REVISION DER ISO 13849 (ISO/DIS 13849-1:2020)

ÜBERSICHT DER ÄNDERUNGEN – MASCHINENSTEUERUNGEN TEIL I

Die Norm EN ISO 13849 stellt Sicherheitsanforderungen und einen Leitfaden für die Gestaltung und Integration sicherheitsbezogener Teile von Steuerungen von Maschinen bereit, einschließlich der Entwicklung von Software. Die Norm gilt für alle Arten von Maschinen, unabhängig von der verwendeten Technologie (z. B. elektrisch, hydraulisch, pneumatisch, mechanisch). Die Revision der ISO 13849, die ISO/DIS 13849-1:2020(E), beinhaltet Neuerungen, die im vorliegenden ersten Teil des Beitrags ausgeführt sind und im zweiten Teil einer folgenden Heftausgabe komplettiert werden.

Autor: *Dipl.-Ing. Christa Düsing, Entwicklungsingenieur, FMEA-Koordinator*
Co-Autor: *Dr.-Ing. Martin Inderelst, Technologie Entwicklung Hydraulikbagger, XCMG European Research Center GmbH, Europark Fichtenhain B4, 47807 Krefeld*

PRÄAMBEL

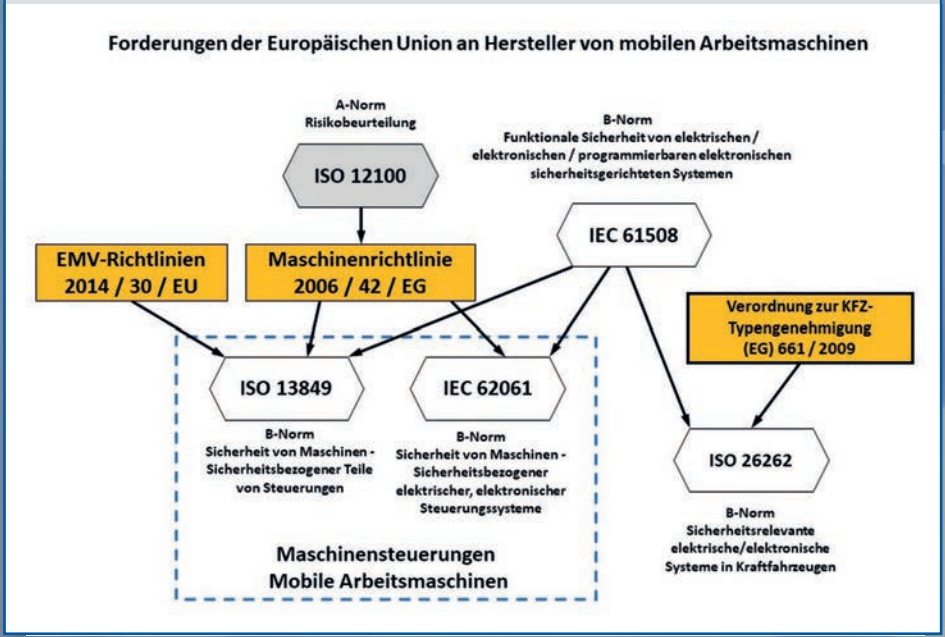
Während der Entwicklung und Konstruktion neuer Maschinen und Maschinensteuerungen orientieren sich Hersteller zuerst an produktspezifischen Normen, den sogenannten C-Normen. Diese verweisen dabei auf weitere weniger konkrete Sicherheitsgrundnormen, den B-Normen und A-Normen, und sollen ebenfalls von den Maschinenherstellern angewendet werden.

Zur Erfüllung der Maschinenrichtlinien 2006/42/EG der EU finden verschiedene internationale Sicherheitsnormen im Bereich der Maschinensteuerungen Anwendung, **vgl. Abbildung 01**. Die A-Norm ISO 12100 [2] dient dabei als Basis für Risikobeurteilungen, die B-Norm ISO 13849 [3] bildet einen Leitfaden zur Konzeption von Maschinensteuerungen.

