Netzwerk Baumaschinen NRMM CV

Functional Safety

for Mobile Machinery NRMM and Vehicles CV

Safety and Industrial Security during development – Risk limitation of control systems
Information for operators, manufacturers and supervisors

Netzwerk Baumaschinen NRMM

The Network for Non Road Mobile Machinery supports the quality of processes increasing economic efficiency and safety in the applicable field of mobile machines (NRMM – Non Road Mobile Machinery). For tasks of common interest, the network discusses information and creates guidelines in cooperation with involved stakeholders.

This sheet about "Functional Safety" complements the guideline "Person/Object Recognition, Warning in Danger Areas – Camera and Sensor Systems, Intelligent Software for Mobile Machinery" developed within the network. The guide explains how people and objects can, through the use of additional technical auxiliaries, be better detected in danger areas under restricted visibility conditions.

Offensive Gutes Bauen

Offensive Gutes Bauen is a national initiative of the construction industry, which is committed to building quality in Germany. Partners are federal and state governments, business associations and chambers, trade unions, employers' liability insurance associations, guilds, consumer protection associations of the clients – more than 150 in total. The Federal Ministry of Labour and Social Affairs (BMAS) initiated and supports Offensive Gutes Bauen.

VISION ZERO.
NULL UNFÄLLE – GESUND ARBEITEN!

Occupational safety is teamwork. Since 2018 the network has been a cooperation partner of the BG RCI prevention strategy "VISION ZERO". VISION ZERO pursues a working environment in which nobody will be seriously injured or killed and nobody gets so sick that he'll suffer lifelong damage.

- www.bgrci.de/vision-zero/vision-zero

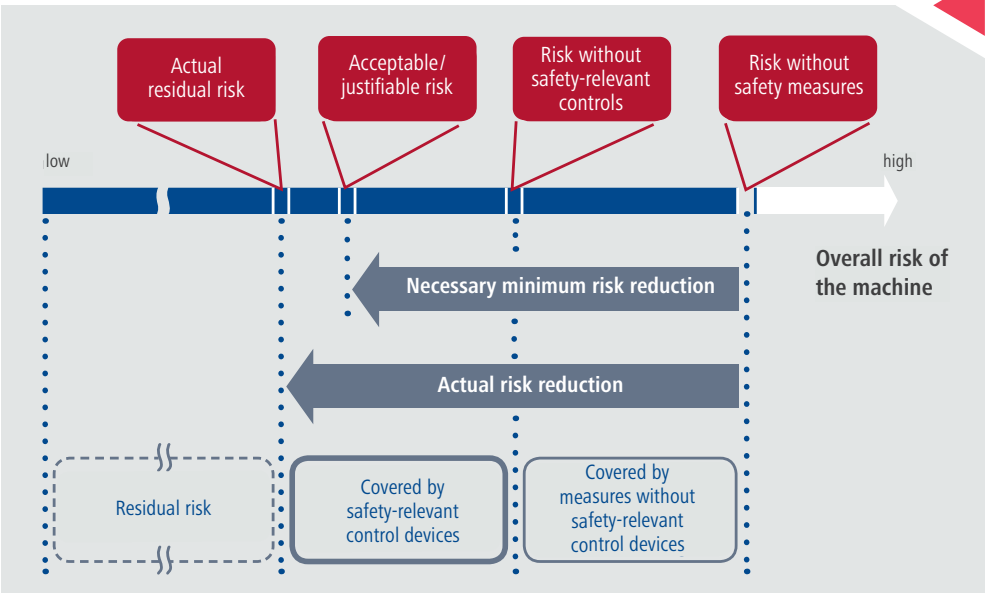
Functional Safety
for Mobile Machinery NRMM and Vehicles CV

Why is functional safety important?

The primary objective of functional safety is to reduce the risk of personal injury. Functional safety concerns the control system of mobile machines on which a safety-relevant function depends. Due to the increasing number of control units in today's applications, functional safety is becoming increasingly important. This is particularly relevant for autonomous systems for accident prevention.

As soon as safety functions are implemented in a machine by means of a control system, the manufacturer must design the control components according to a previously determined safety level (see also page 5). The determination of the required safety level and the corresponding implementation of the safety-relevant control function is based on the relevant standards, e.g. EN ISO 13849.

