Fachbeitrag zum Thema:

DIN EN ISO 13849-1 :2015
Wesentliche Veränderungen gegenüber der Norm: DIN EN 13849-1: 2006

Information und Überblick zur DIN EN ISO 13849-1 über die wesentlichen Merkmale und Änderungen gegenüber der abgelösten Norm vom Jahre 2006.

Autor:
Torsten Skrzypczak
ce-conform

1.0 Allgemeine Information:

Mit Datum 30.06.2016 wurde im Amtsblatt der EU C332-1 vom 09.09.2016 die DIN EN 13849-1 :2006 ohne Übergangsfrist abgelöst.
Für diese Norm tritt mit Datum vom 13.05.2016 die DIN EN ISO 13849-1: 2015 in Kraft.

Mit diesem Dokument werden hier die wesentlichen Änderungen zur Vorgängernorm herausgestellt und aufgezeigt.

2.0 grundlegende Änderungen :

Eine der wohl wesentlichsten Änderungen der neuen DIN EN ISO 13849-1 ist wohl, dass jetzt nicht nur der Hersteller in die Pflicht genommen wird diese Norm zu erfüllen, sondern auch der **Betreiber**. Damit endet nicht mehr automatisch nach Abnahme der Anlagen und dem ersten Nachweisdokument zur Erfüllung der Norm (z.B. Sistema oder PasCal) der eigentliche Prozess der DIN-EN ISO 13849-1. Vielmehr wird der Betreiber mit in die Pflicht genommen durch regelmäßige Prüfungen die ordentliche Funktion der einzelnen SRP/CS * festzustellen.

Die bisherige Tabelle 1 der Norm (empfohlene Anwendung der Normen IEC 62061 und ISO 13849-1 ist durch den Report DIN ISO/TR 23849 ersetzt worden.
Der genannte Bericht stellt die Unterschiede sowie die Gemeinsamkeiten beider Normen dar.

3.0 organisatorische Änderungen:

Mit dem Erscheinen der neuen Norm wurden auch einige Begriffe, welche bisher keine einheitliche Schreibweise hatten, angepasst und in der Norm veröffentlicht:
Dabei handelt es sich um die Begriffe:

- PFH_D: Probability of a dangerous failure per hour . Dieser Wert wurde neu eingeführt, und steht für die durchschnittliche Wahrscheinlichkeit eines gefährlichen Ausfalls je Stunde. Dieser Wert ist mit 1/Zeit oder gebräuchlich 1/h anzugeben.
- $MTTF_D$: Mean time to dangerous failure. Hier wurde lediglich der Index geändert.. Statt der früheren Schreibweise $MTTFD_d$ **** jst jetzt der Index immer mit einem Großbuchstaben zu schreiben.
- Das gilt dann auch für Schreibweise der Werte B_{10D} ** und T_{10D}***

---

* SRP/CS: Saft related parts of a control System (sicherheitsrelevante Teile eines Steuerungssystems)

** B10D: Anzahl von Zyklen, bis 10 % der Komponenten gefährlich ausgefallen sind (für pneumatische und elektromechanische Komponenten)

*** T10D: Gebrauchsdauer

**** MTTFd: mittlere Zeit bis zum gefahrbringenden Ausfall

3.0 Änderungen im Anhang „K“

- Verweise auf die Norm 12100-1 :2003 wurden abgeändert und es wird stattdessen jetzt auf die DIN-EN 12100 :2010 verwiesen.
- Subsysteme eines SRP/CS können jetzt auch nach anderen Normen entworfen werden. (z.B. IEC 61508, IEC 61496, IEC 62061) Diese Systeme können dann nach Umrechnung SILs *zu PL als Subsystem integriert werden. In der Tabelle 4 der neuen Norm wird die Umrechnung aufgezeigt.
- Es sind für diese Vorgehensweise bestimmte Regeln anzuwenden. Diese werden in der neuen Norm unter dem Abschnitt 6.3 erläutert.
- Man findet dazu auch in der DIN ISO/TR 23849[1] ausreichende Information und Anwendungsbeispiele.

