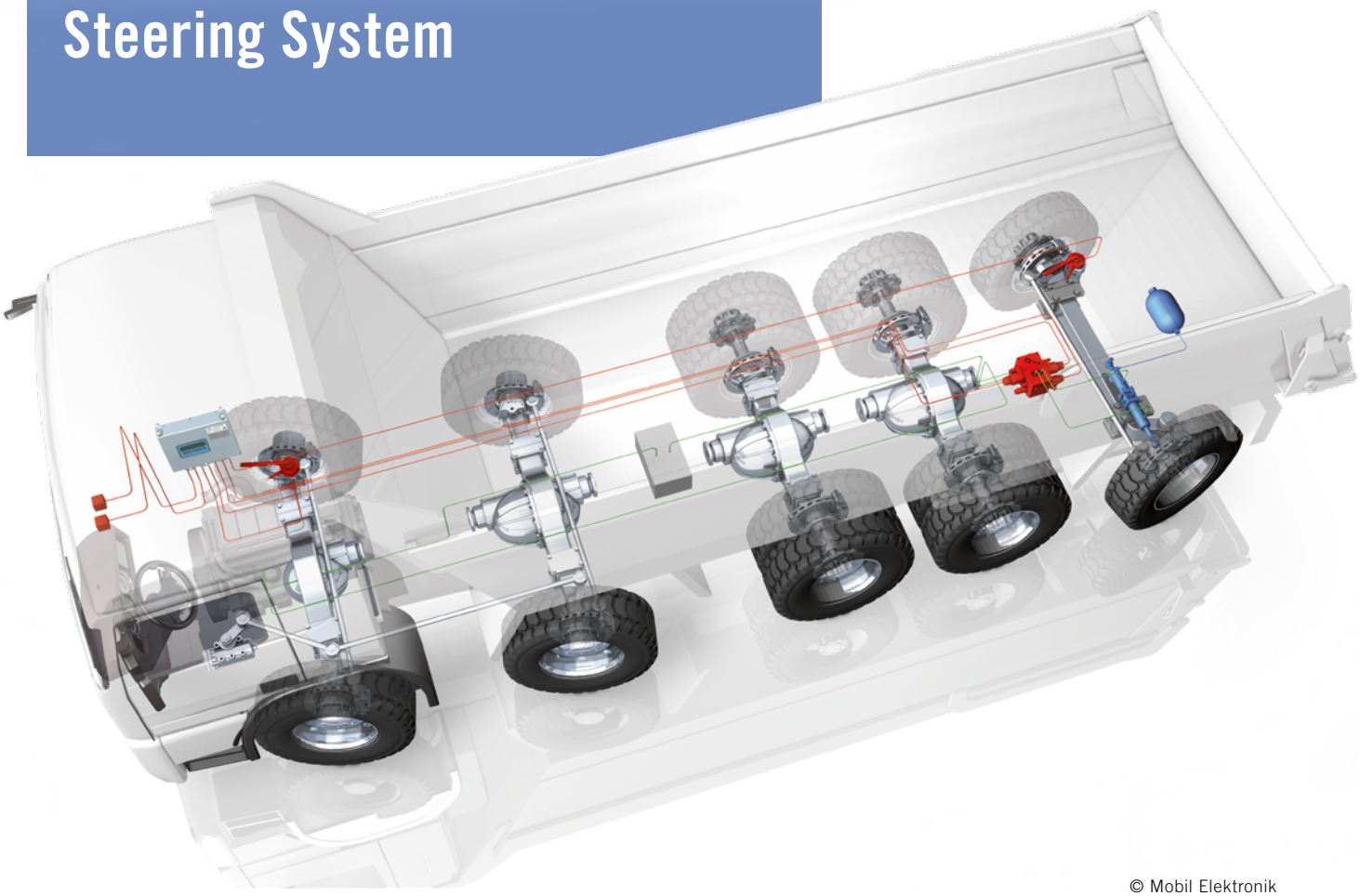
Effects of ISO 26262 on Commercial Vehicle and Steering System



© Mobil Elektronik

AUTHORS

Dr.-Ing. Marco Völker
is Head of R&D at Mobil Elektronik GmbH in Langenbrettach (Germany).

