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

ÜBERSICHT DER ÄNDERUNGEN – MASCHINENSTEUERUNGEN TEIL II

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 ersten Teil des Beitrags in der Ausgabe 2021/01-02 der O+P-Fluidtechnik bereits ausgeführt wurden und nun im vorliegenden zweiten Teil komplettiert werden.

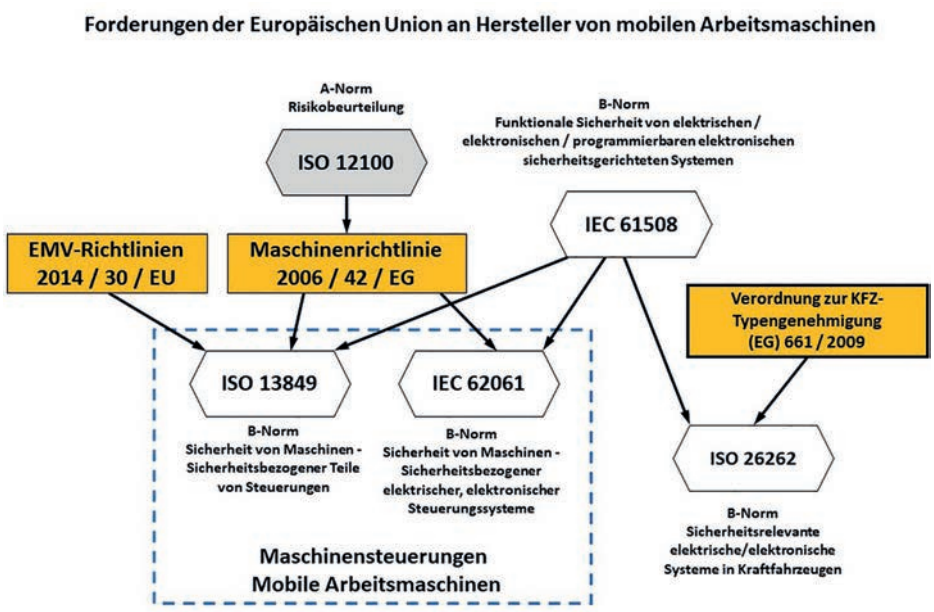
PRÄAMBEL

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.

01 **Internationale Normen zur Maschinensteuerung**

In Anlehnung an Europäische Richtlinien – Grundnormen zur funktionalen Sicherheit



Autoren: *Dipl.-Ing. Christa Düsing*
Co-Autoren: *Dr.-Ing. Martin Inderelst, XCMG European Research GmbH, Europark Fichtenhain B4, Krefeld*

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].

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 13849-1:2020(E) [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.

Einige wichtige Änderungen wurden bereits in der vorangegangenen Ausgabe 2021/01-02 der O+P-Fluidtechnik umfassend erläutert und sind im Folgenden zusammenfassend aufgelistet:

- Überarbeitung
- Änderungen und Detaillierungen
  -Detaillierte Anforderungen an die Spezifikation von Sicherheitsfunktionen
- (SRS – Safety Requirements Specification)
  -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)

Weitere wichtige Änderungen der Revision der DIN EN ISO 13849-1:2016-06 [3] werden im weiteren Verlauf des Artikels anhand der folgenden Gliederung erläutert:

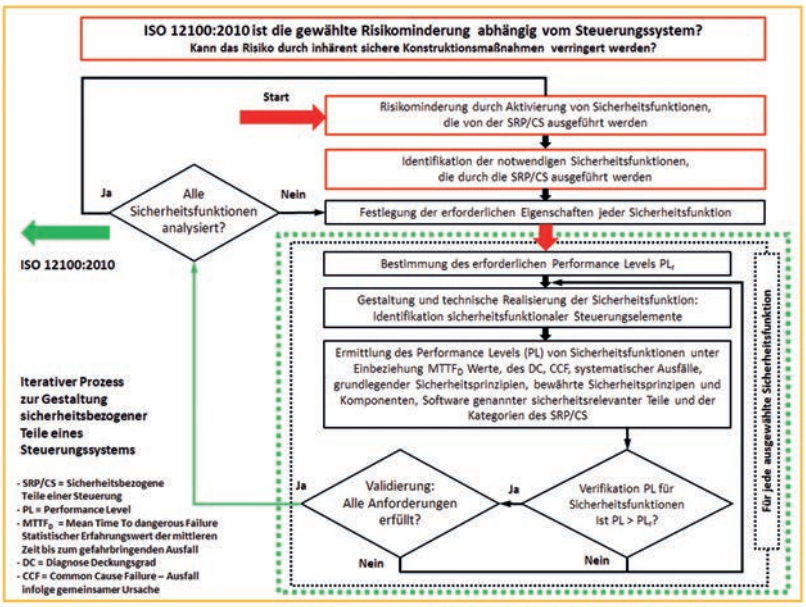
1. Detaillierte Beschreibung von Validierungsprozessen (Übernahme aus DIN EN ISO 13849-2:2013) [5]
2. Integration neuer Aspekte
2.1. Neuer Abschnitt zur Bestimmung des erforderlichen PLr; Integration der Bestimmung von Parameter P über fünf Faktoren und Auswahl der Parameter P1 oder P2
2.2. Neuer Abschnitt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

