideration of random hardware failures. The prerequisite for the definition of FIT rates, however, is that the production processes function properly.

During the investigations, it quickly became clear that due to the complexity of an on-board network it was impossible to consider and investigate all components. In addition, that, according to ISO 26262, the aim should be a reduction in complexity. To meet these requirements, appropriate design rules have been developed.

One essential aspect of this is the automated production of components, because this makes it possible to exclude potential sources of error found in manual production. It should be noted that ISO 26262 does not basically require any particular technological implementations. Automated production can, however, be viewed as expedient because it offers better possibilities of process monitoring and is conducive to the requirements of ISO 26262 traceability and consistency. To be able to produce a cable harness automatically, it is advantageous if it only includes point to point connections. At the same time, this meets the goal of reducing complexity. Simple electric-electronic architectures, as far as possible without separated circuits or other connectors, are thus expedient.

Connectors represent a particular challenge for the functional safety of electrical systems: for instance, the transmission of vibrations along the line during ultrasonic welding processes may lead to breaks on the contacts. With regard to the requirements of ISO 26262, this creates a too high safety overhead. The "ASIL metrics in on-board electrical systems" working group therefore recommends abandoning ultrasonic welded connectors in functional safety-related electrical functions. In addition, the functional safety-relevant parts of the electrical system should be separated from the rest of the cable harness. The choice of the simplest possible wiring architecture is thus essential for ensuring the functional safety because: the less complex the cable harness, the less elements need to be secured according to ISO 26262.In topological terms, crash-protected and low-vibration assembly spaces should also be used. If redundant layouts are necessary for safety-relevant functions, it is advisable to use different sections of the topology for the respective components and cables.

A RETHINK IS REQUIRED

Controlled processes, as well as a matching safety mindset of all stakeholders, are of key importance for functionally safe products: the respective technical design of components ultimately comes down to whether people, within the framework of the processes of ISO 26262, take the right measures to allow the product to mature in the safety life cycle as well as during operation.

The implementation of ISO 26262 thus represents a fundamental challenge in the area of organization. In the automotive sector, the overarching project organization is particularly affected, since everyone involved – OEMs and suppliers – must coordinate their efforts more intensively than they have ever had to do before. The development of functionally safe systems is increasingly becoming an interdisciplinary activity in which everyone must bring in his knowledge and especially his experience. The task of the overall system managers at the respective levels of the supply chain is to establish an awareness of the new processes of ISO 26262 among everyone involved, to network them with each other, and to define responsibilities clearly.

The digression in on-board electrical system development highlights the challenges that the application of ISO 26262 will bring to manufacturing complex components. The most successful companies will be those that manage to implement the adaptation of the new standard the quickest. Finally, the transfer of expertise from other areas will be important.