

Insight



berner & mattner
optimizing your development

Automotive

Special Issue: Functional Safety

Berner & Mattner Establishes Competence Center for Functional Safety

**Safety & Systems Engineering:
Integrated standard-compliant development**

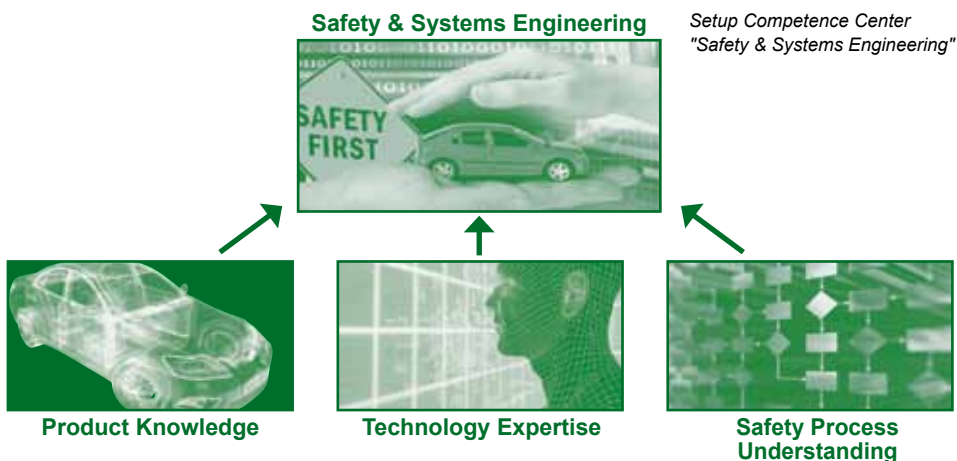
The competence center "Safety & Systems Engineering" is Berner & Mattner's new pool of know-how for Functional Safety, thus forming a team of experts that supports OEMs and suppliers in the efficient implementation of safety-critical product development. By pooling safety experts and system engineers with different technical focus, the competence center covers all development areas of electronic systems that are subject to the new ISO 26262 standard for Functional Safety.

The competence center is based on the consolidation, implementation and communication of the method and domain experience collected by the safety & system engineers of Berner & Mattner in many years. The combined know-how in the fields of safety analysis and safety concept development as well as the verification and validation of these systems is crucial for the effective implementation of safety-critical product development. Today, smooth development of a safe product often suffers from systems not being described in all aspects. There are difficulties in understanding between product developers and safety analysts, but also between OEMs and suppliers or the disciplines of hardware and software. The safety & systems team, acting across regions, helps solve problems in these areas through networked team power. It has already successfully completed several series projects for major car manufacturers and suppliers.



**Dr.-Ing. Bernhard
Kaiser, Head of the
Competence Center:**

"Functional Safety is often seen as a collection of additional process activities. This approach, however, does not do justice to the topic. Due to the complexity of today's systems, such as in the area of advanced driver assistance or e-mobility, feasible and economic solutions for meeting the safety requirements can only be achieved in a team of skilled engineers. The engineers have to understand the functioning of the system and to have a cross-sectional view of the interaction of all components – Functional Safety is an engineering discipline".



Events:

ESE Congress 2011
December 5-9, 2011 – Sindelfingen
Come and see us!

embedded world 2012
February 28 - March 1, 2012 – Nuremberg
You will find us in hall 5 at booth 326.

Automotive Testing Expo Europe 2012
June 12-14, 2012 – Stuttgart
Berner & Mattner welcomes you at booth 1537.

Advances in Automotive Electronics 2012
June 19-20, 2012 – Ludwigsburg
Come and see us!

www.berner-mattner.com/en/events

Presentations (German only):

"Safer advanced driver assistance systems - does ISO 26262 offer the right instruments?"

"AUTOSAR 26262 – how can AUTOSAR systems become safe?"