1 DETAILLIERTE BESCHREIBUNG VON VALIDIERUNGSPROZESSEN (ÜBERNAHME AUS DIN EN ISO 13849-2:2013)

Zur Berücksichtigung der Validierungsprozesse übernimmt ISO/DIS 13849-1:2020 sämtliche Validierungsprozesse der ISO 13849-2:2013, siehe **Tabelle 01**. Offen bleibt, welche Änderungen dies für die zukünftige Ausführung der ISO 13849-2 bedeutet.

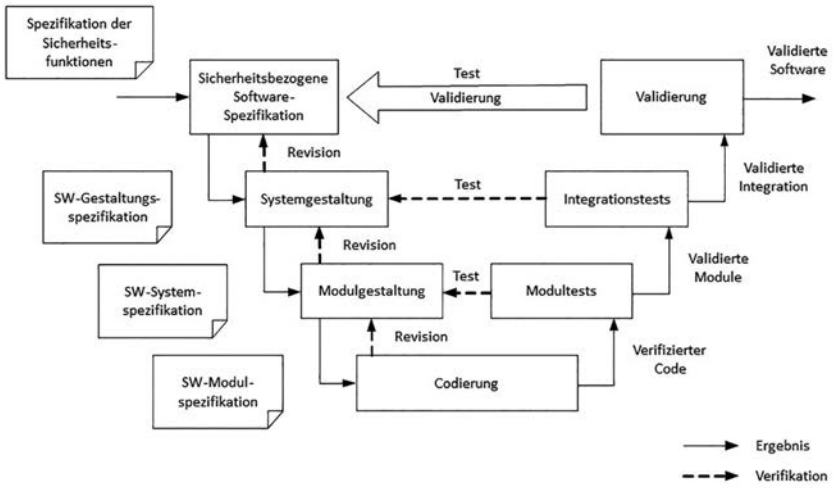
02 **Integration von ISO 13849-1 in den Prozess der Risikobewertung gemäß ISO 12100 unter Berücksichtigung der Ergebnisse**

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



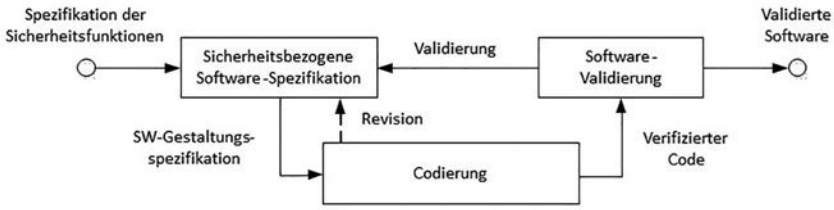
03 **Vereinfachtes V-Modell des Softwaresicherheits-Lebenszyklus**

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



04 **V-Modell für Software, wenn vorbewertete sicherheitsrelevante Hardware- und Softwaremodule in Kombination mit LVL verwendet werden**

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



2 INTEGRATION NEUER ASPEKTE:

2.1 ANFORDERUNGEN AN DIE RISIKOBEWERTUNG UND RISIKOMINDERUNG SOWIE BERÜCKSICHTIGUNG DER ERGEBNISSE AUS DER RISIKOBEURTEILUNG

Der Prozess der Risikobewertung ist in der ISO 12100 [2] definiert. Um die Beziehung zwischen der ISO 12100 [2] und der ISO 13849 [3] besser zu veranschaulichen, wurde die Risikominderung in Abhängigkeit vom Kontrollsystem nach ISO 13849 [3] in den Risikoprozess der ISO 12100 [2] einbezogen. So wird dargestellt, wie die Ergebnisse aus der Risikobeurteilung mit der ISO/DIS 13849-1:2020(E) [4] in den Prozess der Risikominderung einfließen **Abbildung 02**.

