INITIATIVE NEUE QUALITÄT DER ARBEIT

OFFENSIVE GUTES BAUEN

Netzwerk Baumaschinen

Funktionale Sicherheit

Safety und Industrial Security bei der Entwicklung – Risikobegrenzung von Steuersystemen
Information für Betreiber, Hersteller und Aufsichtspersonen

Netzwerk Baumaschinen NRMM

Das Netzwerk Baumaschinen unterstützt die Qualität von Prozessen, die die Wirtschaftlichkeit und Sicherheit im Einsatzbereich von mobilen Maschinen (NRMM – Non Road Mobile Machinery) betreffen. Bei Aufgabenstellungen von gemeinsamem Interesse diskutiert und entwickelt das Netzwerk mit den zuständigen Akteuren abgestimmte Informationen.

Das Themenblatt „Funktionale Sicherheit" ergänzt den im Netzwerk erarbeiteten Leitfaden „Personen- und Objekterkennung in Gefahrenbereichen – Kameratechnologien, Warn- und Sensoriksysteme". Der Leitfaden erläutert, wie bei eingeschränkten Sichtverhältnissen durch den zusätzlichen Einsatz von technischen Hilfsmitteln Personen und Objekte im Gefahrenbereich besser erkannt werden können.

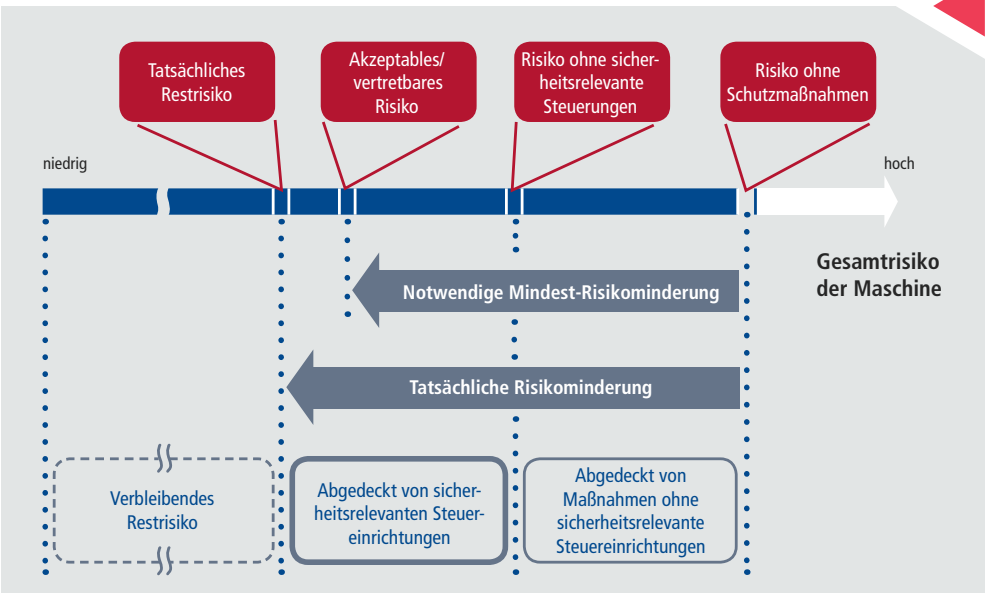
Funktionale Sicherheit

Warum ist Funktionale Sicherheit wichtig?

Oberstes Ziel der Funktionalen Sicherheit (gebräuchliche Abkürzung „FuSi“) besteht darin, das Risiko einer Personengefährdung zu reduzieren. Die Funktionale Sicherheit betrifft das Steuerungssystem mobiler Maschinen, von dem eine sicherheitsrelevante Funktion abhängt. Durch die steigende Anzahl an Steuergeräten in heutigen Anwendungen wird die Funktionale Sicherheit immer wichtiger. Besonders relevant ist dies bei autonomen Systemen zur Unfallvermeidung.

Sobald Sicherheitsfunktionen in einer Maschine mittels einer Steuerung realisiert werden, muss der Hersteller die Steuerungskomponenten entsprechend eines zuvor ermittelten Sicherheitslevels gestalten (siehe hierzu auch Seite 5). Die Bestimmung des erforderlichen Sicherheitslevels sowie die dementsprechende Realisierung der sicherheitsrelevanten Steuerungsfunktion erfolgt auf Grundlage der dafür vorgesehenen Normen, z. B. EN ISO 13849.