EN ISO 13849
"Safety of machinery – Safety-related parts of control systems"
Part 1: General design principles
Part 2: Validation

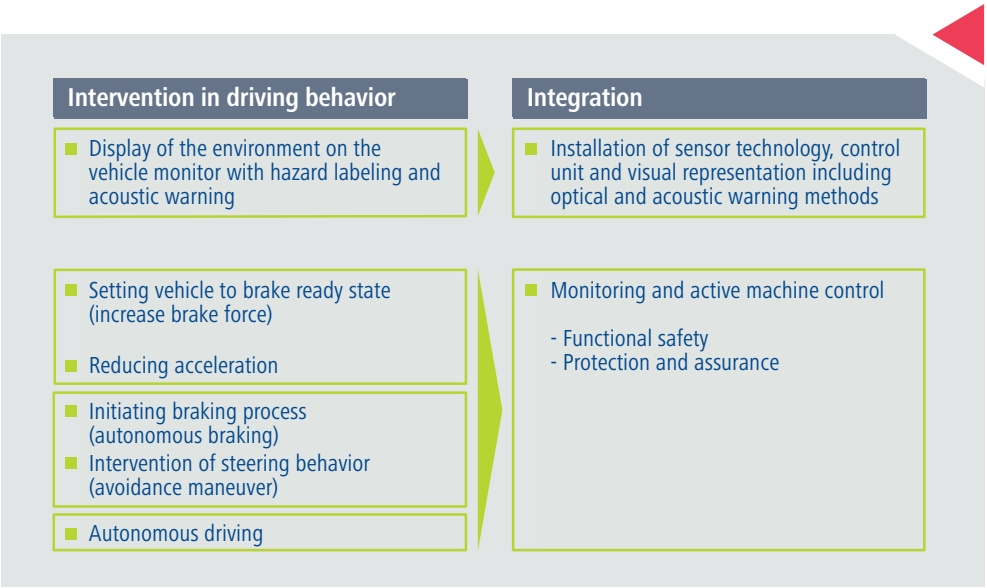


Purpose of functional safety: Reducing risk of personal injury (source: BGIA report 2/2008 on EN ISO 13849).

Limitation of risk

Which systems are subject to functional safety

If the behaviour of a system is actively interfered with in the event of danger – in order to bring the system into a safe state, e.g. in the form of an autonomous braking or evasive manoeuvre – this must in any case be evaluated and implemented in accordance with the criteria of functional safety. In addition, this has a massive impact on the vehicle architecture of the mobile machine.



Integration of safety systems depending on intervention in driving behaviour (source: ITK Engineering GmbH)

Standards regarding mobile machinery

With regard to machine safety, there is a large number of relevant standards. The basic safety requirements can be found in the MRL ("Machinery Directive" – Directive 2006/42/EC). These requirements are specified for the respective machine type, e.g. by:

- **EN 474** (for earth-moving machinery)
- **EN 500** (for mobile road construction machinery)
- **EN 1889** (for mobile machines in underground mining)
- **EN 16228** (for equipment for drilling and foundation work)
- **ISO 25119/EN 16590** (for tractors, agricultural and forestry machinery)

These European standards are harmonised under the EU Machinery Directive 2006/42/EC (MRL). This means that manufacturers can assume that the requirements of the standards are covered by the MRL. The so-called **"presumption of conformity"** applies.

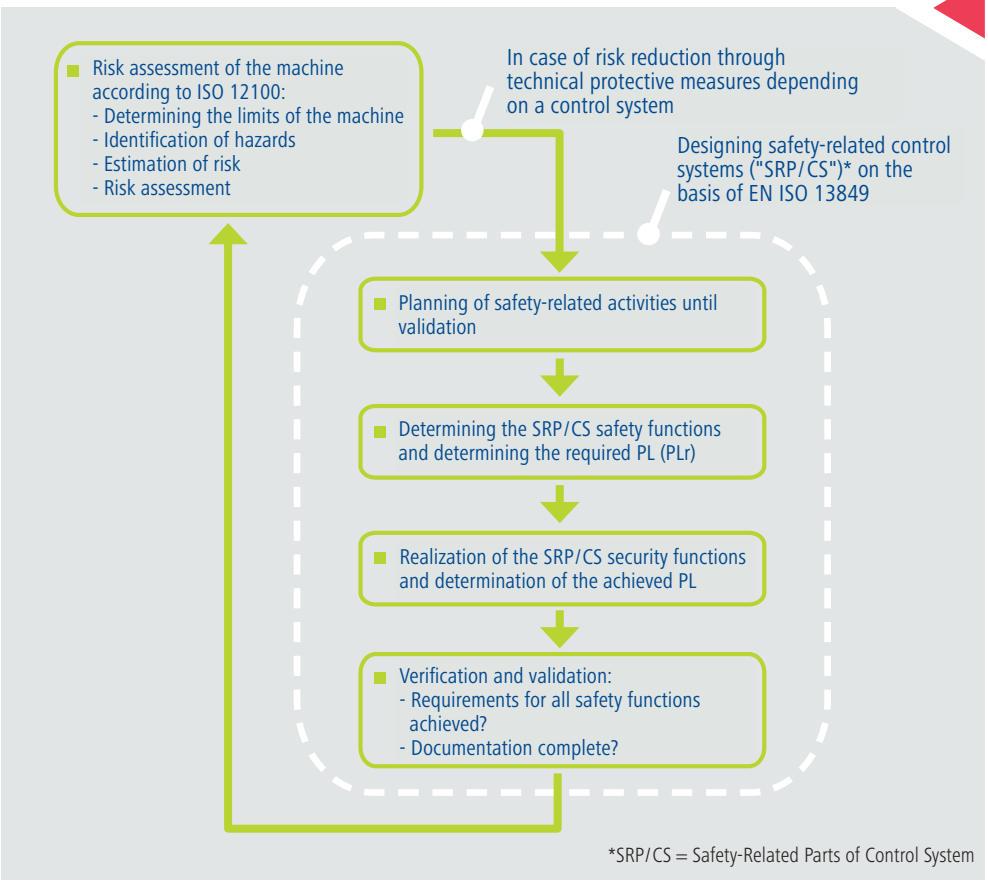
▶ **All standards harmonised under the MRL: https://ec.europa.eu/growth/single-market/european-standards/harmonised-standards/machinery_de** (if you do not have access to the link, please contact us: info@safety-machinery.com)