2.2 NEUER ABSCHNITT ZUR SOFTWARESICHERHEIT (DETAILLIERTE ANFORDERUNGEN)

Die neuen detaillierten Anforderungen zur Softwaresicherheit sehen vor, dass alle Aktivitäten im Lebenszyklus sicherheitsrelevanter eingebetteter Entwicklungssoftware (SRESW) oder sicherheitsrelevanter Anwendungssoftware (SRASW) in erster Linie die Vermeidung von jenen Fehlern sicherstellt, die während des Software-Lebenszyklus nach ISO/DIS 13849-1:2020(E) [4] auftreten können. Das Hauptziel der folgenden Anforderungen ist es, gemäß dem sogenannten V-Modell nach **Abbildung 03** lesbare, verständliche, testbare und wartungsfähige Software zu erstellen.

Ein vereinfachter Software-Lebenszyklus gemäß **Abbildung 04** kann nach ISO/DIS 13849-1:2020 [4] angewendet werden, wenn vorbewertete sicherheitsrelevante Hardware- und Softwaremodule in Kombination mit „Limited Variability Language (LVL)“ verwendet werden. Typischerweise gilt dies für die Verwendung einer modulbasierten Programmierung in LVL, die die Ein- und Ausgänge auf einen vordefinierten Satz von Werten, einschließlich einer Kombination von Modulen, begrenzt.

2.3 NEUER ABSCHNITT ZUR BESTIMMUNG DES ERFORDERLICHEN PL$_r$; INTEGRATION DER BESTIMMUNG VON PARAMETER P ÜBER 5 FAKTOREN UND AUSWAHL DER PARAMETER P1 ODER P2

Die Risikobeurteilung verfolgt das Ziel, zu wissen, ob ein gefährliches Ereignis erkannt werden kann, bevor die Gefahr verursacht wird und vermieden werden kann. Eine gefährliche Exposition kann zum Beispiel direkt anhand physikalischer Eigenschaften identifiziert werden, oder sie kann durch Indikatoren (z. B. Sensoren) erkannt werden. Im Rahmen der Risikominderung führt ISO/DIS 13849-1:2020 nun wichtige

Faktoren ein, vgl. **Tabelle 02**, die die Einstufung der Möglichkeit zur Vermeidung einer Gefährdung (Parameters P) beeinflussen und vereinfachen.

Aus **Tabelle 03** ist die Evaluierung der Parameter P1 und P2 zu entnehmen. Durch diese Vorgehensweise kann jede Gefährdung separat betrachtet und erkannt werden. Der erforderliche PL_r basiert auf der Definition von spezifischen Anwendungsapplikationen.

2.4 NEUER ABSCHNITT ZU ASPEKTEN DER ERGONOMIE

Durch die Anwendung ergonomischer Prinzipien kann vermieden werden, dass Steuerungssysteme umgangen werden oder dass Maschinen versehentlich fehlbedient oder missbraucht werden. Dabei ist die Schnittstelle zwischen den Bedienern und dem SRP/CS so zu gestalten und zu realisieren, dass die Gefährdungsexposition bei der bestimmungsgemäßen Verwendung und dem vernünftigerweise vorhersehbaren Missbrauch der Maschine aufgrund der Vernachlässigung ergonomischer Grundsätze minimiert wird. Relevante Ansätze hierzu führt ISO 12100:2010, 6.2.8, angegebene ergonomische Prinzipien auf.

2.5 ANHANG L ZU IMMUNITÄTSANFORDERUNGEN FÜR ELEKTROMAGNETISCHE KOMPATIBILITÄT (EMV-ANFORDERUNGEN)

EMV-Anforderungen (Normen) dienen zur Minimierung der Risiken die einen Einfluss auf die funktionale Sicherheit von Systemen, Teilsystemen und Komponenten haben Abbildung 05. Die durch ISO/DIS 13849-1:2020 [4] integrierten folgenden Richtlinien enthalten praktische Anleitungen zur Erfüllung der EMV-Störfestigkeitsmaßnahmen für ein SRP/CS oder für Teilsysteme. Mindestens eine oder mehrere Strategien sollten ausgewählt und vollständig angewendet werden.