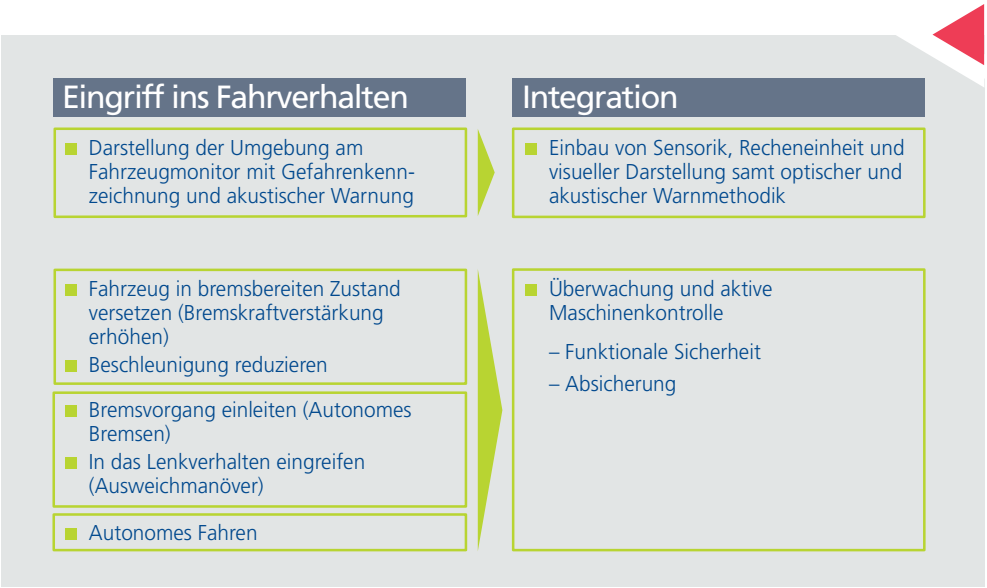
EN ISO 13849
„Sicherheit von Maschinen – Sicherheitsbezogene Teile von Steuerungen“
Teil 1: Allgemeine Gestaltungsleitsätze
Teil 2: Validierung



Ziel der Funktionalen Sicherheit: Das Risiko einer Personengefährdung reduzieren (Quelle: BGIA-Report 2/2008 zur EN ISO 13849).

Welche Systeme unterliegen der Funktionalen Sicherheit?

Wird bei Gefahr aktiv in das Verhalten eines Systems eingegriffen – um das System in einen sicheren Zustand zu bringen, z. B. in Form eines autonomen Brems- oder Ausweichmanövers – muss dies auf jeden Fall nach den Kriterien der Funktionalen Sicherheit bewertet und realisiert werden. Außerdem hat dies massive Auswirkungen auf die Fahrzeugarchitektur der mobilen Maschine.



Integration von Sicherheitssystemen in Abhängigkeit zum Eingriff ins Fahrverhalten (Quelle: ITK Engineering GmbH).

Welche Normen sind bei mobilen Maschinen zu beachten?

Bezüglich der Maschinensicherheit gibt es eine Vielzahl relevanter Normen. Die grundlegenden Sicherheitsanforderungen finden sich in der MRL („Maschinenrichtlinie" – Richtlinie 2006/42/EG). Konkretisiert werden diese Anforderungen für den jeweiligen Maschinentyp, z.B. durch:

- **EN 474** (für Erdbaumaschinen)
- **EN 500** (für mobile Straßenbaumaschinen)
- **EN 1889** (für mobile Maschinen im Bergbau unter Tage)
- **EN 16228** (für Geräte für Bohr- und Gründungsarbeiten)
- **ISO 25119/ EN 16590** (für Traktoren, Maschinen der Agrar- und Forstwirtschaft)