Dipl.-Ing. (FH) Wolfgang Stadie
is Head of Sales & Marketing at Mobil Elektronik GmbH in Langenbrettach (Germany).

So far the automotive international standard ISO 26262 for the development of safety relevant electrical and electronic components is used for vehicles up to 3500 kg gross weight. The foreseeable extension of this standard to heavier commercial vehicles will have effects on vehicle manufacturers and their suppliers. The medium-sized enterprise Mobil Elektronik has already organised itself accordingly and develops its auxiliary steering systems ISO 26262 compliant.

WHY IS THE ISO 26262 NECESSARY AT ALL?

With the complexity of electronic – especially programmable – systems the diversity of the fault potential increases in automotive technology, too. Besides, the origins of the "functional safety" topic lie in industries such as plant engineering, nuclear power plant technology, aviation and railway industry, where the series of standards IEC 61508 [1] is used for a longer time. This series of standards requires the use of diverse methods

to avoid systematic errors (errors in the specification, the implementation etc. of the system) and for a safe mastery of malfunctions and breakdowns (often by physical phenomena or operating errors).

For automobiles this series of standards was transferred and adapted into the standard ISO 26262 [2]. The standard includes an automotive-specific risk-based approach for determining risk classes, so-called ASIL levels, **FIGURE 1**. Therewith the established Safety Integrity Levels (SIL) were transferred to the Automotive Safety Integrity Levels (ASIL). The determination of the risk classes or hazard and risk analysis (G+R) is the responsibility of the vehicle manufacturer. The methods for it are regulated by ISO 26262.

The choice of the electric and electronic components used conforms to the result of this hazard and risk analysis. Basis of all safety standards is IEC 61508, which has relevance besides automotive area also in nuclear or medical technology, **FIGURE 2**.

WHAT KIND OF EFFORT REQUIRES THE ISO 26262 FOR A MEDIUM-SIZED ENTERPRISE?

Mobil Elektronik GmbH, family-owned with 110 employees, develops electrohydraulic auxiliary steering systems for rear axles of commercial vehicles. These steering systems consist of safety steering computer, angle transducer and proportional valve hydraulic units, which represent a closed control loop. Primarily, these systems are used in trucks, buses, mobile cranes and agricultural vehicles, what means in vehicles licensed for use on public roads with more than 3500 kg total weight. The company would be directly affected by the ISO 26262, as soon as the standard is extended to this weight category.

As mentioned previously, the goal of the ISO 26262 is to reduce the safety risks of electric and electronic components by stricter requirements than mandatory in the IEC 61508. In the ISO 26262 the entire safety life cycle of the product to be developed is considered. All activities during the different stages of this life cycle need to be assessed and documented. Especially the effects of safety-related modifications during the project need to be assessed in detail, to meet the requirements of the safety life cycle in each development stage.

Here the ISO 26262 requires a continuous change management. Changes need to be assessed regarding their effects on functional safety (impact analysis), traceably implemented and documented. This issue has significant influence on the entire business process landscape of a company, since a lot of new process steps need to be newly implemented.

Requirements for the validation measures of the individual development steps have to be defined exactly. Basis for the development process defined in the ISO 26262 is the traditional V-model, **FIGURE 3**. The V-model is used for development work on system level as well as for hardware and software development. The end-to-end traceability of requirements is of particular importance. A requirement needs to be traceable at any time from the system to the module level and vice versa. Likewise the connection between requirements and tests on the right hand side of the V-model needs to exist. Usually the creation and maintenance of the traceability of requirements and tests highly challenges medium-sized enterprises with their typical business structures. Apart from that the processes described here have inevitably influence on product liability.

Basis for the implementation of processes according to ISO 26262 is an existing and established ISO 9001 quality management system, which nowadays should not anymore be a problem for medium-sized enterprises.

However, for ISO 26262 compliant processes a so-called functional safety manager is additionally required, who is formally and organisationally independent from the development department. Depending on the customer's requirements regarding the ASIL level of the components to be produced independent tester and reviewer might also be necessary.