4.0 weitere Änderungen:

Der $MTTF_D$ für jeden Kanal wird nicht mehr ausschließlich auf 100 Jahre begrenzt. Geändert wurde dieser Wert bei Subsystemen der Kategorie 4. Hier beträgt der obere Grenzwert jetzt 2500 Jahre.
Da man durch die Redundanz und dem DC in der Kategorie 4 bereits ein hohes Niveau erreicht, hat man entschieden, dass speziell in der Kategorie 4 den $MTTF_D$ Wert angehoben werden kann.
Ein weiterer Vorteil ist: dass jetzt höhere PFH_D Werte erreicht werden, und es wird verhindert, dass man bei Kombination von mehreren PL-e Subsystemen nicht unbedingt in den Level “d“ abgestuft wird.

Sicherheitsfunktionen:
Hier wurde Folgendes ergänzt:

> Es ist hilfreich. Je nach Anwendung, eine separate Sicherheitsfunktion für den Ausfall der Energie zu definieren. Das wäre z.B. zutreffend für Auf -und Abwärtsbewegungen von Achsen, bei denen ein Absinken bei Energieverlust allein durch dessen Schwerkraft, verhindert werden muss.

*SIL Safty integrity Level

4.0 weitere Änderungen:

Änderungen bei den Kategorien:
Kategorie 2 und Erkennung eines Fehlers:
In der Kategorie 2 war es bisher möglich, sofern nach Erkennen eines Fehlers das Herstellen eines sicheren Zustandes nicht möglich ist, lediglich eine Warnung bereit zu stellen.

Ab **sofort** wird festgelegt wann eine Warnung noch in Frage kommt:
Beim PLr- a bis c kann eine Warnung als ausreichend angesehen werden, sofern keine Möglichkeit besteht, einen sicheren Zustand nach Fehlereintritt herzustellen. (z.B. Verkleben von Kontakten)
Ab PLr-d * muss der OTE Ausgang einen sicheren Zustand einleiten bis der Fehler behoben ist. Eine Warnung ist hier nicht mehr ausreichend.

Kombination von SRP/CS
Bei Kombination von SRP/CS (z.B. Reihenschaltung) welche zusammen eine Sicherheitsfunktion ergeben, kann man nun wie folgt vorgehen.
Das kann einmal geschehen durch „nicht qualifizierte“ oder eben „qualifizierte“ Aspekte.

- Begrenzung durch nicht qualifizierte Aspekte: Ergebnis: Der Gesamt PL ist höchstens so groß wie der niedrigste PL aller kombinierten SRP/CS
  oder
- Begrenzung durch qualifizierte Aspekte: Ergebnis: Der Gesamt-PL ist höchstens so groß wie der PL-Wert der sich nach Tabelle 3 der Norm, aus dem Summen-PFH_{D}** ergibt.

Weitere Änderungen in der Kategorie 2
Testhäufigkeit bei Kategorie 2
Für die Anforderungsrate galt bisher in der Kategorie 2 ausschließlich ≤ 1/100 der Testrate. Jetzt darf die Testung auch unmittelbar bei Anforderung einer Sicherheitsfunktion erfolgen. Bedingung dafür ist aber, dass die Gesamtzeit von Erkennen des Ausfalle bis Erreichen des sicheren Zustandes geringer ist, als die Zeit des Erreichen der Gefährdung.
In der DIN-EN ISO 13849-1 :2016 wird dabei explizit auf die DIN EN ISO 13855 verwiesen.

* PLr-d: erforderlicher Peformancelevel
** PFHd: durchschnittliche Wahrscheinlichkeit eines Ausfalls

4.0 weiter Änderungen:

Weitere Änderungen in der Kategorie 2
$MTTF_D$ des Testkanals in Kategorie 2
Für die Kategorie 2 ist die $MTTF_D$ des gesamten Testkanals größer als die Hälfte der $MTTF_D$ des gesamten Funktionskanals. Diese Regel war bisher nur bei nicht aufzuteilenden Blöcken abwendbar.

Im Anhang „K" der Norm wird auf das Verhältnis von Anforderungsrate zu Testrate ebenfalls erläutern eingegangen.

> *Wenn in der Kategorie 2 die obige Bedingung an die Testrate (100x mehr Testen als Anfordern) nicht eingehalten werden kann, aber die Anforderungsrate ≤ 1/25 der Testrate ist, dann können die PFH_D Werte für Kategorie 2 aus Anhang „K" mit dem Faktor 1,1 multipliziert werden uns als Abschätzung zur sicheren Seite herangezogen werden.*
>
> *Dabei wird auch noch verwiesen dass die PFH_D Werte im Anhang K, und hier für alle Kategorien, mit den diskreten DC_{avg}- Werten von 60%, 90% und 99% berechnet wurden.*

Vereinfachtes Verfahren für den Ausgangsteil des SRP/CS (Bestimmung von PL und PFH_d ohne $MTTF_D$. (Energieübertragungselemente)
In die Norm wurde der Abschnitt 4.5.5 neu mit aufgenommen. Hier wird ein Vereinfachtes Verfahren zur Bestimmung von PFH_D und der qualifizierten Aspekte des PL für das Ausgangs-Subsystem aufgezeigt.
Dabei stützt sich dieses System hauptsächlich auf die Bestimmung der Werte mittels Kategorie, des DC_{avg} *und dem CCF. ** Dabei entfällt die Berechnung des $MTTF_D$ Wertes. Voraussetzung, dass dieses Verfahren angewendet werden darf ist, dass ausschließlich bewährte Bauteile in den Kategorien 1,2,3 oder **betriebsbewährte** Bauteile in den Kategorien 2,3 und 4 Anwendung finden.

Der Begriff **betriebsbewährt** ist ebenfalls eine neue Eigenschaft im Rahmen der Norm und sollte nicht mit dem Begriff „bewährte Bauteile" verwechselt werden.
Der Wert **„betriebsbewährt"** wird ermittelt mittels einer Art Analyse der betrieblichen Ergebnisse für eine spezielle Konfiguration des Bauteils in einer bestimmte Applikation ermittelt.

---

* Degree of Diagnosis (Diagnosedeckungsgrad)
** CCF common cause failures (Fehler gemeinsamer Ursache)

4.0 weiter Änderungen:

Vereinfachtes Verfahren für den Ausgangsteil des SRP/CS (Bestimmung von PL und PFH_d ohne $MTTF_D$. (Energieübertragungselemente)

Da dieses Verfahren speziell für den Maschinenbau eher ungeeignet oder nicht üblich ist, hat man dessen Anwendung spezifiziert.
Demnach ist die Anwendung nur in bestimmten Fällen erlaubt:

1. für den Ausgabeteil des SRP/CS
und
2. wenn für mechanische, pneumatische oder hydraulische Bauteile (aber auch Bauteile mit gemischter Technologie) keine anwendungsspezifischen und zuverlässigen Daten wie $MTTF_D$ Ausfallrate oder B_{10D} vorhanden sind.

In Anlehnung der Tabelle des neuen Abschnitts 4.5.5 der Norm hier die Tabelle der Norm (in Anlehnung) als Abschätzung.

PL-Wert	PFHD in 1/h		Kat B	Kat 1	Kat 2	Kat 3	Kat 4
PL-b	$5{,}0 \cdot 10^{-6}$		●	○	○	○	○
PL-c	$1{,}7 \cdot 10^{-6}$		▬	●	●	○	○
PL-d	$2{,}9 \cdot 10^{-7}$		▬	▬	▬	●	○
PL-e	$2{,}9 \cdot 10^{-8}$		▬	▬	▬	▬	●

● angewandte Kategorie (wird empfohlen)
○ angewandte Kategorie (optional)
▬ **Kategorie nicht anwendbar**

4.0 weiter Änderungen:

Vereinfachtes Verfahren für den Ausgangsteil des SRP/CS (Bestimmung von PL und PFH_d ohne $MTTF_D$. (Energieübertragungselemente)

Natürlich ist die Anwendung der Verfahrensweise auf der Seite zuvor, an bestimmte Zusatzbedingungen geknüpft:

Kategorie 1:
Verwendung bewährter Bauteile und bewährter Sicherheitsprinzipien (wie bisher, und in der Kategorie -1-Definition verankert)

Kategorie 2:
$MTTF_d$ des Testkanals beträgt mind. 10 Jahre

Kategorie 2,3 und 4:
Verwendung bewährter oder betriebsbewährter Bauteile, Verwendung bewährter Sicherheitsprinzipien. Bei Kategorie 2 gilt dies auch für den Testkanal.

Kategorie 2 und 3:
ausreichende Maßnahmen gegen CCF und für jedes Bauteil ein DC mind. niedrig

Kategorie 4:
ausreichende Maßnahmen gegen CCF und für jedes Bauteil ein DC von hoch.

Weitere Ergänzungen:
Kategorie 1:
Der Maschinenhersteller soll für die sicherheitsbezogenen Bauteile die T_{10D} Werte auf Basis der Daten der Betriebsbewährung bestimmen. Das aber nur sofern sich der Ausfall nicht im technischen Prozess bemerkbar macht.

Kategorie 2,3 und 4
Die DC_{avg} Wert Berechnung soll hier über einen arithmetischen Mittelwert gebildet werden. Dieser Wert ist aus den Werten der einzelnen DC´s aller Komponenten zu bilden. Das ergibt sich weil man mittels der fehlenden $MTTF_D$ Werte die Berechnung des DC-Wertes mittels der Formel E1 nicht durchführen kann.

5.0 Änderungen in den Anhängen der Norm:

Anhang F: CCF (Fehler gemeinsamer Ursache)
Hier wurde in der Tabelle F1 die Schreibweise und daraus resultierend die Lesbarkeit verbessert. Es wurden Informationen angehängt.

Anhang E: DC (Diagnosedeckungsgrad)
In der Tabelle E1 wurden auf Grund von mangelndem Einsatz in der Praxis zwei Maßnahmen gelöscht:

- Redundanter Abschaltpfad ohne Überwachung des Antriebselements (DC = 0%)
- Redundanter Abschaltpfad mit Überwachung eines der Antriebselemente entweder durch Logik oder Testeinrichtung

Vielmehr wird die DC-Maßnahme „Fehlererkennung durch den Prozess“ ausführlicher erläutert.

- Um den DC von 0-99% abschätzen zu können, sollten alle relevanten gefahrbringenden Ausfälle zunächst identifiziert werden und es ist einzuschätzen welche dieser Ausfälle im Prozess erkannt werden. Aus dem erkannten Anteil kann dann einer der Werte :0% keine DC, 60% niedriger DC, 90% mittlerer DC, oder 99% hoher DC, abgeschätzt werden.
- diese Maßnahme darf nur genutzt werden, wenn gefahrbringende Ausfälle sich auch wirklich im Prozess offenbaren. Werden dagegen Bauteile nur durch die Anforderung der Sicherheitsfunktion betätigt, dann kann die Fehlererkennung durch den Prozess nicht beansprucht werden.:

Anhang A: Berechnung des Performancelevels
Im Anhang A gibt es mehrere Änderungen.

Für viele Wohl endlich mal mit Werten versehen die Einstufungen F1 und F2 bei der Arbeit mit dem Risikographen

F2 liegt vor, wenn die Häufigkeit höher als einmal alle 15min ist.
F1 darf gewählt werden, wenn die gesamte Expositionsdauer 1/20 der gesamten Betriebsdauer nicht überschreitet, und die Häufigkeit nicht höher als einmal alle 15min. Ist.

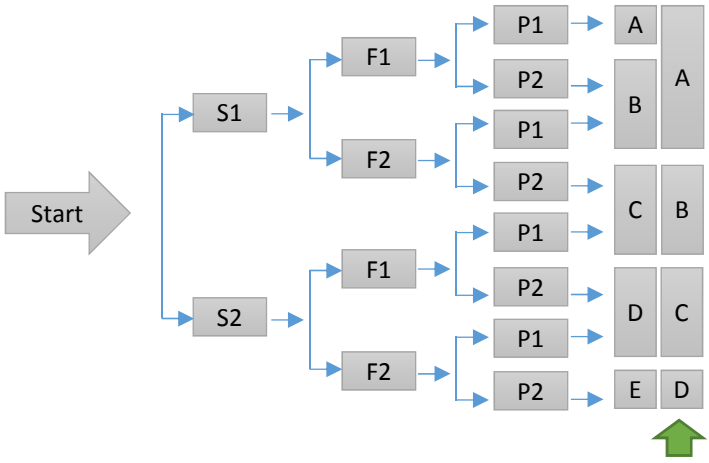
5.0 Änderungen in den Anhängen der Norm:

Anhang A: Berechnung des Performancelevels

Es wird auch drauf verwiesen das die in Typ-C Normen genannten PLr-Festlegungen durchaus von den eigens ermittelten PLr-Wert abweichen darf.
Außerdem wird auf den informativen Charakter des im Anhang A dargestellten Verfahrens verwiesen. Man spricht nicht mehr von verbindlich, sondern von einer Einschätzung des PLr-Wertes.

Aber die wohl größte auffallende Änderung des Anhang A und die der Norm DIN EN ISO 13849-1:2016 ist das nun der Risikograph zur Ermittlung des PLr-Wertes eine weitere Einschätzungsvariante mit hinzubekommen hat.
In Anlehnung des Risikographen der DIN EN ISO 12100 kann jetzt auch noch die Eintrittswahrscheinlichkeit mit zur Bewertung herangezogen werden.
Allerdings nicht so wie das die Gefahrenanalysegraphen der DIN EN ISO 12100 erlauben sondern in abgeschwächter Form.
Es werden hier nicht betrachtet die möglichen Wahrscheinlichkeiten in klein, mittel, groß, wie man es von der 12100 kennt, sondern es ändert sich lediglich der Performancelevel wenn man von einer niedrigen Wahrscheinlichkeit des Eintreffens ausgehen kann.
Unterscheidungen wie bei der 12100 hat man hier nicht vorgesehen.

Der Risikograph gestaltet sich nun wie folgt:



Unter Voraussetzung, dass man davon Ausgehen kann, dass die Eintrittswahrscheinlichkeit einer Gefährdung „niedrig“ ist

Anhang C und D: $MTTF_D$ –Werte
Hier gab es im wesentlichen 3 Veränderungen:

In der Tabelle C1 haben sich folgende Änderung als notwendig erwiesen:

1. Für hydraulische Bauteile (vor allem Ventile) können nun –abhängig von der mittleren Anzahl jährlicher Betätigungen n_{op} – auch der höhere typische $MTTF_D$ Wert angesetzt werden. Der bisherige Wert von 150 Jahren kann bei n_{op} kleiner als 1.000.000 Zyklen/Jahr auf 300 Jahre verdoppelt werden. Bei noch kleinere Betätigungswerte (weniger 500.000 oder weniger als 250.000 Zyklen/Jahr führt dies zu weiteren Verdopplungen auf 600 bzw. 1200 Jahre. Damit wurde die hydraulischen Bauteile den ähnlichen pneumatischen Bauteilen angenähert.

2. Der typische B_{10D} Wert für Schütze mit nominaler Last wurde von 2.000.000 Zyklen auf 1.300.000 Zyklen reduziert. Das ergab sich aus der Produktnorm für Schütze (DIN EN 60947-4-1)die einen Anteil gefährlicher Ausfälle von 74% vorgibt.

3. Die beiden Zeilen für Not-Halt Geräte wurden zusammengefasst. Die Nothaltgeräte und Zustimmungsschalter können je nach Anzahl der elektrischen Ausgangskontakte und der Fehlererkennung im nachgeordneten SRP/CS als Teilsysteme der Kategorie 1 oder den Kategorien 3 oder 4 abgeschätzt werden. Jedes Kontaktelement (einschließlich der Mechanik) kann als ein Kanal mit entsprechenden B_{10D} Wert von 100.000 Zyklen betrachtet werden. Bei den Zustimmungsschaltern trifft das auf die Öffnungsfunktionen zu.

4. In den Tabellen C.2 und C.7 für Halbleiter und passive Bauelemente wurde die Spalte $MTTF_D$ für Bauteile „ungünstigster Fall“ gelöscht. Mittlerweile gibt es von den Herstellern bessere Werte als die dort in der Spalte vorgegeben sind, so das eine weitere Anwendung nicht mehr als relevant angesehen wurde.

6.0 Was noch verbessert wurde:

Die Norm greift auch im neuen Abschnitt A.3 das Thema „überlagerte Gefährdungen“ auf. Hier wird nun eindeutig klar gestellt, dass während der Risikobewertung jede Gefährdung getrennt bewertet werden kann.

Das heißt, dass die Sicherheitsfunktionen für getrennte Gefährdungen separiert werden dürfen, sodass als Ausgang des zugehörigen SRP/CS jeweils nur die Leistungssteuerungselemente für eine Gefährdung auftauchen (und in die PFH_D eingehen).

So können jetzt z.B. bei einer Fertigungszelle mit mehreren Roboter die sicherheitsbezogenen Stoppfunktionen als Reaktion des Öffnen einer Schutztür, als separate Sicherheitsfunktion für jeden Roboter einzeln definiert werden.

7.0 Quellenverzeichnis:

- Ableitung IFA Institut zur Änderung der DIN EN ISO 13849-1 :2016
- DIN EN ISO 13849-1 :2015 und DIN-EN ISO 13849-1 :2006
- DIN EN ISO 13849-2 :2006
- DIN EN ISO 12100 : 2010
- IFA BGA-Report
- mündliche Informationen der Referenten von der BGHM