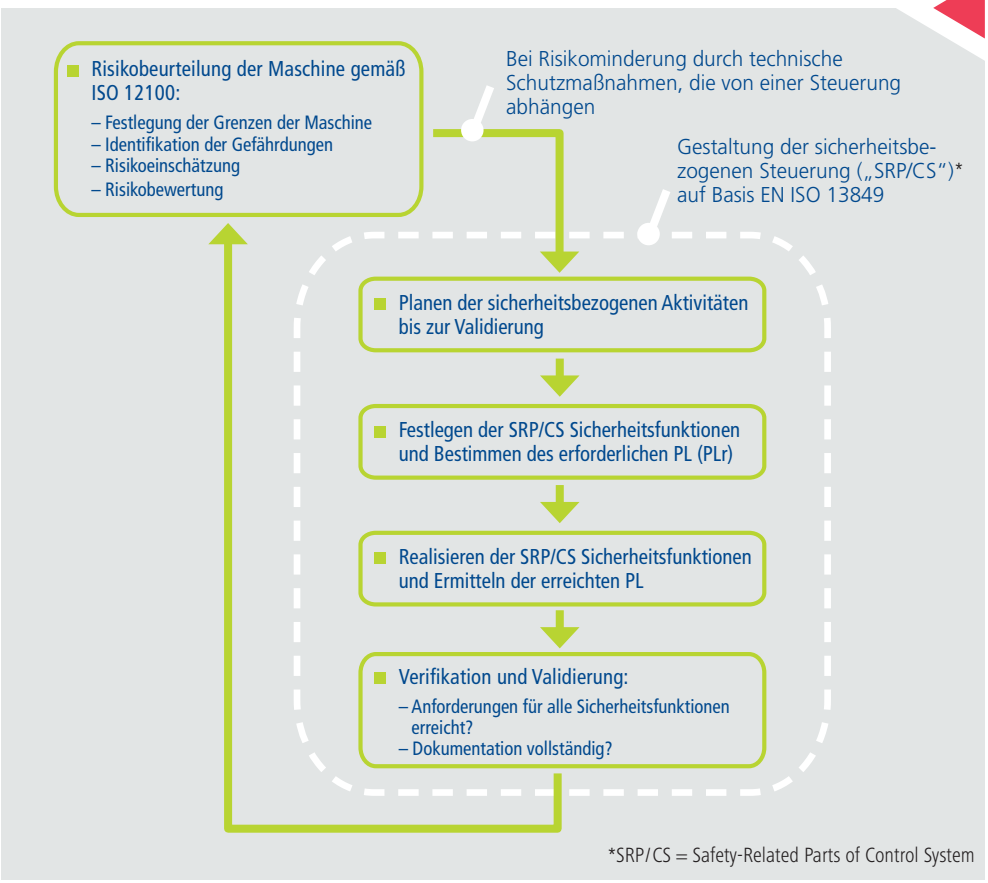
Diese Europäischen Normen sind unter der EU-Maschinenrichtlinie 2006/42/EG (MRL) harmonisiert. Damit können Hersteller bei ihrer Anwendung davon ausgehen, dass die von der Norm behandelten Anforderungen der MRL abgedeckt sind. Es gilt die sogenannte **„Vermutungswirkung"**.

▶ **Alle unter der MRL harmonisierte Normen: https://ec.europa.eu/growth/single-market/european-standards/harmonised-standards/machinery_de** (sollten Sie nicht auf den Link zugreifen können, bitte wenden an: info@netzwerk-baumaschinen.de)

Um Konformität zur MRL zu erreichen, ist bei Lenkanlagen in gummibereiften Maschinen wie z.B. Baggern ergänzend die **EN 12643 (ISO 5010)** anzuwenden. Speziell zur Funktionalen Sicherheit von Erdbaumaschinen gibt es die **ISO 15998**, die jedoch nicht harmonisiert ist und deshalb formal nicht zur Erreichung der Konformität zur MRL angeführt werden kann. Teile von nicht harmonisierten Normen, die von harmonisierten Normen zitiert werden, können jedoch zur Erreichung der Konformität zur MRL herangezogen werden. Unabhängig vom jeweiligen Maschinentyp sollte bezüglich der Funktionalen Sicherheit auf die Basisnorm **EN ISO 13849** zurückgegriffen werden. In dieser sind fünf Sicherheitsstufen, als sogenannte **„Performance Level (PL)"** von PL a bis PL e, definiert.

Was müssen Hersteller bei der Entwicklung berücksichtigen?

Bei der Entwicklung sind die von den Normen zur Funktionalen Sicherheit geforderten Prozesse einzuhalten und entsprechende Dokumente zu erstellen. Dazu gehört eine **frühzeitige Risikobeurteilung** (nach EN ISO 12100) sowie eine geeignete Planung der relevanten Aktivitäten, um eine effiziente und nachvollziehbare Entwicklung sicherzustellen. Für jede Gefährdung, bei der die Risikominderung durch eine sicherheitsbezogene Steuerung erreicht werden soll, ist eine geeignete Sicherheitsfunktion zu definieren und das Sicherheitslevel (z. B. PL gemäß EN ISO 13849-1) zu bestimmen.