"Configuration qualification of an integration HiL providing evidence of a driver assistance function in the context of ISO 26262."

www.berner-mattner.com/de/vortraege

Current Job Openings (German only):

Expert (m/f) for Functional Safety

Trainee Automotive (m/f)

www.berner-mattner.com/de/stellenangebote

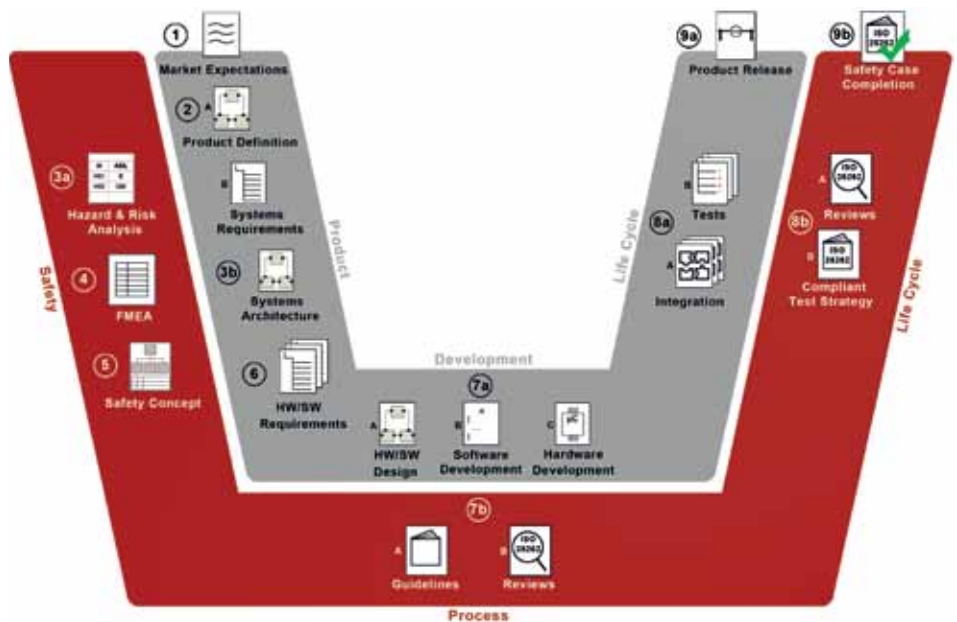
ISO 26262

Integration of Functional Safety in the Development Process

The new safety standard ISO 26262 forces automotive electronic system manufacturers to align all their development processes with safety considerations. To date, safety activities are often still undertaken quite independently from the developers' "normal" work, however, with the consequence of safety requirements entering the development process at an advanced state causing costly additional development work. Berner & Mattner presents a new methodology for the tool-based combination of safety activities with traditional system development and early implementation of safety requirements in the system design.

The method combines hierarchical modeling of system architectures and failure nets, allocating safety mechanisms, and systematic requirements tracking including proof of test coverage. This methodology consists of combining basically known and proven approaches in an intelligent, tool-integrated way. In addition, the models and concept modules are modular and reusable. With this method, the efficiency has significantly increased in various customer projects.

➔ Read more in the technical paper "Integration of Functional Safety in the Development Process" published in ATZ Elektronik 5 at www.berner-mattner.com/en/technical-papers



Overview: Integration of Functional Safety in the Development Process

1. Product characteristics based on market expectations
2. Product definition and systems requirements with the help of safety and systems engineers
3. Parallel and interrelated work on Functional Safety and product development
4. Development of the hierarchical FMEA (Failure Mode and Effects Analyses)
5. Safety concept design
6. Safety concept integration into the existing requirements management
7. Implementation and execution of HW/SW design (7aA), SW and HW development (7aB, 7aC) according to ISO 26262
8. Gradual integration (8aA) and testing (8aB) in compliance with ISO 26262 test strategy (8aA) as well as reviews of test cases and test results in terms of safety (8bB)
9. Safety case completion (9b) and vehicle release (9a)

Advantages of the Service Portfolio of Berner & Mattner

- Reduction of failure, recall and product liability risks
- Coverage of all activities of the safety life cycle according to ISO 26262
- Closing the knowledge gap between the disciplines during the development of software controlled electronic systems
- A faster way to a safe system functioning in compliance with specifications: reduction of development cost and time, avoiding product risks
- Continuous training of our employees ensures that all innovations and changes of the standard requirements as well as the latest interpretations of the standard in practice are directly transferred to the affected development projects.