Depending on the ASIL level the ISO 26262 requires for the safety assessment and confirmation reviews different degrees of independence of the reviewer. Medium-sized enterprises often cannot realise the required independence internally. The new processes increase the amount of work for the development of

Classes of severity

S0	S1	S2	S3
No injuries	Light & moderate injuries	Severe & life-threatening injuries	Life-threatening injuries, Fatal injuries
AIS 0	AIS 1 & 2	AIS 3 & 4	AIS 5 & 6

Classes of probability of exposure regarding operational situations

E1	E2	E3	E4
Very low probability	Low probability	Medium probability	High probability
Not spec.	< 0.01	< 0.1	> 0.1

Classes of controllability

C0	C1	C2	C3
Controllable in general	Simply controllable	Normally controllable	Difficult to control or uncontrollable
Not spec.	> 99 %	> 90 %	< 90 %

Severity class	Probability class	Controllability class		
		C1	C2	C3
S 1	E1	QM	QM	QM
	E2	QM	QM	QM
	E3	QM	QM	ASIL A
	E4	QM	ASIL A	ASIL B
S 2	E1	QM	QM	QM
	E2	QM	QM	ASIL A
	E3	QM	ASIL A	ASIL B
	E4	ASIL A	ASIL B	ASIL C
S 3	E1	QM	QM	ASIL A
	E2	QM	ASIL A	ASIL B
	E3	ASIL A	ASIL B	ASIL C
	E4	ASIL B	ASIL C	ASIL D

FIGURE 1 Determination of the risk classes according to the safety standard ISO 26262-3 and its tables 1, 2, 3, 4 and B1, B2, B4 – source: ISO 26262-3:2011, Beuth-Verlag (© Mobil Elektronik)

products. This increase results in higher costs reflected accordingly in sales prices. In case these prices are not feasible it influences significantly the margin.

HOW HAS ISO 26262 BEEN SUCCESSFULLY IMPLEMENTED?

The basis for a successful implementation of the standard is a continuous, usually new, process landscape of the company in line with the ISO 26262.

Mobil Elektronik has analysed its status quo within an extensive internal project, detected deviations and established a new process landscape with the name Mobil Elektronik Product Development Process (ME-PEP), **FIGURE 4**. The project was started in 2014 with the support of external business consulting and finished in mid-2015.

The different quality gates 1 to 8 assure that customer requirements and changes are assessed regarding their influence on the safety system at each stage of the product development process, **FIGURE 3**. If it is influenced, the safety concept can be changed accordingly and the necessary working packages in the development initiated. Although the ISO 26262 standard is stricter than its IEC 61508 prior version, it nevertheless offers possibilities to limit the necessary effort by tailor-made processes.

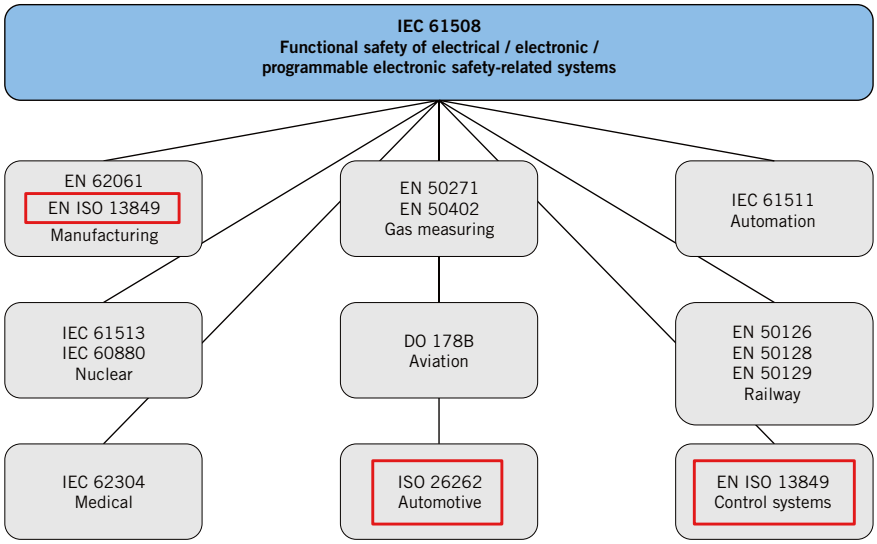


FIGURE 2 Overview of existing standards with IEC 61508 as starting point, automotive relevance is marked in red (© Mobil Elektronik)