Im Entwicklungsprozess von mechanischen, hydraulischen, elektrischen sowie digitalen Maschinensteuerungen beschreibt die ISO 13849 [3] die wichtigsten Schritte zur Wahrung der funktionalen Sicherheit. Dabei klassifiziert sie die Sicherheitsfunktionen in Kategorien, die unter Zuordnung einer vorgegebenen Architektur das Hardwaresystem wiederspiegeln und es ermöglichen, einen sogenannten Performance Level (PL) zu bestimmen. Durch das zielgerechte Identifizieren, Einrichten und Überprüfen von Sicherheitsfunktionen erreicht die B-Norm ISO 13849 somit einen konstruktiven Beitrag zur Risikominderung innerhalb der Maschinensteuerung [1].

01 **Internationale Normen zur Maschinensteuerung**

In Anlehnung an Europäische Richtlinien – Grundnormen zur funktionalen Sicherheit



Der neue Entwurf der ISO 13849, die ISO/DIS 13849-1:2020(E) [4], beinhaltet einige Neuerungen. Der logische Aufbau bzw. die Gliederung wurden überarbeitet, die Kapitel zur Validierung aus ISO 13849 Teil 2 [5] wurden in die neue ISO/DIS 13849 Teil 1 [4] überführt und integriert. Weiterhin gibt es zusätzliche Erläuterungen und Interpretationen zum besseren Verständnis normativer Anforderungen. Alle Änderungen sollen eine Empfehlung und einen richtungsweisenden Weg durch die verschiedenen Phasen der international vereinheitlichten Anforderungen ebnen, welche sich auf die Risikobeurteilung, die erforderlichen Performance Levels, die Identifikation sicherheitsrelevanter Steuerungsteile, bis hin zur Implementierung der Sicherheitsfunktionen beziehen. Bei der Neugestaltung der DIN EN ISO 13849-1:2016-06 [3] wurde erstmals unter Berücksichtigung der Gefährdung auch eine Ausfallwahrscheinlichkeit umfassend berücksichtigt.

Die wichtigsten Änderungen der Revision der DIN EN ISO 13849-1:2016-06 [3] sind wie folgt aufgelistet und werden im weiteren Verlauf bis einschließlich Unterpunkt 2.2 in diesem Artikel erläutert:

1.0 Überarbeitung
2.0 Änderungen und Detaillierungen
2.1. Detaillierte Anforderungen an die Spezifikation von Sicherheitsfunktionen (SRS – Safety Requirements Specification)
2.2. Beschreibung der Anforderungen an Design und die Performance Level
- Kombination mehrerer Teilsysteme
- Alternatives Verfahren zur Quantifizierung von Teilsystemen ohne $MTTF_D$ Wert (Die mittlere Zeit bis zum gefahrbringenden Ausfall)

2.3. Detaillierte Beschreibung von Validierungsprozessen (Übernahme aus DIN EN ISO 13849-2:2013) [5]
3.0 Integration neuer Aspekte
3.1. Neuer Abschnitt zur Bestimmung des erforderlichen PL_r; Integration der Bestimmung von Parameter P über fünf Faktoren und Auswahl der Parameter P1 oder P2
3.2. Neuer Abschnitt zum Aspekt Ergonomie
3.3. Anhang L zu Immunitätsanforderungen für elektromagnetische Kompatibilität (EMV-Anforderungen)
3.4. Anhang M mit zusätzlichen Informationen zur Risikoreduzierung für das SRS-System (Safety Requirements Specifications)
3.5. Anhang N zur Vermeidung von systematischen Fehlern im Software-Design
3.6. Neuer Abschnitt zu den Anforderungen an die Risikobewertung und Risikominderung sowie Berücksichtigung der Ergebnisse aus der Risikobeurteilung
3.7. Neuer Abschnitt zur Softwaresicherheit (Detaillierte Anforderungen)

1 ÜBERARBEITUNG

Normative Verweise, Begriffe und Definitionen wurden überarbeitet und aktualisiert. Es wurden strukturelle Verbesserungen vorgenommen und der logische Aufbau wurde angepasst.