- Richtlinie A: Befolgen der EMV-Anforderungen der entsprechenden Produktnorm (siehe IEC 61000-6-7,4.1, Satz1) [7].
- Richtlinie B: Für PL a und PL b sind die EMV-Anforderungen der IEC 61000-6-2 [6] zu befolgen.
- Richtlinie C: Für PL c, PL d und PL e müssen alle „verpflichtenden“ EMV-Maßnahmen und genügend andere EMV-Maßnahmen integriert werden, um eine Punktzahl von mindestens 70 (von möglichen 100) nach Tabelle „EMV“ L.1 zu erreichen (IEC 61000-6-7,4.1 [7], Anmerkung 1). Für PL e kann nur unter Anwendung der Anforderungen der Kategorie 4 erreicht werden.
- Richtlinie D: IEC 61000-6-7 [7] oder andere allgemeine EMV-Normen für funktionale Sicherheit befolgen.

05 **Beziehung zwischen Performance Level und EMV-Anforderungen**

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

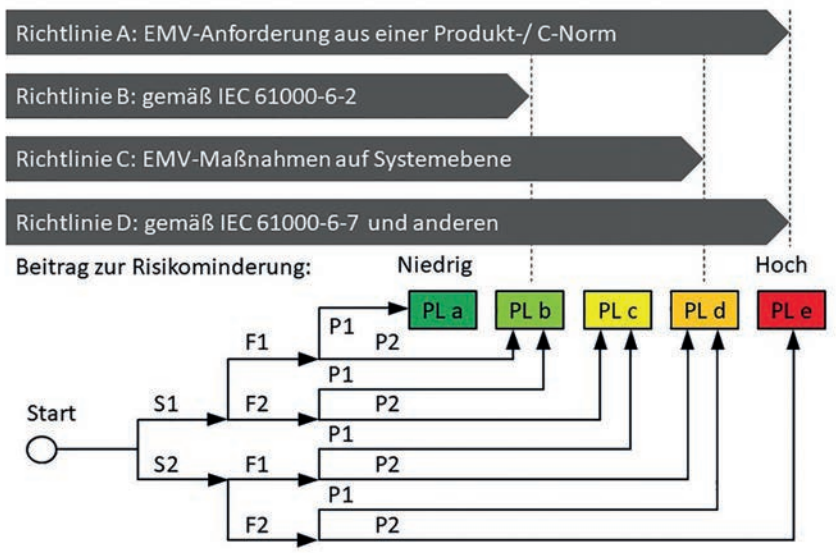


Tabelle 01: Zusammenführung der Validierungsprozesse

ISO/DIS 13849-1:2020	ISO 13849-2:2013
1 Anwendungsbereich	1 Anwendungsbereich
2 Normative Verweisungen	2 Normative Verweisungen
3 Begriffe und Definitionen	3 Begriffe und Definitionen
4 Überblick	4 Validierungsprozesse
5 Spezifikation der Sicherheitsfunktionen (SRS, ...)	5 Validierung durch Analyse
6 Design Betrachtungen (PL, Kategorien, PFH_D, ...)	6 Validierung durch Testen
7 Software Sicherheitsanforderungen	7 Validierung der Spezifikation der Sicherheitsanforderungen für die Sicherheitsfunktion
8 Verifizierung, dass der erreichte PL dem geforderten PL_r entspricht	8 Validierung der Sicherheitsfunktionen
9 Ergonomische Aspekte des Designs	9 Validierung von Leistungsniveau und Kategorien
10 Validierungsprozesse	10 Validierung von Umweltanforderungen
11 Instandhaltung	11 Validierung von Instandhaltungsanforderungen
12 Technische Dokumentation	12 Validierung von technischer Dokumentation und Gebrauchsinformationen
13 Information zur Verwendung	Annex A bis E
Annex A bis N	Annex ZA

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

Tabelle 02: Bestimmung von Parameter P über fünf Kriterien

Faktor	C	B	A
1. Verwendung der Maschine		Ungeschulte Person	Geschulte Person
2. Geschwindigkeit des Teils, das ein gefährliches Ereignis verursachen kann	Hohes Tempo < 1 s	Mittleres Tempo < 3 s	Geringes Tempo ≥ 3 s
3. Räumliche Möglichkeit, sich der Gefahr zu entziehen	Nicht möglich	Weniger als 50% der Fälle	Möglich in mehr oder gleich 50 % der Fälle
4. Möglichkeit des Erkennens	Nicht möglich	Nur in weniger als 50% der Fälle möglich	Möglich in mehr oder gleich 50 % der Fälle
5. Komplexität der Arbeitsaufgabe		Hoch Komplexe Fehlersuche	Keine Interaktion

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

Tabelle 03: Gesamtbewertung des Parameters „P“

Gesamtbewertung	Parameter „P“
Ein oder mehrmals Rot	P2
Kein Rot, drei oder mehrmals Orange	P2
Kein Rot, zweimal Orange, der Rest Grün	P1 oder P2 Abhängig von der Maschine
Kein Rot, ein oder kein Orange, der Rest Grün	P1