Prozess zur Gestaltung sicherheitsbezogener Steuerungen (Quelle: ITK Engineering GmbH)

Passend zu dem ermittelten Sicherheitslevel werden dann die Sicherheitsfunktionen nach den relevanten Anforderungen der Norm entwickelt. Wesentliche Punkte dabei sind die Verifikation und Dokumentation. Im Rahmen der Validierung muss am Ende ein Nachweis für die Sicherheitsfunktionen erbracht werden. Frühzeitige Sicherheitsanalysen zur Verifikation des Sicherheitskonzepts in Form einer System-FMEA (Fehlermöglichkeits- und Einflussanalyse) oder FTA (Fehlerbaumanalyse) sind dabei empfehlenswert.

Am Ende des Entwicklungsprozesses kann der Hersteller nach Durchführung des vorgeschriebenen Konformitätsbewertungsverfahren der gesamten Maschine eine EU-Konformitätserklärung ausstellen. Erst dann darf er die Maschine in Verkehr bringen. Soll eine Drittstellenzertifizierung der Funktionalen Sicherheit erfolgen, sollte diese frühzeitig, bereits in der Konzeptphase, eingebunden werden.

Die Erstellung einer Risikobeurteilung durch den Hersteller ist gesetzlich vorgeschrieben:
▶ EN ISO 12100 „Sicherheit von Maschinen – Allgemeine Gestaltungsleitsätze – Risikobeurteilung und Risikominderung"

PL und SIL

Performance Level (PL) und Safety Integrity Level (SIL) beschreiben die Zuverlässigkeit von Sicherheitsfunktionen bei Maschinen und Anlagen. Jedes sicherheitsbezogene Steuerungssystem besitzt ein spezifisches PL oder SIL, über welches die Fähigkeit dargestellt wird, ein Risiko zu vermindern.

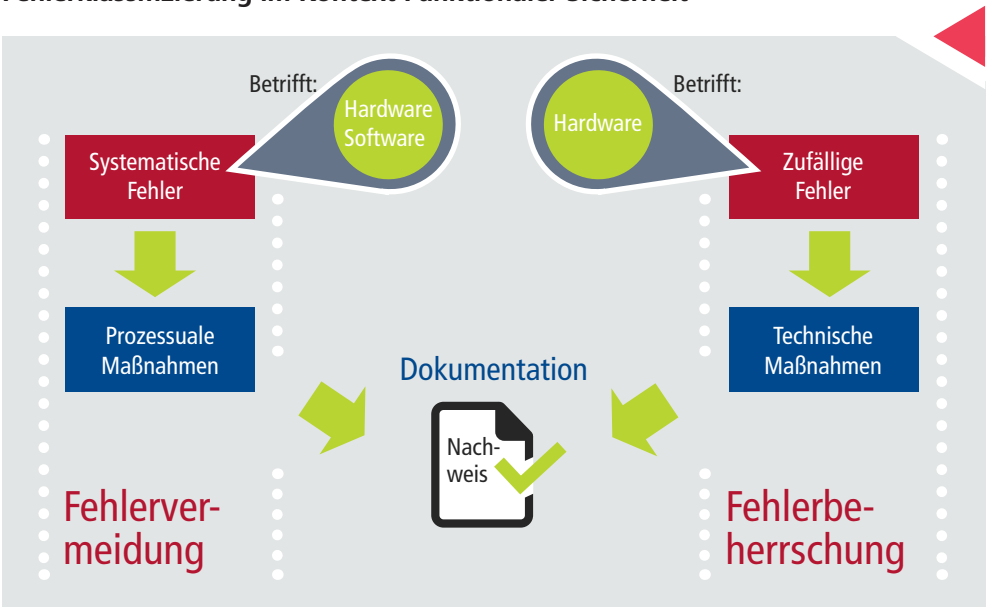
▶ Performance Level:
PL-Stufen: a bis e
Grundlage: EN ISO 13849

▶ Safety Integrity Level:
SIL-Stufen: 1 bis 3
Grundlage: EN 62061 (und EN 61508)

In drei Schritten zur Funktionalen Sicherheit

1. **Erfassung und Klassifizierung von Gefährdungen**
2. **Definition und Umsetzung von Maßnahmen zur Risikoreduktion**
3. **Nachweis und Dokumentation**

Fehlerklassifizierung im Kontext Funktionaler Sicherheit



Quelle: ITK Engineering GmbH

Wie lässt sich das Risiko einer Gefährdung reduzieren?