Project example:**Green Project****Start/stop systems on the rise**

Start/stop systems with additional energy storage to support the electrical system are being implemented into many vehicles. Their development and implementation according to the requirements of ISO 26262 is, however, only at an early stage. In a pilot project for a major supplier, Berner & Mattner has carried out the requirements engineering, the creation of the system architecture, all Functional Safety activities as well as the failure analysis and test management. In this comprehensive project, all experts of the competence center complemented each other perfectly and efficiently implemented the project according to ISO 26262 under tight cost and time constraints.

Project example:**Challenge CO₂ Reduction****ECU development for energy storage**

Solutions for the energy supply of the e-motor can not only be found in the battery technology. In summer 2011, Daimler showed with the circumnavigation of its hydrogen-powered research fleet that other environmentally friendly technologies, too, are suitable for driving vehicles. Berner & Mattner takes on the development and safety analysis of a safety-critical control device for storing energy for a major OEM. Here, the know-how in ECU development is required as well as the expertise in Functional Safety. Documentation, hazard analysis, FMEA

(Failure Mode and Effects Analysis) and pragmatic suggestions for implementing the safety requirements are key elements of this project.

Project example:**Safe E-Mobility****Challenge of powertrain electrification accepted**

Electronic powertrains present big challenges for the development, not only in terms of new drive concepts to be developed but also in terms of ensuring the Functional Safety of heavily electrified systems. Berner & Mattner has taken on the Functional Safety activities in several projects, including a project for a global supplier, amongst others. Key elements are the creation of hazard analysis and safety concepts as well as the development and execution of test concepts of power inverters for synchronous machines for electric and hybrid vehicles of European OEMs. The result is the successful development-friendly integration of comprehensive safety activities into the customer's existing development process.

Project example:**Developments on the Highest Hazard Level****Steering system on ASIL level D**

According to ISO 26262, electronic steering falls in ASIL level D and therefore the highest hazard level. Accordingly comprehensive are the safety measures concerning the development, validation and documentation. Berner & Mattner has developed a technical safety concept for this highly safety-critical system for a supplier

as well as provided him with consultancy on choosing a processor. A highly advanced dual core processor with special hardware-based fault detection mechanisms is used. Other tasks within the project: Creation of software architecture, definition of hardware diagnostics, implementation of FMEA as well as creation of fault tree and common cause failure analyses. This project required all subject areas of the competence center, namely the definition and execution of the safety activities in the product life cycle, embedded systems engineering, methods application and interface communication between corporate locations, OEM and processor manufacturer. The customer benefits from an integrated support and a seamless integration into his development activities without coordination difficulties.

Project example:**Safety Processes****Also an issue for trucks!**

Consultancy on safety processes is a key portfolio area of the competence center. Berner & Mattner has accomplished the safety process implementation for a truck manufacturer, including gap analysis and training with focus on both traditional and model-based code generation, amongst others. In addition, a pragmatic procedure approach has been proposed in the current project because the OEM wanted his trucks to be on the right track, already anticipating the future standard becoming mandatory. In this context, an evaluation of validation techniques for processes and the applicability of standard safety architectures (such as e-gas) has been conducted. In addition, recommendations were given with respect to the qualification of development tools and the improvement of the testing process.

**Workshop****Are we on the same page?**

Workshops for process definition and modeling, methods training and product understanding as well as for bridging difficulties in the understanding between departments are a regular part of our customer projects – held by experienced senior consultants with many years of industry experience. These workshops can of course also be booked separately.

 www.berner-mattner.com/en/trainings



Outlook

What challenges can the industry expect from ISO 26262?