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, dass 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
LVL	Begrenzte Variabilität Sprache	Programmiersprache mit eingeschränktem Sprachumfang
FVL	Vollständige Variablensprache	Programmiersprache mit uneingeschränktem Sprachumfang
SRESW	Sicherheitsrelevante eingebettete Software	Software, die als Teil des Systems durch den Steuerungshersteller geliefert wird und die durch den Anwender der Maschine nicht verändert werden kann
SRASW	Sicherheitsrelevante Anwendungssoftware	Software, die speziell für die Anwendung vom Hersteller in die Maschine implementiert wird
P1	Parameter P1 – Möglichkeit unter speziellen Konditionen	Möglichkeit der Gefahrenvermeidung oder Schadensbegrenzung
P2	Parameter P2 – Kaum möglich	Sehr geringe Möglichkeit der Gefahrenvermeidung oder Schadensbegrenzung

2.6 ANHANG M MIT ZUSÄTZLICHEN INFORMATIONEN ZUR RISIKOREDUZIERUNG FÜR DAS SRS-SYSTEM (SAFETY REQUIREMENTS SPECIFICATIONS)

Typische Sicherheitsfunktionen, ihre Eigenschaften und sicherheitsrelevante Parameter werden mit Anhang M der ISO/DIS 13849-1:2020 [4] in mehreren Tabellen erstmalig gelistet, wobei auch auf andere internationale Normen verwiesen wird, deren Anforderungen sich auf Sicherheitsfunktionen, Sicherheitseigenschaften oder Sicherheitsparameter beziehen.

2.7 ANHANG N ZUR VERMEIDUNG VON SYSTEMATISCHEN FEHLERN IM SOFTWARE-DESIGN

Zur Vermeidung von systematischen Fehlern im Software Design werden mit Anhang N der ISO/DIS 13849-1:2020 [4] ab sofort Vorschläge zur Auswahl von Maßnahmen zur Fehlervermeidung für sicherheitsrelevante eingebettete Software (SRESW) oder sicherheitsrelevante Anwendungssoftware (SRASW) in Tabellen aufgeführt. Tabelle 01 zeigt eine Auswahl der Maßnahmen, welche für SRASW in “Limited Variability Language” (LVL) zu verwenden sind, und Tabelle 02 listet eine Auswahl von Maßnahmen die für SRESW & SRASW in „Full Variability Language“ (FVL) anzuwenden sind.

FAZIT:

Die Wahrscheinlichkeit eines gefahrbringenden Ausfalls der Sicherheitsfunktionen hängt von mehreren Faktoren ab, unter anderem von der Hard- und Softwarestruktur, dem Umfang der Fehlererkennungsmechanismen [Diagnosedeckungsgrad (DC)], der Zuverlässigkeit der Komponenten [mittlere Zeit bis zum gefahrbringenden Ausfall ($MTTF_D$), Ausfall durch gemeinsame Ursache (CCF)], dem Konstruktionsprozess, der Betriebsbelastung, den Umgebungsbedingungen und den Betriebsverfahren.

Die international vereinheitlichen Anforderungen gemäß dem Neuentwurf der ISO/DIS ISO/DIS 13849-1:2020 [4] zeigen Richtlinien und Detaillierungen auf, die den Hersteller, zum Beispiel von mobilen Arbeitsmaschinen, dabei unterstützen, die Maschinenrichtlinien 2006/42/EG und die EMV-Richtlinien 2014/30/EU zielführender anzuwenden, zu erfüllen, und umzusetzen.

Bilder: *Aufmacher: Tierney – stock.adobe.com*

www.xcmg-erc.com

Literaturhinweis:

[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 61000-6-2:2016-08 Elektromagnetische Verträglichkeit (EMV) - Teil 6-2: Fachgrundnormen - Störfestigkeitsnorm für Industriebereiche

[7] IEC 61000-6-7:201-12 5 Elektromagnetische Verträglichkeit (EMV) - Teil 6-7: Fachgrundnormen - Störfestigkeitsanforderungen an Geräte und Einrichtungen, die zur Durchführung von Funktionen in sicherheitsbezogenen Systemen (funktionale Sicherheit) an industriellen Standorten vorgesehen sind

[8] Revision der ISO 13849-1 Fachveranstaltung Maschinen Dr. Michael Huelke, Michael Hauke, Bamberg, 11. Juli 2019