In order to achieve conformity with the MRL, directive **EN 12643 (ISO 5010)** must also be applied to steering systems in rubber-tired machines such as excavators. **ISO 15998** exists specifically for functional safety of earth-moving machinery, but is not harmonised and therefore cannot be formally used to achieve conformity with the MRL. However, parts of non-harmonised standards cited by harmonised standards can be used to achieve conformity regarding MRL. Regardless of the respective machine type, the basic standard **EN ISO 13849** should be taken into account regarding functional safety. In this standard, five safety levels are defined, so-called **"Performance Level (PL)"**, ranging from PL a to PL e.

What do manufacturers have to take into account during development?

During development, the processes required by the functional safety standards must be adhered to and corresponding documents must be prepared. This includes an **early risk assessment** (according to EN ISO 12100) as well as suitable planning of the relevant activities to ensure efficient and traceable development. A suitable safety function must be defined and the safety level determined (e.g. PL in accordance with EN ISO 13849-1) for each hazard for which risk reduction is to be achieved by a safety-related control system.

Manufacturers are required by law to conduct a risk assessment:
▶ EN ISO 12100 "Safety of machinery – General principles for design – Risk assessment and risk mitigation".



Process for designing safety-related control systems (Source: ITK Engineering GmbH)

The safety functions are then developed according to the relevant requirements of the standard in accordance with the determined safety level. Essential points here are verification and documentation. Within the framework of validation, proof of safety functions must be provided at the end. Early safety analyses to verify the safety concept in the form of a system-FMEA (Fault Probability and Effects Analysis) or FTA (Fault Tree Analysis) are recommended.

At the end of the development process, the manufacturer can issue an EU Declaration of Conformity after conducting the prescribed conformity assessment procedure for the entire machine. Only then may the manufacturer release the machine onto the market. If third party certification of functional safety is to take place, this should be done at an early stage, such as the concept phase.

PL and SIL

Performance Level (PL) and Safety Integrity Level (SIL) describe the reliability of safety functions in machines and plants.
Each safety-related control system has a specific PL or SIL that represents the ability to reduce a risk.

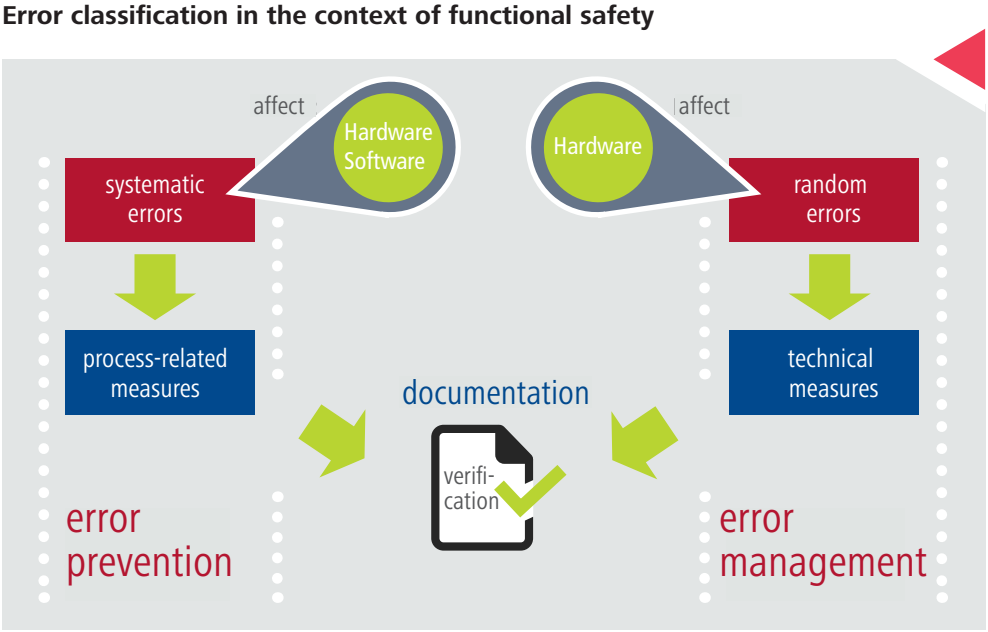
▶ Performance Level:
PL levels: a to e
Basis: EN ISO 13849