TAILOR-MADE PROCESSES

Medium-sized enterprises are often faced with both large-scale and very small projects. That is why it is necessary and also possible to tailor the processes

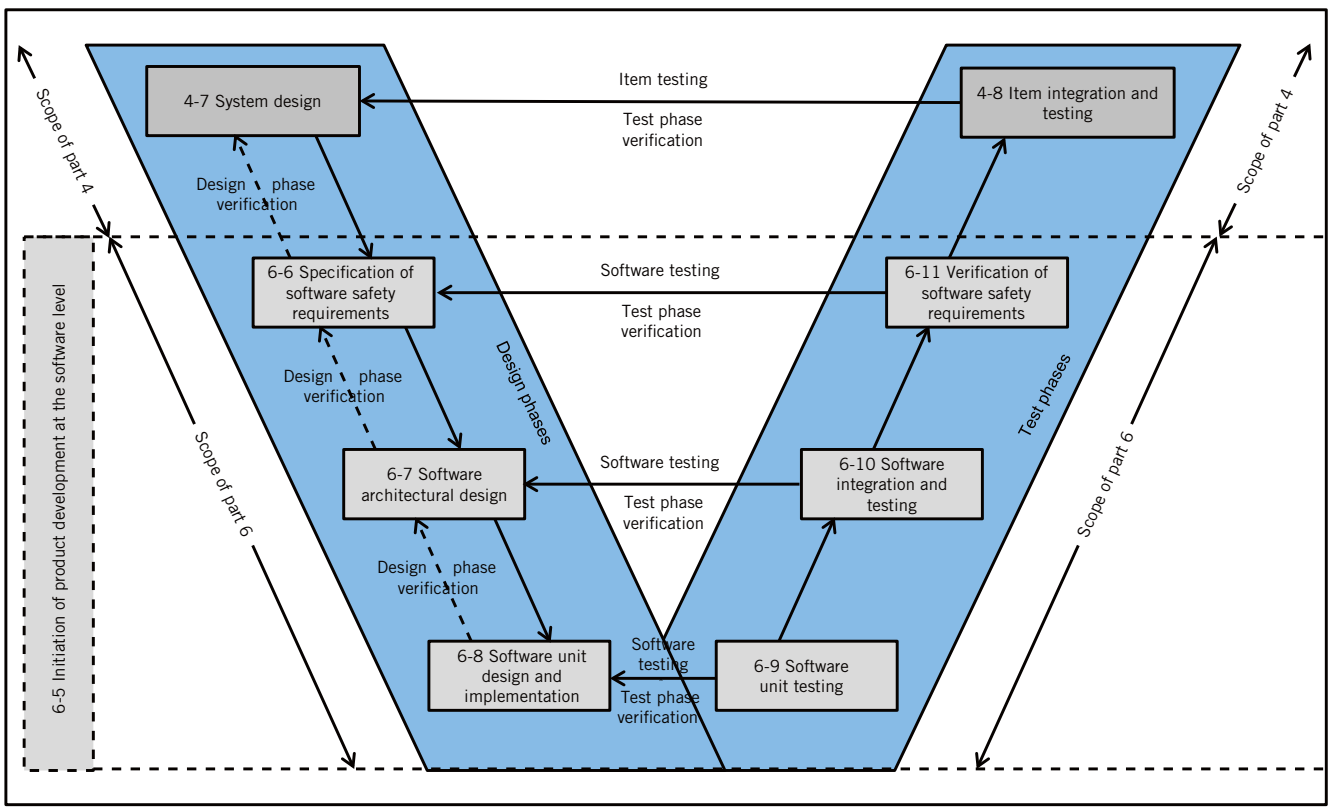


FIGURE 3 Traditional V-model of the product development process according to the safety standard ISO 26262-6 – source: ISO 26262-6:2011, Beuth-Verlag (© Mobil Elektronik)