The compliance with ISO 26262 has been a standard for the development of safety-critical systems since its release in November 2011. Functional Safety is required in the development of braking and steering systems and alternative drive concepts, as these systems have a high hazard potential. But all other electronic systems in the vehicle are affected as well, even light and wiper control systems. Trends such as increasing complexity and connectivity, functionality shift to software, function-oriented development of new safety assistance functions, variant variety and AUTOSAR coincide with ISO 26262. Together, they have even higher demands on the development process. So what will be important when developing vehicle systems according to the standard's requirements in real life?

AUTOSAR and ISO 26262 – Safety for integrated systems

The AUTOSAR standard aims at shifting functionalities to software and integrating more functions into one ECU. These functionalities should also be freely allocable to ECUs. The merging, however, implies the safety risk of mutual interference. To validate this risk in terms of the standard, all functions have to be analyzed regarding their hazard potential already in the requirements specification and their impact potential on other functions has to be verified. Moreover, the functions developed across location and company boundaries have to fulfill the standard requirements in the development and validation process. The safety of the entire system can only be proven with the combination of these aspects.

The competence center provides help already in the early phase assessing the hazard potential of individual functions based on cross-company experience. It also functions as a link between OEMs and the suppliers invol-

ved in the development of safety-critical functions. During the definition of safety concepts, AUTOSAR-inherent mechanisms (version 4.0) are referenced – exemplary mappings of failure modes and diagnostic coverage degrees are already available! Major manufacturers are currently working with us on the "Compositional Safety Case", significantly reducing evidence testing when porting functionalities.

Autonomous driving – Other technologies affected by ISO 26262

A vehicle determining speed and lane tracking in stop-and-go traffic without any driver intervention, parking automatically or braking independently before inevitable collisions is a vision all companies in the automotive industry are working intensively on. Until obtaining the homologation of such systems, some hurdles still have to be taken by the developers. This also refers to the question of how the Functional Safety of autonomous driving interventions can be guaranteed. This is a complex issue far

beyond the scope of ISO 26262, extending to disciplines such as sensors, ergonomics, liability and regulatory law. In addition to the car's sensor systems, such functions increasingly include data in their strategy which are transferred from other vehicles or stationary infrastructure, such as the terrain, road utilization or hazard warnings. For this form of data exchange, the term "Car-to-X-Communication" is used.

Extended interfaces influencing the driver's behavior require the consideration of other technologies in the safety-compliant development process – sensor fusion algorithms, data transmission and data security are just a few of them. Automotive manufacturers and suppliers will benefit from Berner & Mattner's experience. This expertise is based on development and validation of various advanced driver assistance functions (e. g. camera- or radar-based), in the infotainment area and standardization services in fields such as TPEG.

Safety for vehicle individualization?

Vehicles need to be flexibly adaptable to the needs and demands of the consumers in order to remain competitive. Variant variety, only viable with software variants and parameterization, is a consequence of the different consumer demands. Another trend is the integration of future advanced driver assistance systems into the vehicle using apps. Here, security (protection against unauthorized manipulation) and safety (protection against accidents) work closely together. They must also be involved in the activities of Functional Safety via the integration of external technologies. Technology is progressing rapidly – Stay safe with Berner & Mattner.



berner & mattner
optimizing your development

Contact persons

Gudrun Wehrle

Phone +49 (0) 89 608090-255
gudrun.wehrle@berner-mattner.com

Ute Herold

Phone +49 (0) 89 608090-270
ute.herold@berner-mattner.com

Imprint

Publisher:

Berner & Mattner Systemtechnik GmbH
Erwin-von-Kreibitz-Str. 3
D-80807 Munich
Phone +49 (0) 89 608090-0
Fax +49 (0) 89 6098182
www.berner-mattner.com
marketing@berner-mattner.com

Editorship and Layout:

Martina Heinze, Gudrun Wehrle
© Berner & Mattner / December 2011