2 ÄNDERUNGEN UND DETAILLIERUNGEN

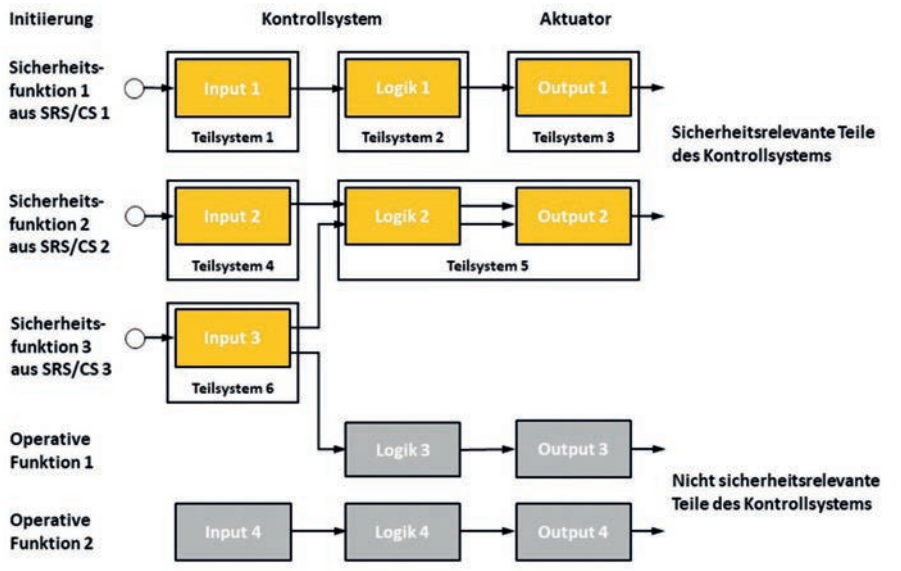
2.1 DETAILLIERTE ANFORDERUNGEN AN DIE SPEZIFIKATION VON SICHERHEITSFUNKTIONEN

Zur ausführlichen Erläuterung, Vereinfachung und Spezifizierung der Übergangsvoraussetzung bzgl. der Risikobeurteilung und dem Risikominderungsprozess nach ISO 12100 [2] wurde in den Entwurf der neuen ISO/DIS 13849-1:2020(E) der Punkt „Safety Requirement Specification (SRS)“ – „General requirements“ eingeführt. Er bietet eine Liste mit detaillierten Spezifikationen zur Erstellung der Risikobeurteilung für Sicherheitsfunktionen und relevante Beispiele für die Anforderungen sämtlicher Sicherheitsfunktionen.

Darüber hinaus bietet der Entwurf der neuen ISO/DIS 13849-1:2020(E) [4] detaillierte Beschreibungen für verschiedene Sicherheitsfunktionen und fordert zudem, jede Einzelheit einer SRS bzgl. der auszuführenden Sicherheitsfunktionen zu dokumentieren.

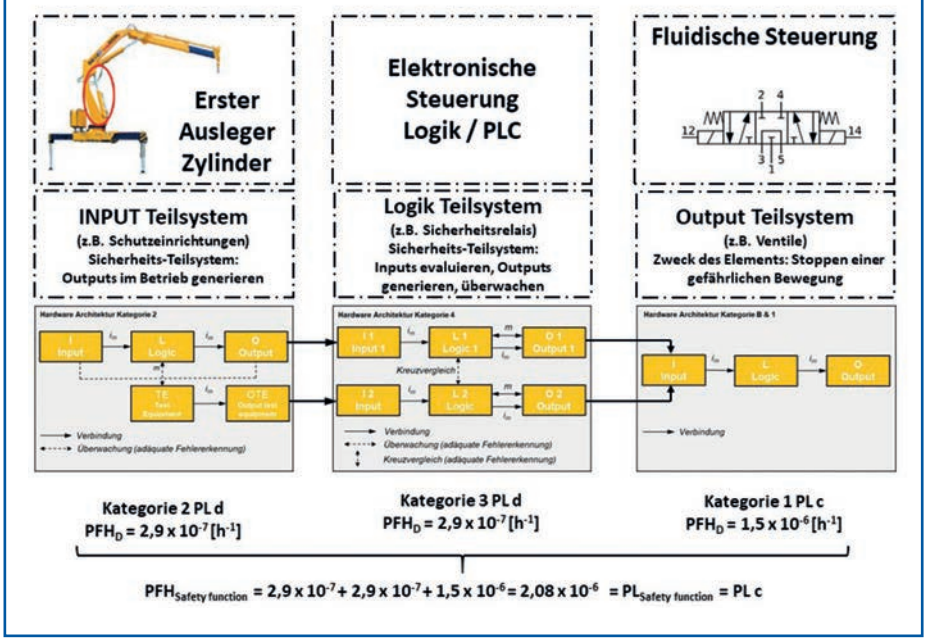
02 **Beispiel für die Aufschlüsselung einer Sicherheitsfunktion und ihre Zuordnung zu Teilsystemen**