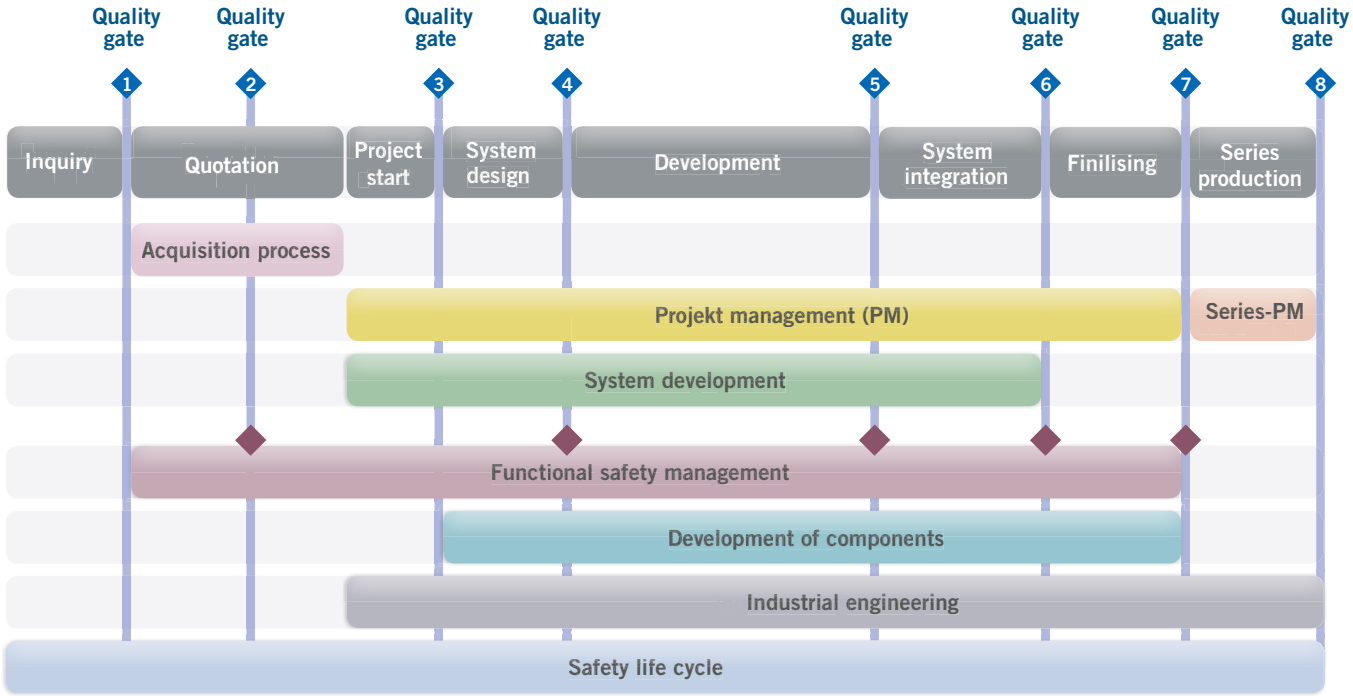


FIGURE 4 Structure of the Mobil Elektronik Product Development Process (ME-PEP) (© Mobil Elektronik)

depending on the project size. This means the processes need to be designed in a way that they can be tailored. It is necessary to individually analyse for each project, which work products and which processes are required in the particular case. However, tailoring has its limits. Especially when developing components for functional safety it is important to tailor the work products to be initiated regarding the specific project.

For instance it is always required to define the responsibilities during product development clearly towards the customer but also towards the supplier. The corresponding work product in the ISO 26262 is called Development Interface Agreement, DIA in short. A DIA is fundamentally important for each project related to functional safety and cannot be omitted.

TOOL-BASED APPROACH

Furthermore it is essential to reduce the effort for the traceability of requirements and their allocation to tests on the different test levels. An increasing number of requirements results in a disproportionate increase of effort. To establish and maintain the connection between system requirements, component requirements, component tests and system tests manually is not reasonably realisable even for a relatively small number of requirements. That is why it is important for middle-sized enterprises to switch to tool-based approaches for it at an early stage. Appropriate requirements management software tools or more general application lifecycle management tools support the user when establishing and maintaining requirements and tests as well as connecting individual elements – this in part specifically in regard to ISO 26262.