▶ Safety Integrity Level:
SIL levels: 1 to 3
Basis: EN 62061 (and EN 61508)

Achieving functional safety in three steps

1. **Identification and classification of hazards**
2. **Definition and implementation of risk reduction measures**
3. **Verification and documentation**

Error classification in the context of functional safety



source: ITK Engineering GmbH

How can the risk of hazards be reduced?

According to the Machinery Directive and the Basic Safety Standard EN ISO 12100, risk reduction for every hazard must be carried out in the following three stages (it is mandatory to do so in this order):

1. **Inherently safe design:** the design of machinery must be such that it does not present any hazards (inherently safe). If this is not possible, the risk must be reduced with technical protective measures.
2. **Technical protective measures:** Technical protective measures include both protective devices and safety functions in a machine which are implemented by means of a control system, whereby the methods of functional safety described above are to be applied.
3. **User information about the residual risk:** the machine manufacturer must inform the operator about risks which cannot be completely controlled by inherently safe design or technical measures. The operator of the machine must take note of the machine manufacturer's user information and, if necessary, take suitable organizational measures, such as training, work instructions, regular checks and personal protective equipment.

▶ To what extent does industrial security play a role?

With the increasing degree of networking in mobile machines and, above all, the increasing "opening" of previously internal data/communication networks and components, in addition to functional safety, industrial security is becoming increasingly important. The danger of an external attack and the possibilities of manipulation of software and data are increasing. This can have serious consequences for (functional) safety. Industrial security thus becomes the focus of attention at all levels and phases of development and operation. The main objectives of industrial security are confidentiality, integrity and availability of data and software functions.

▶ Functional Safety : Protecting people from the machine (occupational health and safety); design measures to make machines safer

▶ Industrial Security: Protecting the machine from third-party attacks; protection of information technology in industrial plants, machines and systems

In many applications, security methods must supplement the well-known methods of safety engineering. In order not to make the development process of safety-critical systems unnecessarily complex, a fundamental question must first be clarified when integrating industrial security activities:

Industrial Security → Protecting the machine from third-party attacks

Where and how must safety and industrial security aspects be considered together and where separately?

The prioritisation of objectives is very project-specific and is determined by means of risk analysis. The introduction and implementation of industrial security in the development process as well as in operation is a great challenge, because, when looking to the future, safety can only be possible in combination with industrial security.

Netzwerk Baumaschinen NRMM CV

This supplementary publication to the guideline "Person/Object Recognition, Warning in Danger Areas – Camera and Sensor Systems, Intelligent Software for Mobile Machinery" was developped by Netzwerk Baumaschinen NRMM.

Publisher:
Netzwerk Baumaschinen NRMM of the Offensive Gutes Bauen
www.safety-machinery.com
The Offensive Gutes Bauen is part of the National Initiative Neue Qualität der Arbeit

Coordination:
info@safety-machinery.com
Wilhelmshöher Allee 262, D-34131 Kassel, Germany, Fon: +49 (0)561 81041-11

Editing, concept, design:
www.fact3.de, www.itk-engineering.de

For content support, we would like to thank:
BAuA – Bundesanstalt für Arbeitsschutz und Arbeitsmedizin
BG RCI – Berufsgenossenschaft Rohstoffe und chemische Industrie
BMAS – Bundesministerium für Arbeit und Soziales
KAN – Kommission Arbeitsschutz und Normung
ITK Engineering GmbH

Picture credits:
Graphics: ITK Engineering GmbH; Titel ©fotolia.com/K. Thalhofer/santiago silver; p.3 ©fotolia.com/everythingpossible; p.7: Zeppelin GmbH

Status 03/2019.

Presented by:

VISION ZERO. Wir machen mit!
NULL UNFÄLLE – GESUND ARBEITEN!