Quelle: ISO/DIS 13849-1:2020(E) [4]



03 **Kombination von Teilsystemen zur Erzielung eines einheitlichen PL**

Quelle: ISO/DIS 13849-1:2020(E) [4]



Gegenüber der alten Norm wird ein detaillierter Aufbau des Safety-related Parts of Control System (SRP/CS) beschrieben. In einem SRP/CS müssen nun alle Sicherheitsfunktionen in Teilfunktionen bzw. Unterfunktionen gegliedert werden, welche den Teilsystemen zugeordnet werden. Jede Teilfunktion muss künftig die Beschreibung der Sicherheitsanforderungen für die Unterfunktion aufweisen bzw. darstellen. Dies betrifft zudem die Abbildung der Ein- und Ausgänge für jede Unterfunktion.

2.2 BESCHREIBUNG DER ANFORDERUNGEN AN DESIGN UND PERFORMANCE LEVEL KOMBINATION MEHRERER TEILSYSTEME

Ein SRP/CS setzt sich aus validierten Teilsystemen zusammen, oder es besteht aus Systemelementen, die ein Teilsystem bilden. Die Möglichkeit zur Aufschlüsselung einer Sicherheitsfunktion wird in **Abbildung 02** dargestellt. Sie zeigt hierzu einen beispielhaften Aufbau von Sicherheitsfunktionen aus mehreren Teilsystemen und Systemelementen. Für die Aufschlüsselung der Teilsysteme gilt per Definition: Ein beliebiger Ausfall eines beliebigen Teilsystems kann zum Verlust der gesamten Sicherheitsfunktion führen, auch innerhalb einer Kategorie.

Das Diagramm zeigt verschiedene Kombinationen von Teilsystemen, die als SRP/CS für eine Sicherheitsfunktion kombiniert werden können. Eingänge bzw. Inputs in den Teilsystemen 1, 4 und 6 können beispielsweise durch Sensoren und Schaltsignale abgebildet werden. Die Weiterverarbeitung der Inputs erfolgt in der Logik, vgl. Teilsysteme 2 und 5 in Abbildung 02. Schließlich werden die entsprechenden Ausgänge für Aktuatoren, wie beispielsweise Ventile, generiert (Teilsysteme 3 und 5).

In der neuen ISO/DIS 13849-1:2020(E) [4] werden die Anforderungen für spezielle Sicherheitsfunktionen detailliert beschrieben. Hierzu gehören unter anderem:

- Sicherheitsrelevante Stoppfunktionen
- Manuelle Reset-Funktionen (Rückstellfunktionen)
- Neustart-Funktionen
- Lokale Steuerungsfunktionen
- Stummschaltfunktionen
- Abweichungen von sicherheitsrelevanten Parametern
- Verluste und Wiederherstellungen von Energiequellen
- Anforderungen für die Auswahl der Betriebsart
- Wartungserwägungen für Sicherheitsfunktionen

Gegenüber der alten Norm werden die Anforderungen zur Kombination mehrerer Teilsysteme mit unterschiedlichen Performance Level (PL) zielgerechter beschrieben. Die Erzielung eines einheitlichen PL für die Realisierung einer Sicherheitsfunktion basiert auf zuvor validierten Teilsystemen nach IEC 62061 [6], IEC 61508 [7] oder anderen relevanten Produktnormen. **Abbildung 03** stellt dies exemplarisch am Sicherheitssystem des Auslegerzylinders eines LKW-Ladekrans dar.

ALTERNATIVES VERFAHREN ZUR QUANTIFIZIERUNG VON TEILSYSTEMEN OHNE VORHANDENEN MTTFD-WERT

Das alternative Verfahren im neuen Entwurf der Norm ist beschränkt auf Teilsysteme aus den Bereichen Mechanik, Hydraulik, Pneumatik, Elektro-Hydraulik sowie Elektropneumatik, für welche keine Zuver-

lässigkeitsdaten bzw. die mittlere Zeit bis zum Ausfall der Komponente oder des Systems ($MTTF_D$) verfügbar sind. Gemäß ISO/DIS 13849 [4] wird für diese Verfahren die Beziehung verschiedener Hardware-Kategorien und Performance Level analog zum derzeitigen Stand in einer Tabelle beschrieben. Die Beschreibung erfolgt hinsichtlich der berechneten Wahrscheinlichkeit eines gefährlichen Ausfalls pro Stunde (=PFH_D-Wert) und bezüglich der Inputs und Outputs des Sicherheitssystems. Diese Beziehungen werden in **Abbildung 04** durch rote Punkte in das konventionelle System mit vorhanden $MTTF_D$-Werten grafisch eingeordnet. Man erkennt, dass die alleinige Berücksichtigung dieser Werte hohe Aufwände seitens der Hersteller zur Umsetzung von Risikovermeidung erwirkt.

Weiterhin können durch die Neuerungen nun unter diesen Bedingungen für Kategorie B, 2 und 3 ein $MTTF_D$-Wert von 10 Jahren für jeden Kanal angesetzt werden. Für Kategorie 1 müssen entsprechend bewährte Komponenten (aktuelle Version der ISO 13849 [4]: betriebsbewährte Komponenten) vorgesehen werden, um einen angenäherten $MTTF_D$-Wert von 30 Jahren erreichen und berücksichtigen zu können, wobei maximal ein Performance Level PL c erreicht wird. Bei Fehlern gemeinsamer Ursache „Common Cause Failure“ (CCF) sind auch weiterhin, wie in der aktuell gültigen ISO 13849 [3] für Kategorie 2 und 3, der Diagnosedeckungsgrad „Diagnostic Coverage“ (DC) zu berücksichtigen. Der DC muss für Kategorie 2 und 3 mindestens 60 % betragen. Diese zusätzlichen Regelungen und Zusammenhänge werden in Abbildung 04 durch Einführung der gelben Punkte verdeutlicht.

Entsprechend dem neuen Entwurf der Norm darf bei Kategorie 4 diese Methode nicht berücksichtigt bzw. angewendet werden. Für Kategorie 4 müssen generell bewährte Komponenten, Grundprinzipien und bewährte Sicherheitsprinzipien verwendet werden. Dies bedeutet, ein $MTTF_D$ Wert muss vorliegen bzw. berechnet worden sein. Diese alternative Methode versetzt den Hersteller nun in die Lage, eine Bewertung des Performance Levels auch ohne Vorliegen eines $MTTF_D$ Wertes anzuwenden bzw. vorzunehmen.

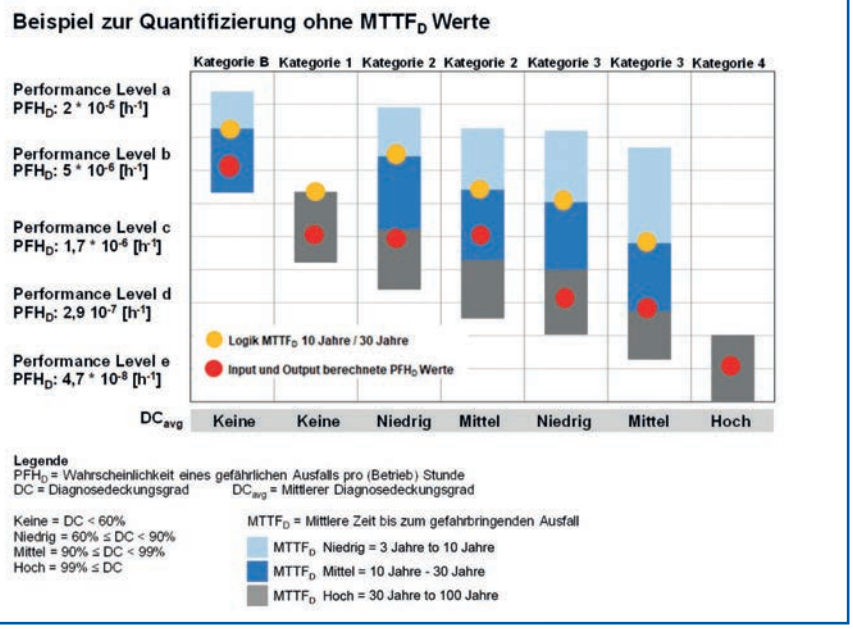
Die bisher beschriebenen Änderungen stellen deutlich klarere Rahmenbedingungen für die Entwicklung von sicherer Maschinensteuerungen. Weitere Änderungen können Sie in der nächsten Ausgabe der O+P-Fluidtechnik erfahren.

Fotos: *Aufmacher: Adobe Stock*

www.xcmg-erc.com

04 **Quantifizierung ohne $MTTF_D$ Wert**

Quelle: ISO/DIS 13849-1:2020(E) [4] [8]



Begriffsdefinition/Abkürzungen

Abk.	Bedeutung	Erläuterung
DC	Diagnosedeckungsgrad	Die Summe aller erkannter gefahrbringender Ausfälle im Verhältnis zur Gesamtzahl aller gefahrbringenden Ausfälle
$MTTF_D$	Mittlere Zeit bis zum gefahrbringenden Ausfall	Statistische Erwartung der mittleren Zeit bis zum gefährlichen Ausfall
PL	Performance Level	Diskreter Level, der die Fähigkeit sicherheitsbezogener Teile von Steuerungen spezifiziert
PL_r	Erforderliche Performance Level	Erforderlicher Level, der die Fähigkeit sicherheitsbezogener Teile von Steuerungen spezifiziert
SRS	Spezifikation der Sicherheitsanforderungen	Sicherstellung, das alle Aspekte zur Prozesssicherheit berücksichtigt werden
SRP/CS	Sicherheitsbezogene Teile eines Steuerungssystems	Teile von Maschinensteuerungen, die Sicherheitsaufgaben übernehmen
PFH_D	Wahrscheinlichkeit eines gefährlichen Ausfalls pro Stunde	Berechnung der gefahrbringenden Ausfallwahrscheinlichkeit nach verwendeter Architektur (Referenzwert für den Performance Level)
CCF	Fehler gemeinsamer Ursache	Ausfall verschiedener Einheiten aufgrund eines einzigen Ereignisses, wobei sich diese Ausfälle nicht gegenseitig beeinflussen
EMV	Elektromagnetische Verträglichkeit	Die Fähigkeit eines technischen Systems, andere Systeme nicht durch ungewollte elektrische oder elektromagnetische Effekte zu stören oder durch andere Systeme gestört zu werden
P1	Parameter P1 – Möglichkeit unter speziellen Konditionen	Möglichkeit der Gefahrenvermeidung oder Schadensbegrenzung
P2	Parameter P2 – Kaum möglich	Kaum Möglichkeit der Gefahrenvermeidung oder Schadensbegrenzung

Literaturverzeichnis

[1] Sicherheitsnormen im neuen Konzept (O + P 3/2006)
[2] DIN EN ISO 12100:2011-03 Sicherheit von Maschinen – Allgemeine Gestaltungssätze – Risikobeurteilung und Risikominderung
[3] DIN EN ISO 13849-1:2016-06 Sicherheit von Maschinen – Sicherheitsbezogene Teile von Steuerungen – Allgemeine Gestaltungssätze
[4] ISO/DIS 13849-1:2020(E) Sicherheit von Maschinen – Sicherheitsbezogene Teile von Steuerungen – Allgemeine Gestaltungssätze
[5] DIN EN ISO 13849-2:2013 Sicherheit von Maschinen – Sicherheitsbezogene Teile von Steuerungen - Validierung
[6] IEC 62061 Sicherheit von Maschinen – Sicherheitsbezogener elektrischer elektronischer Steuerungssysteme
[7] IEC 61508:2010-04 Funktionale Sicherheit von elektrischen / elektronischen / programmierbaren elektronischen sicherheitsgerichteten Systemen
[8] Revision der ISO 13849-1 Fachveranstaltung Maschinen Dr. Michael Huelke, Michael Hauke, Bamberg, 11. Juli 2019