The proof required by the standard that each requirement is covered by at least one test is therewith created full automatically in the background. These tools also simplify further supporting processes required by the standard considerably (for example the configuration management). That way the efforts are kept in limits and the cost-price structure is not unnecessarily put under pressure.

DECOMPOSITION

ISO 26262 offers the possibility of the so-called decomposition, so that high ASIL levels can be divided into several parallel paths of lower ASIL levels. This particularly makes sense if a complex basic function (for example the entertainment system) needs a simple, but highly rated safety function (for example "the entertainment must not be used when driving"). With decomposition the complex basic function can be developed with a low or no ASIL, while the complex development of the safety function with high ASIL is only required for a simple function block.

In the entertainment example an independent path would have to be created, in which a simple circuit assesses the vehicle's speed and switches off the entertain system above a defined threshold. Usually decomposition of a system results in less total efforts as if to develop the entire function with a high ASIL.

Decomposition is linked to different boundary conditions. For instance it is only permitted if common cause errors can be excluded from all ASIL paths of the decomposition. Corresponding analyses help to discover common cause errors.

IMPLEMENTATION

The ISO 26262 has also influence on the actual implementation. Depending on the required ASIL degree, different requirements are specified regarding the programming language used and the

usage standards. For instance, it is advisable to limit the huge language range of the programming language C by using the Misra rules [3].

Similar high requirements as for the specification the ISO 26262 specifies for verification and validation. Tests take place on different levels. Here too the requirements are difficult to handle without a tool-based approach for module tests and system tests.

RESULTS AND CURRENT USE CASE

The new development process at Mobil Elektronik has already been confirmed by TÜV Nord after a process audit as ISO 26262 compliant. A major commercial vehicle manufacturer approached Mobil Elektronik with very high requirements. The electrohydraulic auxiliary steering for a rear axle should comply with the ASIL-D level, because the hazard and risk analysis of the manufacturer specified this.

Solely by the early implementation of the processes described here and strict compliance Mobil Elektronik succeeded in developing a new safety steering computer for this project based on a new software and hardware architecture. First article inspections have already taken place.

FUTURE MARKET REQUIREMENTS

Manufacturers of vehicles with more than 3500 kg total weight will be forced for the medium term to accept the new regulations and to comply with the ISO 26262 standard. Although the ISO 26262 is currently still limited to road vehicles with maximum 3500 kg gross weight it becomes apparent that many commercial vehicle manufacturers have started implementing the standard by now. If an ASIL safety level is specified instead of an established SIL in the specifications for electric and electronic components, which usually are supplied externally, it then has direct effects on the supplier who also has to comply with this safety.

Mobil Elektronik was faced with the requirement to realise the safety level ASIL-D for some safety related functions. A new hardware platform and new software architecture were necessary for this. The development process for software and hardware was restructured ahead to be ISO 26262 compliant, so that on this basis could be built on.

SUMMARY AND OUTLOOK

The ISO 26262 safety standard highly challenges companies since implementation is expensive and time-consuming. To keep costs within limits, the standard offers the option to adapt tailor-made the required processes to the requirements and needs of the individual project.

However, the newly created process structure also has many advantages for the companies. It increases competitiveness because the new customer requirements can be met. Furthermore these processes lead to a considerable step forward regarding quality, documentation and project management in the company. Therefore it is recommended to establish the required processes early, to be ready in time for the compliance to ISO 26262. External consulting might support it.

REFERENCES

[1] IEC 61508-1:2010: Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 1: General requirements. https://www.beuth.de/en/standard/din-en-61508-1/135302584, access: 29 September 2017

[2] ISO 26262:2011: Road vehicles – Functional safety. Part 1 to10. Online: https://www.iso.org/standard/43464.html, access: 29 September 2017

[3] Misra C:2012: Guidelines for the Use of the C Language in Critical Systems. ISBN 978-1-906400-10-1 (paperback), ISBN 978-1-906400-11-8 (PDF), March 2013