Gemäß Maschinenrichtlinie und Sicherheits-Grundnorm EN ISO 12100 muss die Risikominderung für jede Gefährdung in den folgenden drei Stufen erfolgen (zwingend in der angegebenen Reihenfolge):

1. **Inhärent sichere Konstruktion:** Die Konstruktion einer Maschine muss so gestaltet werden, dass von ihr keine Gefährdungen ausgehen (inhärent sicher). Ist dies nicht möglich, muss mit technischen Schutzmaßnahmen das Risiko reduziert werden.
2. **Technische Schutzmaßnahmen:** Zu den technischen Schutzmaßnahmen zählen sowohl Schutzeinrichtungen als auch Sicherheitsfunktionen in einer Maschine, die mittels einer Steuerung realisiert werden, wobei die oben beschriebenen Methoden der Funktionalen Sicherheit anzuwenden sind.
3. **Benutzerinformation über das Restrisiko:** Über Risiken, die nicht vollständig durch inhärent sichere Konstruktion oder technische Maßnahmen beherrschbar sind, muss der Maschinenhersteller den Betreiber über die Benutzerinformation informieren. Der Maschinenbediener bzw. -betreiber muss die Benutzerinformationen des Maschinenherstellers beachten und gegebenenfalls geeignete organisatorische Maßnahmen treffen, z. B. Ausbildung, Arbeitsanweisungen, regelmäßige Kontrollen, persönliche Schutzausrüstung, etc.

Inwieweit spielt „Industrial Security“ eine Rolle?

Mit steigendem Vernetzungsgrad in mobilen Maschinen und vor allem durch die zunehmende Öffnung vormals interner Daten-/Kommunikations-Netzwerke und Komponenten gewinnt neben Funktionaler Sicherheit auch Industrial Security an Bedeutung. Die Gefahr eines Angriffs von außen und damit möglicherweise einhergehende Manipulation von Software und Daten steigt. Dies kann gravierende Folgen für die Safety (Funktionale Sicherheit) haben. Industrial Security rückt damit in allen Ebenen und Phasen der Entwicklung und des Betriebs in den Fokus. Hauptziele von Industrial Security sind Vertraulichkeit, Integrität und Verfügbarkeit von Daten und Software-Funktionen.

Security-Methoden müssen in vielen Anwendungsfällen die bekannten Methoden des Safety Engineerings ergänzen. Um den Entwicklungsprozess sicherheitskritischer Systeme nicht unnötig komplex zu gestalten, gilt es bei der Integration der Industrial Security-Aktivitäten zunächst eine grundlegende Frage zu klären:

> **Wo und wie müssen die Safety- und Industrial Security-Aspekte gemeinsam und wo getrennt voneinander betrachtet werden?**

Die Priorisierung von Zielen ist sehr projektspezifisch und wird mittels Risikoanalyse ermittelt. Die Einführung und Umsetzung von Industrial Security im Entwicklungsprozess sowie im Betrieb ist eine große Herausforderung, da in Zukunft nur mit Industrial Security, Safety möglich sein kann.

Safety:
Schutz des Menschen vor der Maschine (Arbeitsschutz); Konstruktive Maßnahmen um Maschinen sicherer zu gestalten

Industrial Security:
Schutz der Maschine vor Angriffen durch Dritte; Absicherung von Informationstechnik in industriellen Anlagen, Maschinen und Systemen (vgl. VDMA: „Leitfaden Industrie 4.0 Security“)

INITIATIVE NEUE QUALITÄT DER ARBEIT

OFFENSIVE GUTES BAUEN

Netzwerk Baumaschinen

Diese Ergänzung zum Leitfaden „Personen- und Objekterkennung in Gefahrenbereichen – Kameratechnologien, Warn- und Sensoriksysteme“ wurde im Netzwerk Baumaschinen NRMM entwickelt.

Herausgeber:
Netzwerk Baumaschinen NRMM der Offensive Gutes Bauen
www.netzwerk-baumaschinen.de
Die Offensive Gutes Bauen ist Bestandteil der nationalen Initiative Neue Qualität der Arbeit

Koordination und Kontakt:
Karlheinz Pfeiffer
Wilhelmshöher Allee 262, 34131 Kassel, Fon: 0561 8104111
pfeiffer@netzwerk-baumaschinen.de

Redaktion, Konzeption, Gestaltung:
www.fact3.de, www.itk-engineering.de

Wir bedanken uns für die inhaltliche Unterstützung bei:
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

Bildnachweis:
Grafiken ITK Engineering GmbH; Titel ©fotolia.com/K. Thalhofer/santiago silver; S.3 ©fotolia.com/everythingpossible;
Seite 7: Zeppelin GmbH

Stand 07/2017.

Überreicht durch: