BGHM
Berufsgenossenschaft
Holz und Metall

Ihre gesetzliche Unfallversicherung

Funktionale Sicherheit

ISO 13849-1

IEC 62061

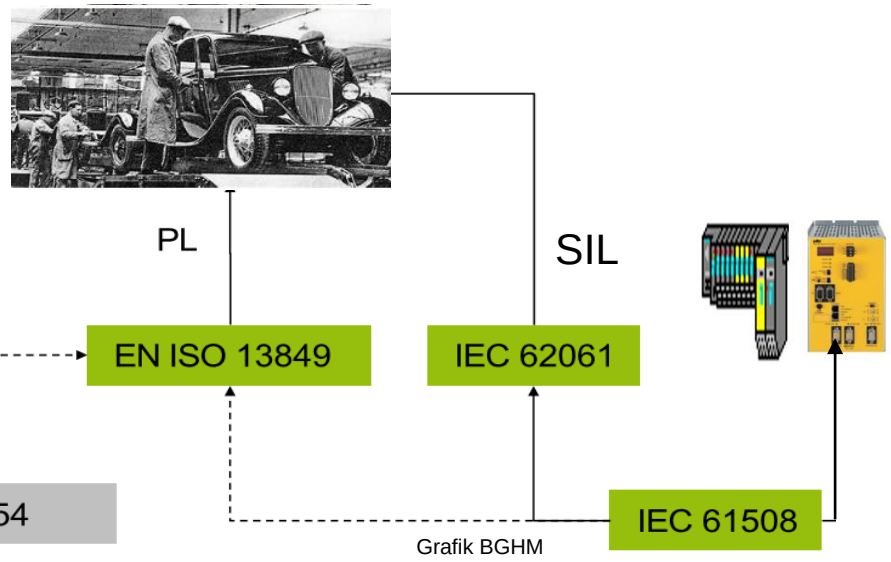
ISO 14119

Stand 9/2023

Fachveranstaltung Maschinensicherheit

Hr. T. Schulz-Basten, 19.09.2023

Normungssituation (FuSi)



Grafik BGHM

EN ISO 13849-1 und **2**, Sicherheit von Maschinen Sicherheitsbezogene Teile von Steuerungen

IEC 62061 Sicherheit von Maschinen Funktionale Sicherheit sicherheitsbezogener Steuerungssysteme

IEC 61508 Reihe "Funktionale Sicherheit elektrischer / elektronischer / programmierbarer elektronischer Systeme"

- **EN 50128:** Bahnanwendungen – Telekommunikationstechnik, Signaltechnik und Datenverarbeitungssysteme – Sicherheitsrelevante elektronische Systeme für Signaltechnik
- **IEC 61513:** Kernkraftwerke – Leittechnik für Systeme mit sicherheitstechnischer Bedeutung – Allgemeine Systemanforderungen
- **ISO 26262**: Road vehicles – Functional safety
- **ISO 25119:** Tractors and machinery for agriculture and forestry – Safety-related parts of control systems – Functional Safety[1]
- **DIN EN 13814-1 bis 3:**Sicherheit von Fahrgeschäften und Vergnügungsanlagen
- **DIN EN 61511** Funktionale Sicherheit - PLT-Sicherheitseinrichtungen für die Prozessindustrie - Teil 1: Allgemeines, Begriffe, Anforderungen an Systeme, Hardware und Anwendungsprogrammierung
- usw.

Inhalt

Änderungen der ISO 13849-1 / IEC 62061 und ISO 14119 (Pkt.13.)

1. **Allgemein**
2. Software
3. EMV / EMC
4. Architekturanforderungen
5. Akzeptanz von Teilsystemen
6. Security-Aspekte
7. Validierung
8. Management der funktionalen Sicherheit
9. Unabhängigkeit von Aktivitäten
10. Risikoeinschätzung
11. Gerätetypen
12. Sonstiges
13. ISO 14119

1. Allgemein

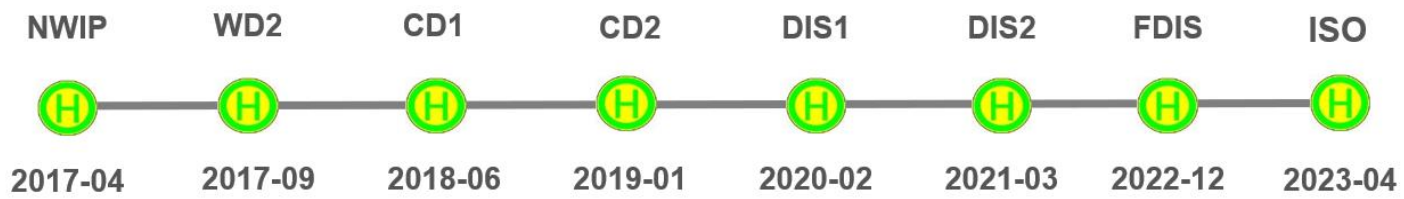
ISO 13849-1

- verbesserte Struktur
- Anforderungen an elektromagnetische Störfestigkeit
- Validierung (ISO 13849-2)
- Management der Funktionalen Sicherheit
- Softwareanforderungen
- Spezifikation der Sicherheitsfunktion
- Gerätetypen

IEC 62061

- Erweiterung auf Nicht-Elektrik
- Low Demand wurde nicht aufgenommen
- Anwendungssoftware (HW & SW Plattform)
- kein Design komplexer Teilsysteme
- Management der Funktionalen Sicherheit

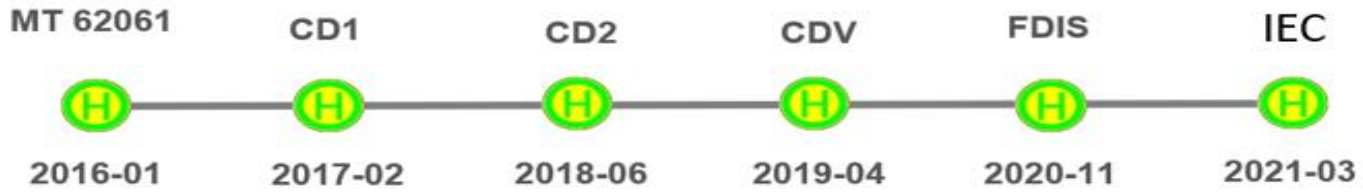
ISO 13849-1 Maintenance für Edition 4



Quelle: BGHM

Die Übergangsfrist beträgt nach aktueller Planung drei Jahre.
Deutsche Übersetzung zeitnah.

IEC 62061 Maintenance für Edition 2



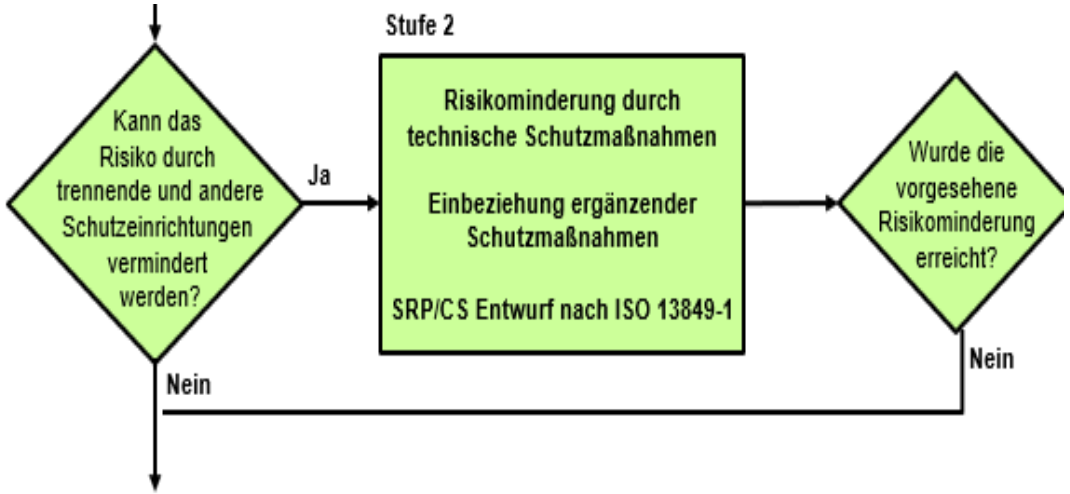
Quelle: BGHM

Harmonisierte Norm
Deutsche Ausgabe Februar 2023

Integration in die 3-Stufenmethode der ISO 12100

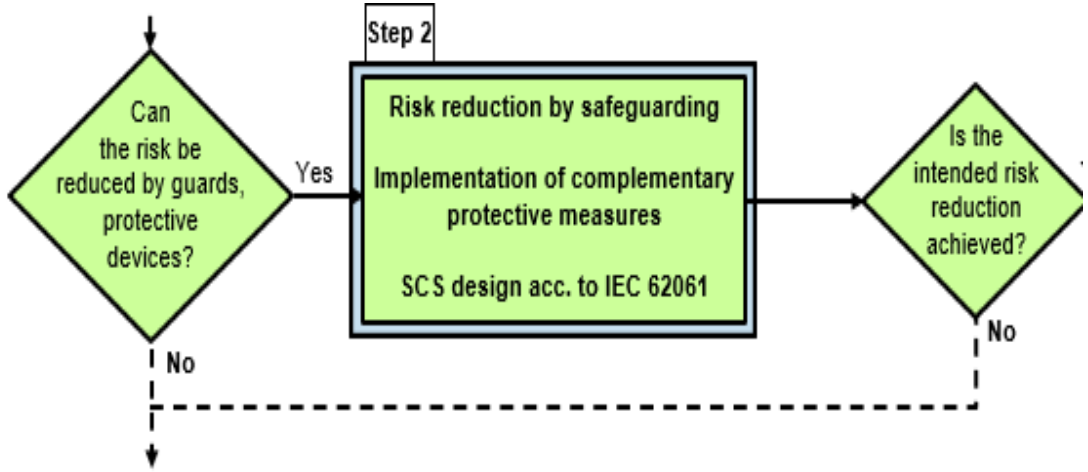
Umsetzung der Stufe 2 durch funktional sichere Steuerungen (SRP/CS)

ISO 13849-1



Quelle: In Anlehnung an ISO 13849-1, FDIS-ballot Dokument (2022

IEC 62061



Quelle: In Anlehnung an IEC 62061:2021,

Spezifikation der Sicherheitsfunktion wird in ISO 13849 (Abs. 5) und IEC 62061 detallierter beschrieben!

Name der SF	Eindeutige Identifizierung
Auslösendes Ereignis	Durch welches Ereignis wird die Sicherheitsfunktion ausgelöst?
Sicherheitsgerichtete Reaktion	Was ist die Sicherheitsgerichtete Reaktion?
Betriebsart	In welcher Betriebsart soll die Sicherheitsfunktion aktiv sein?
PLr / SIL	Mit welchem Performance Level soll die Sicherheitsfunktion ausgeführt werden?
Häufigkeit der Anforderung	Wie häufig ist mit der Anforderung der Sicherheitsfunktion zu rechnen?
Nachlauf	In welcher Zeit nach Anforderung der Sicherheitsfunktion soll der sichere Zustand erreicht werden?
Verhalten bei Energieausfall	Welche Sicherheitsgerichtete Reaktion ist bei Energieausfall erforderlich?
Priorität	Ist die Sicherheitsfunktion vor- oder nachrangig gegenüber anderen Sicherheitsfunktionen?
Ergänzende SF	Setzt der Einsatz der Sicherheitsfunktion weitere aktive Sicherheitsfunktionen voraus?
Zusätzliche Parameter	Welche zusätzlichen Parameter müssen berücksichtigt werden?
Fehlererkennende Maßnahmen	Welche Diagnosemaßnahmen müssen berücksichtigt werden?
Fehlerreaktionsmaßnahmen	Welche Maßnahmen sind bei Fehlererkennung erforderlich?

Quelle: DGUV – Webcode: D109240

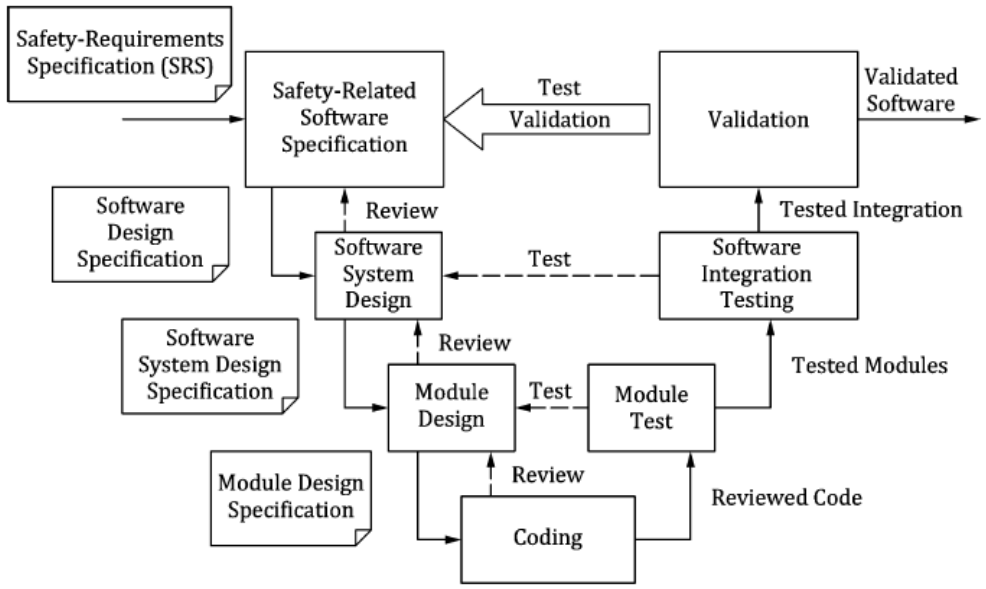
Inhalt

Änderungen der ISO 13849-1 / IEC und ISO 14119

1. Allgemein
2. **Software**
3. EMV / EMC
4. Architekturanforderungen
5. Akzeptanz von Teilsystemen
6. Security-Aspekte
7. Validierung
8. Management der funktionalen Sicherheit
9. Unabhängigkeit von Aktivitäten
10. Risikoeinschätzung
11. Gerätetypen
12. Sonstiges
13. ISO 14119

ISO 13849-1 (Software)

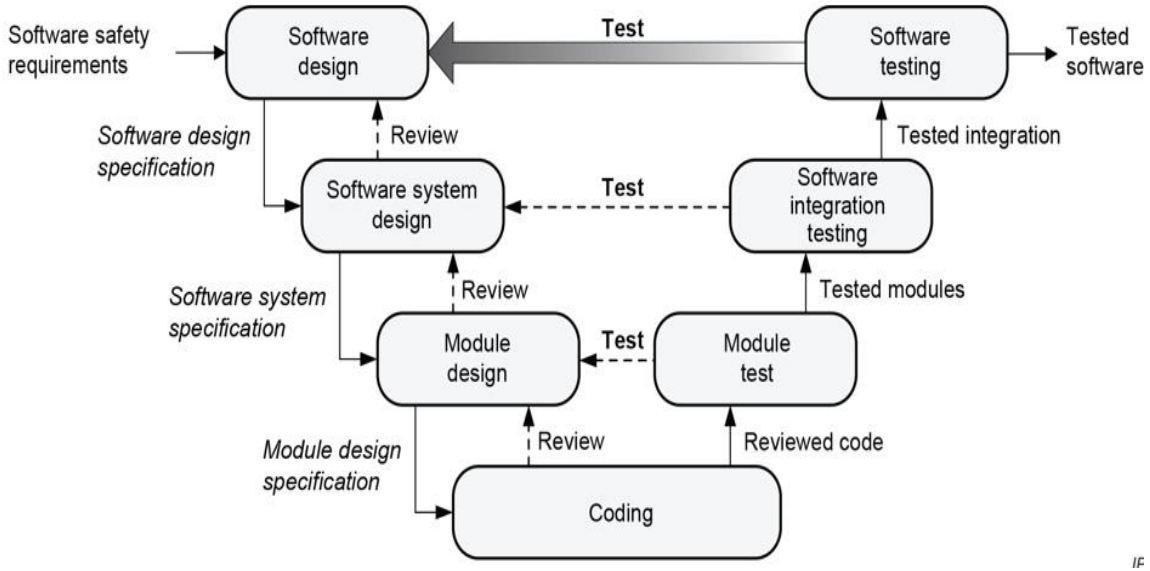
Vereinfachtes V-Modell nach ISO 13849-1



Quelle ISO 13849-1

IEC 62061 (Software)

Vereinfachtes V-Modell nach IEC 62061

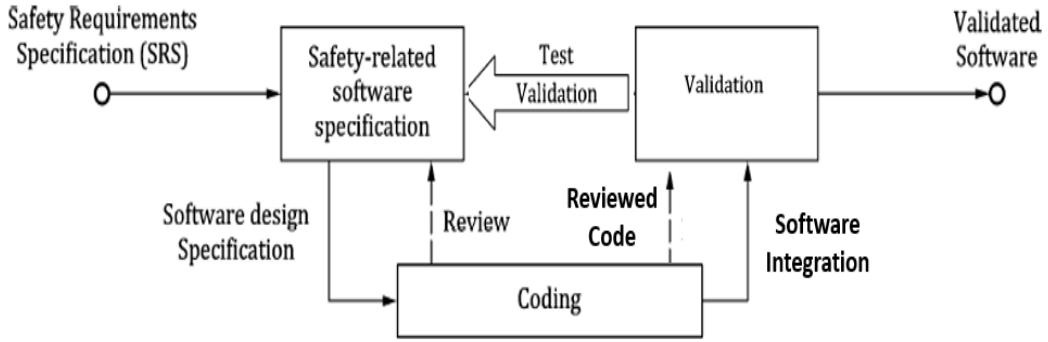


Quelle IEC 62061

Es gibt keine spezielle Forderung für einzelne Dokumente.

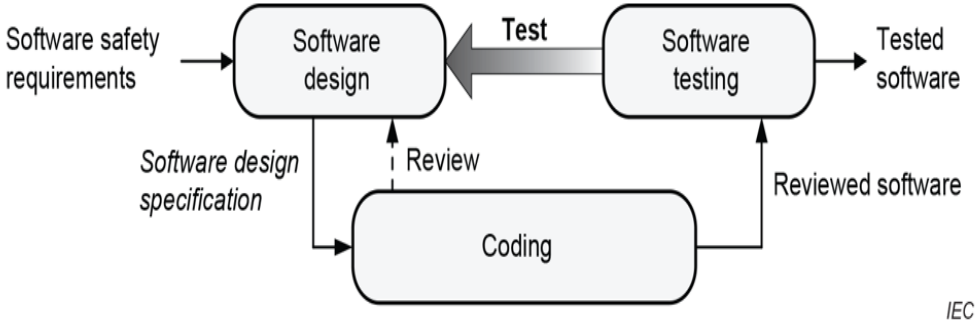
Vereinfachtes V-Modell für Software, falls zuvor beurteilte sicherheitsbezogene Hardware- und Softwaremodule in Kombination mit LVL (limited variability language) verwendet werden.

ISO 13849-1



Quelle ISO 13849-1

IEC 62061



Quelle IEC 62061

ISO 13849-1 (Software)

Anforderungen ⇨ Kapitel 7

Umsetzung ⇨ Anhang N1 und N2

Anhang N1 **„Maßnahmen zur Fehlervermeidung für den Entwurf von sicherheitsbezogener Software“**

- **Tabelle 1** Gruppierung von Fällen für die Auswahl von Maßnahmen.
- **Tabelle 2** Auswahl von Maßnahmen für SRASW (sicherheitsgerichtete Anwendersoftware) in LVL
- **Tabelle 3** Auswahl von Maßnahmen für SRESW (Embedded Software) & SRASW in FVL (full variability language) verwendet werden.

Tabelle N.1 — Gruppierung von Fällen für die Auswahl von Maßnahmen

PL_r	Kategorie	Software verwendet in	Fall
a und b	B	Funktionskanal	Fall 1
a, b und c	2	Testkanal	
a und b	2	Funktionskanal	
a und b	3	bereits bewertete Plattform	
a und b	3	Kanal 1 UND 2	
a, b und c	3	Kanal 1 ODER 2	
c	2	Funktionskanal	Fall 2
c	3	bereits bewertete Plattform	
c	3	Kanal 1 UND 2	
d	2	Testkanal	
d	3 und 4	Kanal 1 ODER 2	
d	2	Funktionskanal	Fall 3
d	3 und 4	bereits bewertete Plattform	
d	3 und 4	Kanal 1 UND 2	
e	3 und 4	Kanal 1 ODER 2	
e	3 und 4	bereits bewertete Plattform	Fall 4[a]
e	3 und 4	Kanal 1 UND 2	

[a] Der einzige Unterschied in den beiden Zeilen von Fall 4 besteht in den Anforderungen an die Werkzeugauswahl.

Legende

— Kanal 1 UND 2: SRESW oder SRASW wird in beiden Funktionskanälen der Kategorie 3 oder 4 verwendet;

— Kanal 1 ODER 2: SRESW oder SRASW wird nur in einem der beiden Funktionskanäle der Kategorie 3 oder 4 verwendet;

— bereits bewertete Plattform: die Hardware und die interne Software (SRESW) wurden für die Sicherheitsanwendungen entworfen und bereits beurteilt, so dass sie diesem Dokument oder der Normenreihe IEC 61508 oder IEC 62061:2021 für den erforderlichen Performance Level (PL_r) entsprechen.

Quelle: Anhang N ISO 13849-1

ISO 13849-1 (Software)

Anhang N1, Tabelle 2
Auswahl der Maßnahmen für sicherheitsbezogene Anwendungssoftware (SRASW) in LVL

	Fall	Fall 1	Fall 2	Fall 3	Fall 4
1	Diese grundlegenden Maßnahmen sollten angewendet werden:				
a)	Entwicklungslebenszyklus mit Verifizierungs- und Validierungstätigkeiten, siehe Bild 14 a) und Bild 14 b);	m	m	m	m
b)	Dokumentation der Spezifikation und des Entwurfs;				
c)	Modulare und strukturierte Programmierung;				
d)	Funktionstests (z. B. Black-Box-Tests);				
e)	Geeignete Entwicklungsaktivitäten nach Änderungen.				
2	Die Spezifikation der sicherheitsbezogenen Software sollte überprüft werden (siehe auch Anhang J) und jeder Person zur Verfügung stehen, die am Lebenszyklus des V-Modells beteiligt ist, und sollte die Beschreibung enthalten von:				
a)	Sicherheitsfunktionen mit erforderlichem PL und zugehörigen Betriebsarten;	—	m	m	m
b)	Leistungskriterien, z. B. Reaktionszeiten;				
c)	Hardwarearchitektur mit externen Signalschnittstellen; und				
d)	Erkennung und Beherrschung von Hardware-Ausfällen.				
3	Auswahl der Werkzeuge, Bibliotheken, Sprachen:				

Quelle: Anhang N ISO 13849-1

ISO 13849-1 (Software)

Embedded SW von Standardkomponenten

Bauteile mit **nicht zugänglicher Embedded Software** dürfen unter **folgenden alternativen Bedingungen** verwendet werden:

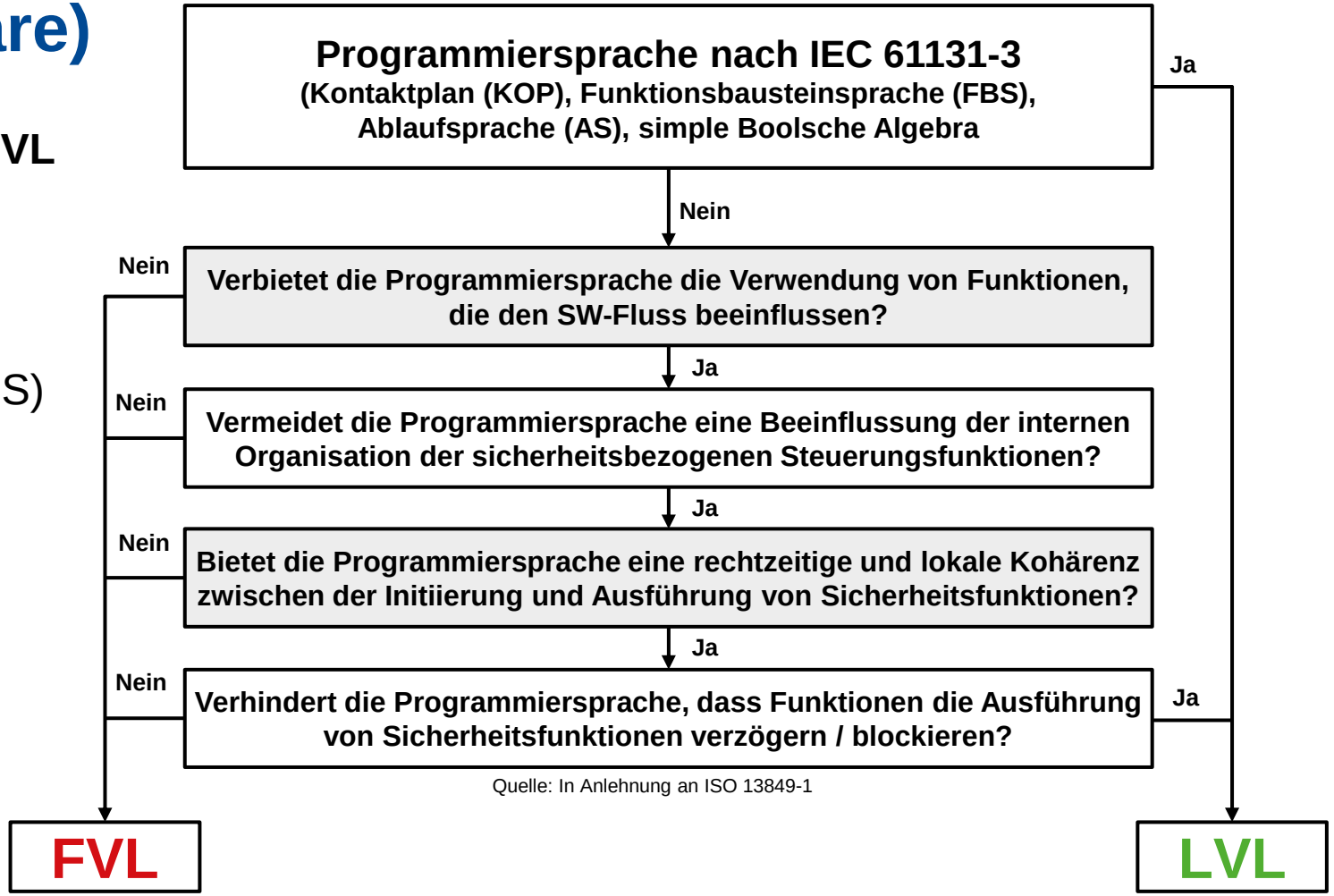
- das **Teilsystem** ist auf **PL a** oder **PL b** begrenzt und verwendet **Kategorie B, 2 oder 3**
- das **Teilsystem** ist auf **PL c** mit **Kategorie 2** oder **PL d** mit **Kategorie 3** begrenzt **und … beide Kanäle** verwenden **diverse Technologien**, **Entwicklungen** oder **physikalische Prinzipien**
- die zugehörige **Hardware** und die **Anforderungen** zu **SRASW** müssen gemäß den **Anforderungen** der **ISO 13849-1** beurteilt werden, …

ISO 13849-1 (Software)

Entscheidungshilfe LVL oder FVL

LVL Sprachen nach IEC 61131-3:

- Kontaktplan (KOP)
- Funktionsbausteinsprache (FBS)
- Ablaufsprache (AS)
- simple Boolsche Algebra



Quelle: In Anlehnung an ISO 13849-1

IEC 62061 (Software)

Softwarelevel nach der IEC 62061

SW level	Wesentliches Prinzip	Grundlage	Beispiel
1	Plattform (Kombination aus Hardware und Software), die gemäß IEC 61508 oder anderen mit IEC 61508 verknüpften Normen zur funktionalen Sicherheit, z. B. IEC 61131-6, bereits entworfen und geprüft wurde. Anwendungssoftware, die eine Sprache mit begrenzter Variabilität (LVL) verwendet.	Anwendungssoftware, die mit diesem Dokument übereinstimmt.	Sicherheits-SPS mit LVL oder programmierbares Sicherheitsrelais
2	Plattform (Kombination aus Hardware und Software), die gemäß IEC 61508 oder anderen mit IEC 61508 verknüpften Normen zur funktionalen Sicherheit, z. B. IEC 61131-6, bereits entworfen und geprüft wurde. Anwendungssoftware, die eine Sprache mit begrenzter Variabilität (LVL) verwendet	Anwendungssoftware, die mit diesem Dokument übereinstimmt.	Sicherheits-SPS mit FVL (FVL, die diesem Dokument entspricht.)
3		Anwendungssoftware, die der IEC 61508-3 entspricht.	Sicherheits-SPS mit LVL oder FVL (FVL gemäß IEC 61508)

Quelle: IEC 62061

Software-Level 3
ist nicht Bestandteil der
IEC 62061

Inhalt

Änderungen der ISO 13849-1 / IEC 62061 und 14119

1. Allgemein
2. Software
3. **EMV / EMC**
4. Architekturanforderungen
5. Akzeptanz von Teilsystemen
6. Security-Aspekte
7. Validierung
8. Management der funktionalen Sicherheit
9. Unabhängigkeit von Aktivitäten
10. Risikoeinschätzung
11. Gerätetypen
12. Sonstiges
13. ISO 14119

Anforderungen zur elektromagnetischen Störfestigkeit (EMI)

ISO 13849-1

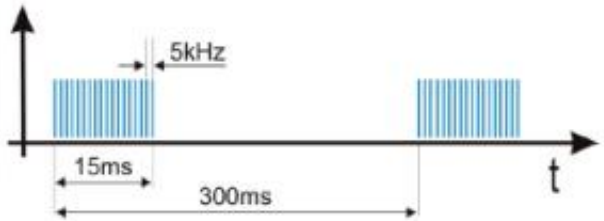
Ein neuer informativer Anhang L beschreibt vier verschiedene Pfade zur Erfüllung der Anforderungen zur elektromagnetischen Störfestigkeit.

IEC 62061

Das SCS muss die anwendbaren Anforderungen der IEC 61000-1-2 erfüllen.

Die entsprechenden Störfestigkeitslevel für industrielle Umgebungen sind mindestens in IEC 61326-3-1 oder IEC 61000-6-7 festgelegt.

Quelle: BGHM



Inhalt

Änderungen der ISO 13849-1 / IEC 62061 und ISO 14119

1. Allgemein
2. Software
3. EMV / EMC
4. **Architekturanforderungen**
5. Akzeptanz von Teilsystemen
6. Security-Aspekte
7. Validierung
8. Management der funktionalen Sicherheit
9. Unabhängigkeit von Aktivitäten
10. Risikoeinschätzung
11. Gerätetypen
12. Sonstiges
13. ISO 14119

Bewährte Bauteile in Kategorie 1 (ISO 13849-1)

Kategorie 1: Anforderungen an **„bewährte Bauteile“** sind jetzt im **separaten Abschnitt** (6.1.11)

6.1.11 Bewährte Bauteile sind:

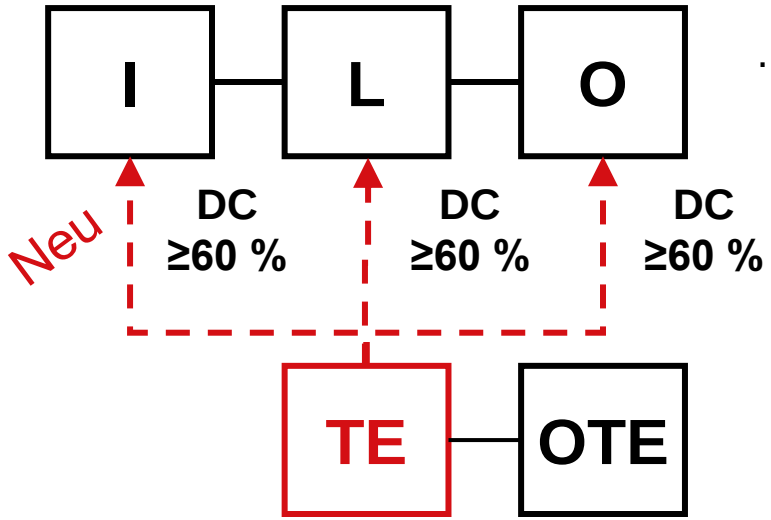
a) in der Vergangenheit weit verbreitet mit **dokumentierten** erfolgreichen Ergebnissen in ähnlichen Anwendungen verwendet worden;
   Anmerkung: Siehe IEC 61508-2:2010, 7.4.10, für „betriebsbewährt“

b) in den informativen **Anhängen A bis D der ISO 13849-2** aufgelistet, **oder**

c) unter **Anwendung** von **Prinzipien hergestellt** und **verifiziert**, die ihre **Eignung** und **Zuverlässigkeit** für **sicherheitsbezogene Anwendungen** gemäß **relevanten Produktnormen** zeigen.

ANMERKUNG: **Komplexe elektronische Bauteile** (z. B. PLC, Mikroprozessor, integrierte Schaltung, …) dürfen **nicht** als **„bewährt“** betrachtet werden.

Änderung in der Kategorie 2 (ISO 13849-1)



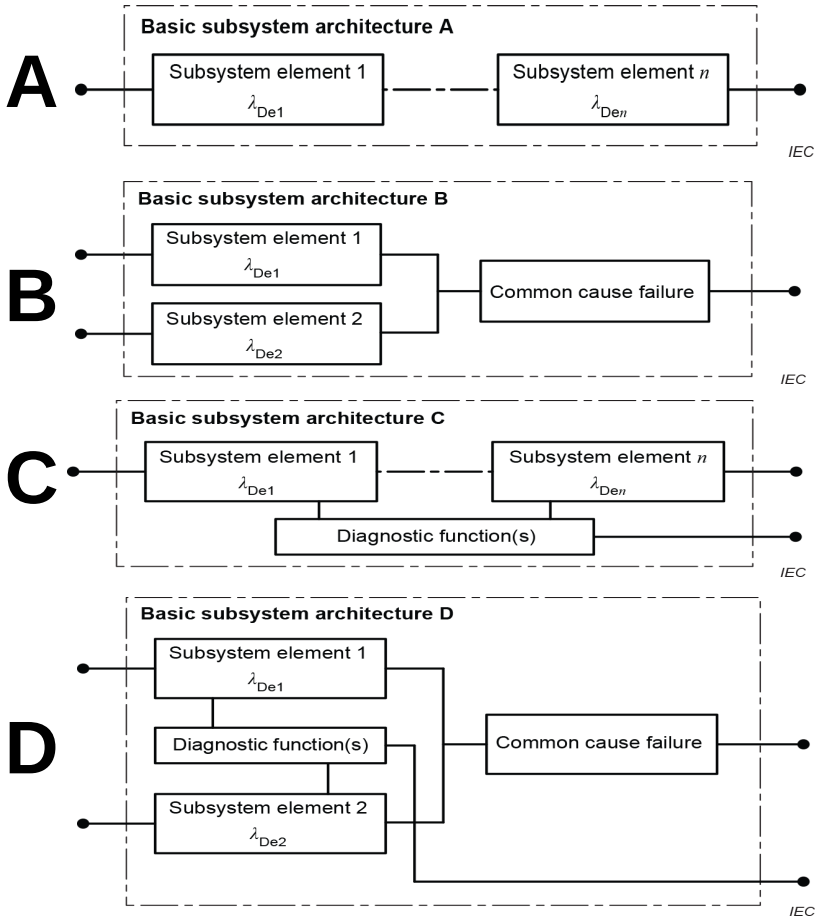
Neu

- $MTTF_D$ des Testkanals ist größer als die Hälfte der $MTTF_D$ des Funktionskanals

- *Das Testen der Sicherheitsfunktion (SIF) muss*
  - vor dem Beginn eines neuen Zyklus oder
  - vor Anlauf von Bewegungen oder
  - unmittelbar vor Anforderung der SIF oder
  - in angemessen Zeiträume (Anforderungsrate ≤ 1/100 der Testrate)

  erfolgen!

Basisanforderungen für Teilsystem-Architekturen A bis D (IEC62061)



Grundlegende Anforderungen	Hardware-Fehlertoleranz (HFT) 0		1	
	SFF <60 %	*SFF* ≥ 60 %	*SFF* <60 %	*SFF* ≥ 60 %
Grundlegende Sicherheitsprinzipien	M	M	M	M
Bewährte Sicherheitsprinzipien	M	M	M	M
Bewährte Bauteile	M	--	--	--
CCF	nicht relevant	M	M	M
Basis-Teil-systemarchitektur	**A**	**C**	**B**	**D**

M = verpflichtend (mandatory)

Quelle: In Anlehnung an IEC 62061:2021

Inhalt

Änderungen der ISO 13849-1 / IEC 62061 und ISO 14119

1. Allgemein
2. Software
3. EMV / EMC
4. Architekturanforderungen
5. **Akzeptanz von Teilsystemen**
6. Security-Aspekte
7. Validierung
8. Management der funktionalen Sicherheit
9. Unabhängigkeit von Aktivitäten
10. Risikoeinschätzung
11. Gerätetypen
12. Sonstiges
13. ISO 14119

Akzeptanz von nach anderen Standards entworfenen Teilsystemen

ISO 13849-1

Route 1_H nach IEC 61508-2 für High Demand Systeme und / oder mit kontinuierlicher Anforderung

PL	SIL
a	-
b	1
c	1
d	2
e	3

Quelle: In Anlehnung an ISO 13849-1

IEC 62061

Route 1_H nach IEC 61508-2 für High Demand Systeme und / oder mit kontinuierlicher Anforderung

Keine Akzeptanz von Teilsystemen nach ISO 13849, die komplexe Komponenten verwenden

IEC 62061 (IEC 61508)	IEC 62061	IEC 61508 [a]	ISO 13849 [b]	IEC 61496
PFH	SIL	at least ...	at least ...	at least ...
< 10^{-5}	SIL 1	SIL 1	PL b, c	Type 2
< 10^{-6}	SIL 2	SIL 2	PL d	Type 3
< 10^{-7}	SIL 3	SIL 3	PL e	Type 4

NOTE A relation between IEC 62061 and IEC 61511 (all parts) or ISO 26262 cannot be assumed within this table.

[a] This column includes SIL-based standards that fulfil the architectural constraints of IEC 61508, such as IEC 61800-5-2 and IEC 60947-5-3.

[b] **Does not apply to subsystems using complex components**, unless they meet the requirements of IEC 61508 or applicable functional safety products standards.
Performance Level b does not correspond to SIL1 in case of a category B (ISO 13849-1) structure.

Quelle: In Anlehnung an IEC 62061:2021

Inhalt

Änderungen der ISO 13849-1 / IEC und ISO 14119

1. Allgemein
2. Software
3. EMV / EMC
4. Architekturanforderungen
5. Akzeptanz von Teilsystemen
6. **Security-Aspekte**
7. Validierung
8. Management der funktionalen Sicherheit
9. Unabhängigkeit von Aktivitäten
10. Risikoeinschätzung
11. Gerätetypen
12. Sonstiges
13. ISO 14119

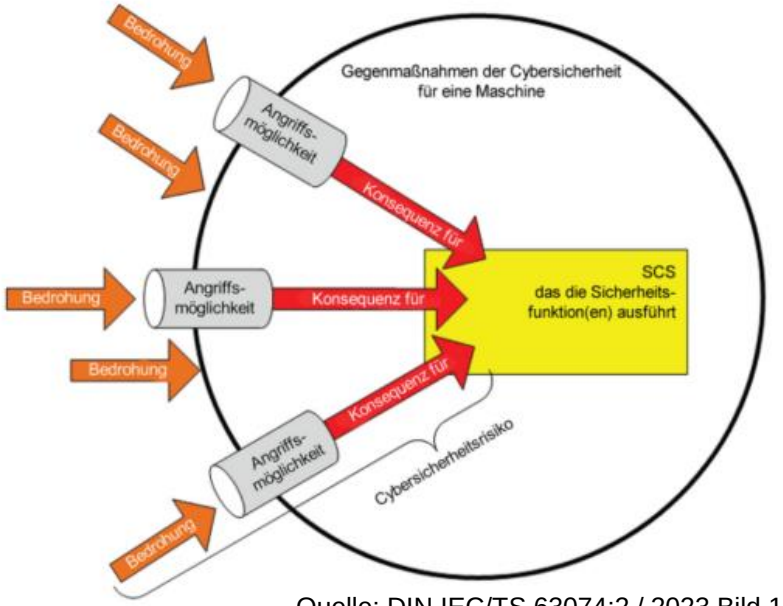
Security

ISO 13849-1

- Enthält keine Securitymaßnahmen.
  Anmerkung: Securityaspekte können einen Einfluss au Sicherheitsfunktionen haben.

IEC 62061

- Wenn Maßnahmen gegen Securityeinflüsse zur Anwendung kommen, dürfen sie die Sicherheits-integrität nicht nachteilig beeinflussen.



Quelle: DIN IEC/TS 63074:2 / 2023 Bild 1

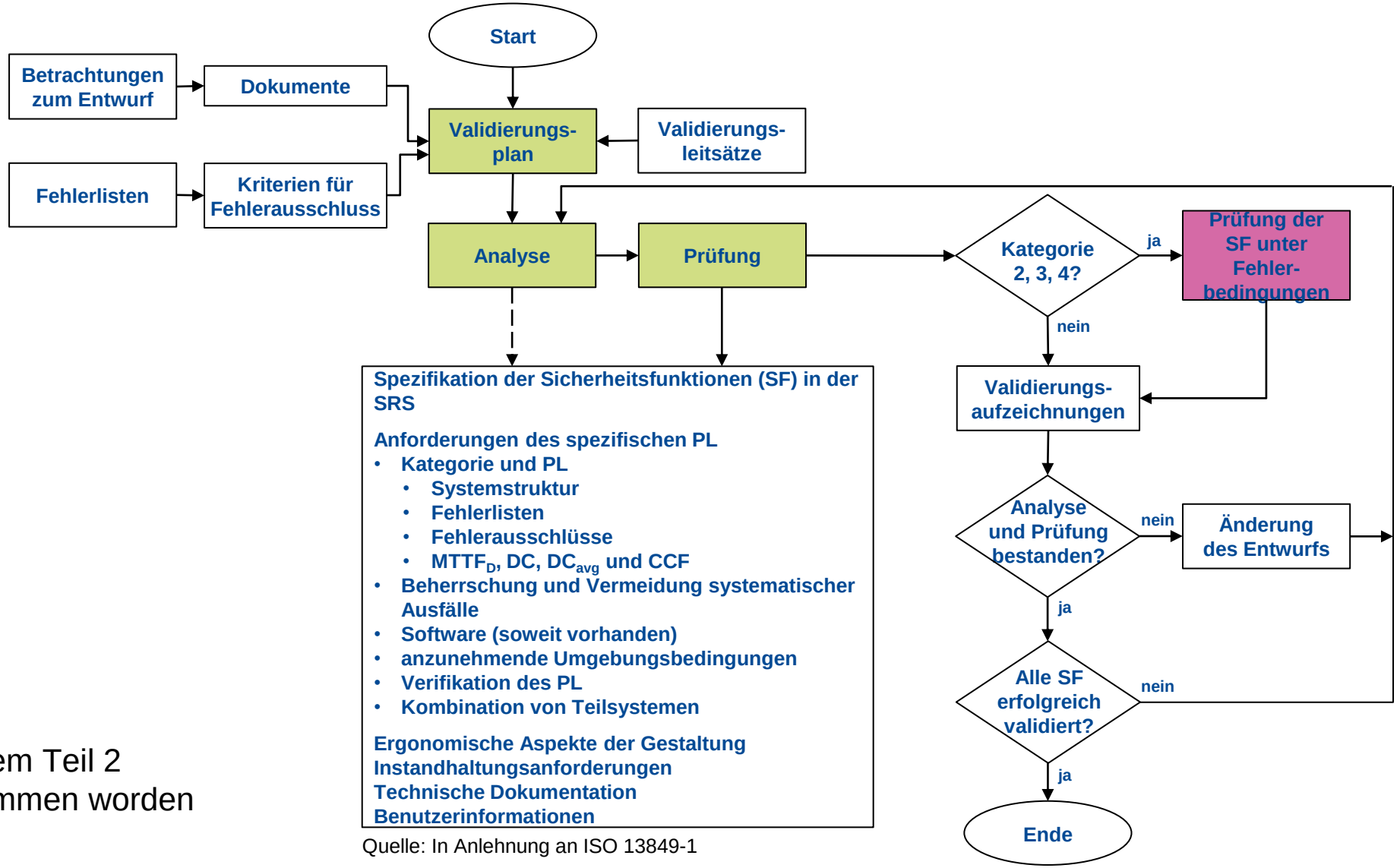
Beide Normen verweisen z.B. auf die **IEC/TS 63074 (2 / 2023)** „Aspekte zur **Cybersicherheit** in Verbindung mit der funktionalen Sicherheit von **sicherheitsrelevanten Steuerungssystemen“!**

Inhalt

Änderungen der ISO 13849-1 / IEC 62061 und ISO 13814

1. Allgemein
2. Software
3. EMV / EMC
4. Architekturanforderungen
5. Akzeptanz von Teilsystemen
6. Security-Aspekte
7. **Validierung**
8. Management der funktionalen Sicherheit
9. Unabhängigkeit von Aktivitäten
10. Risikoeinschätzung
11. Gerätetypen
12. Sonstiges
13. ISO 14119

Validierung (ISO 13849-1)

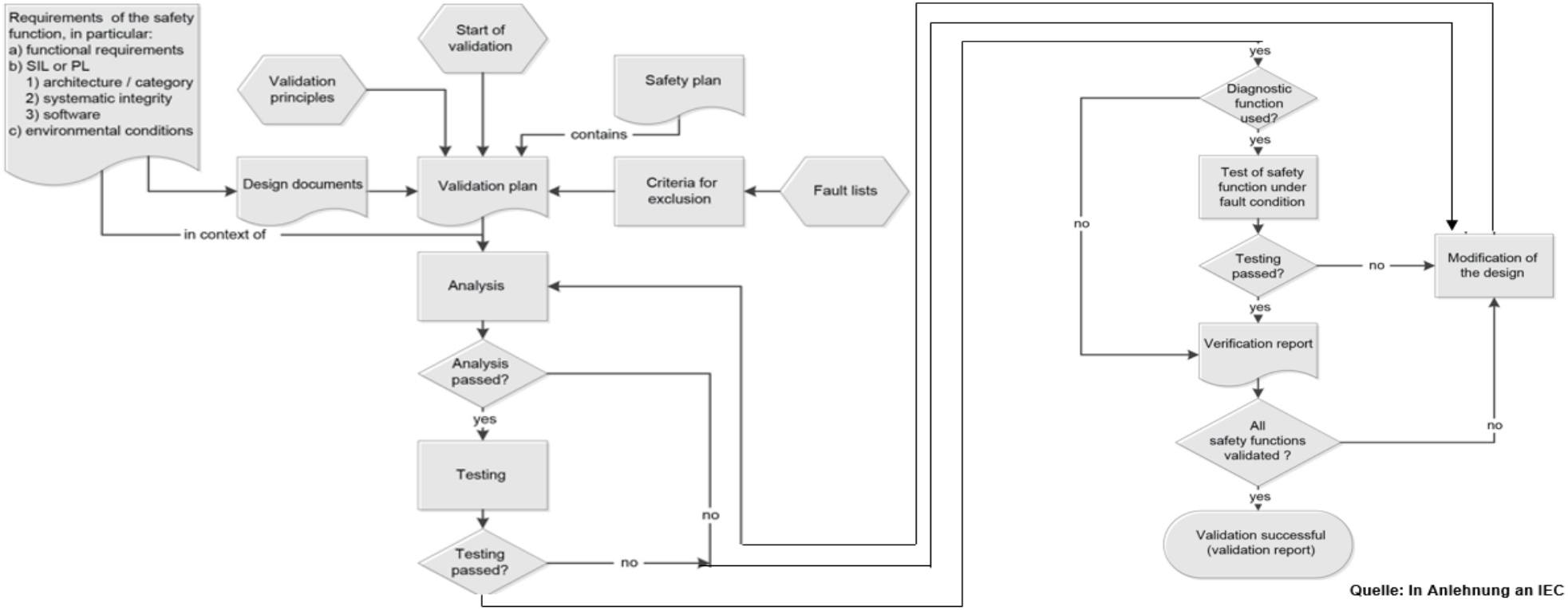


Quelle: In Anlehnung an ISO 13849-1

Die Validierung ist aus dem Teil 2 der ISO 13849-2 übernommen worden

Validierung (IEC 62061)

- Validierung durch Analyse und Prüfung nach einem Validierungsplan

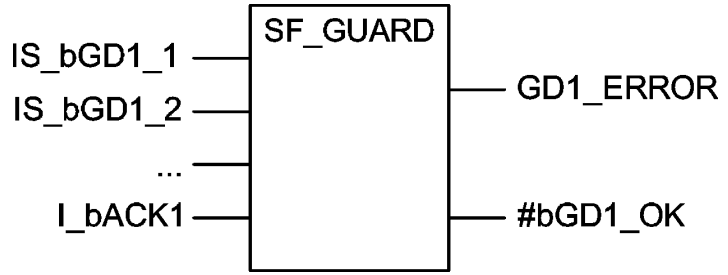


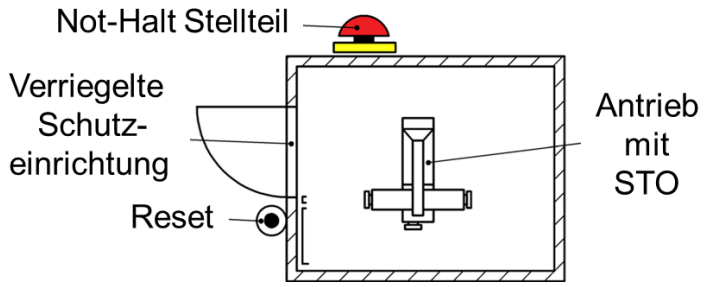
Quelle: In Anlehnung an IEC 62061:2021, Bild 15

Validierung Software (ISO 13849-1)

Sicherheitsfunktionen:

- Stoppfunktion eingeleitet durch Öffnen der verriegelten Schutzeinrichtung
- Nothaltfunktion





Nr.	Fehler	Reaktion	OK?

1	IS_bGD1_1 = LOW,
	IS_bGD1_2 = LOW
		#bGD1_OK = LOW,
		GD1_ERROR = LOW
			✓

2	IS_bGD1_1 = HIGH (permanent),
	IS_bGD1_2 = HIGH → LOW
		#bGD1_OK = LOW,
		GD1_ERROR = LOW → HIGH
			✓

3	IS_bGD1_1 = HIGH → LOW,
	IS_bGD1_2 = HIGH (permanent)
		#bGD1_OK = LOW,
		GD1_ERROR = LOW → HIGH
			✓

4	…	…	

Quelle: In Anlehnung an ISO 13849-1 Anhang N2

In der IEC 62061 ist auch ein Beispiel vorhanden!

Inhalt

Änderungen der ISO 13849-1 / IEC 62061 und ISO 14119

1. Allgemein
2. Software
3. EMV / EMC
4. Architekturanforderungen
5. Akzeptanz von Teilsystemen
6. Security-Aspekte
7. Validierung
8. **Management der funktionalen Sicherheit**
9. Unabhängigkeit von Aktivitäten
10. Risikoeinschätzung
11. Gerätetypen
12. Sonstiges
13. ISO 14119

Management der funktionalen Sicherheit

ISO 13849-1

- Ein Plan zur funktionalen Sicherheit soll Maßnahmen zur **Vermeidung** von **Fehlern** bei der **Spezifikation, Implementierung** oder **Änderung** enthalten (neuer informativer Anhang G.5).

IEC 62061

- Ein Plan zur funktionalen Sicherheit muss Maßnahmen zur **Vermeidung** von **Fehlern** bei der **Spezifikation, Implementierung** oder Änderung vorsehen.

Auszug aus Abschnitt 6.1.7 (ISO13849-1):

Aktivitäten, die für das Erreichen der erforderlichen funktionalen Sicherheit des SRP/CS notwendig sind, müssen in einem Plan der funktionalen Sicherheit festgelegt sein.

Quelle: BGHM

Inhalt

Änderungen der ISO 13849-1 / IEC 62061 und ISO 14119

1. Allgemein
2. Software
3. EMV / EMC
4. Architekturanforderungen
5. Akzeptanz von Teilsystemen
6. Security-Aspekte
7. Validierung
8. Management der funktionalen Sicherheit
9. **Unabhängigkeit von Aktivitäten**
10. Risikoeinschätzung
11. Gerätetypen
12. Sonstiges
13. ISO 14119

Unabhängigkeit von Aktivitäten (Review, Prüfung, Verifikation, Validierung)

IEC 62061

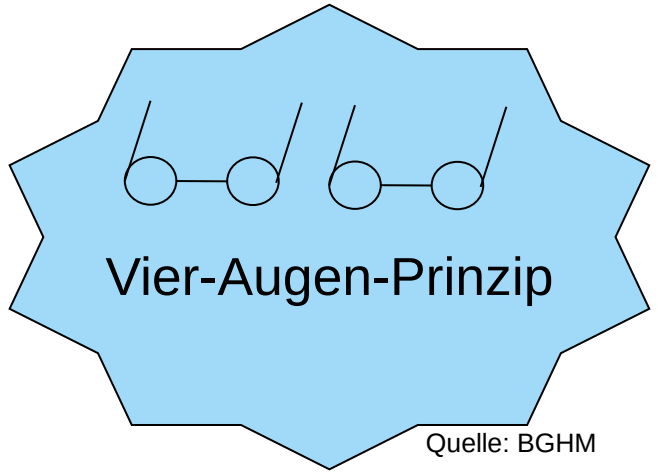
Minimum level of independence	SIL 1	SIL 2	SIL 3
Same person	not sufficient	not sufficient	not sufficient
Other person	not sufficient *	not sufficient *	not sufficient
Independent person	sufficient	sufficient	sufficient

*Eine "andere Person" ist ausreichend für Software-Level 1 (Kombination vorgefertigter Softwaremodule)

Eine „unabhängige Person“
- kann am selben Projekt beteiligt sein,
- sollte aber nicht an Entwurfsaktivitäten beteiligt sein,
- sollte nicht für das Projektmanagement verantwortlich sein
- und keine übergeordnete Rolle spielen.

ISO 13849-1

Der Validierungsprozess sollte von Personen durchgeführt werden, die unabhängig vom Entwurf des SRP/CS sind.



Quelle: BGHM

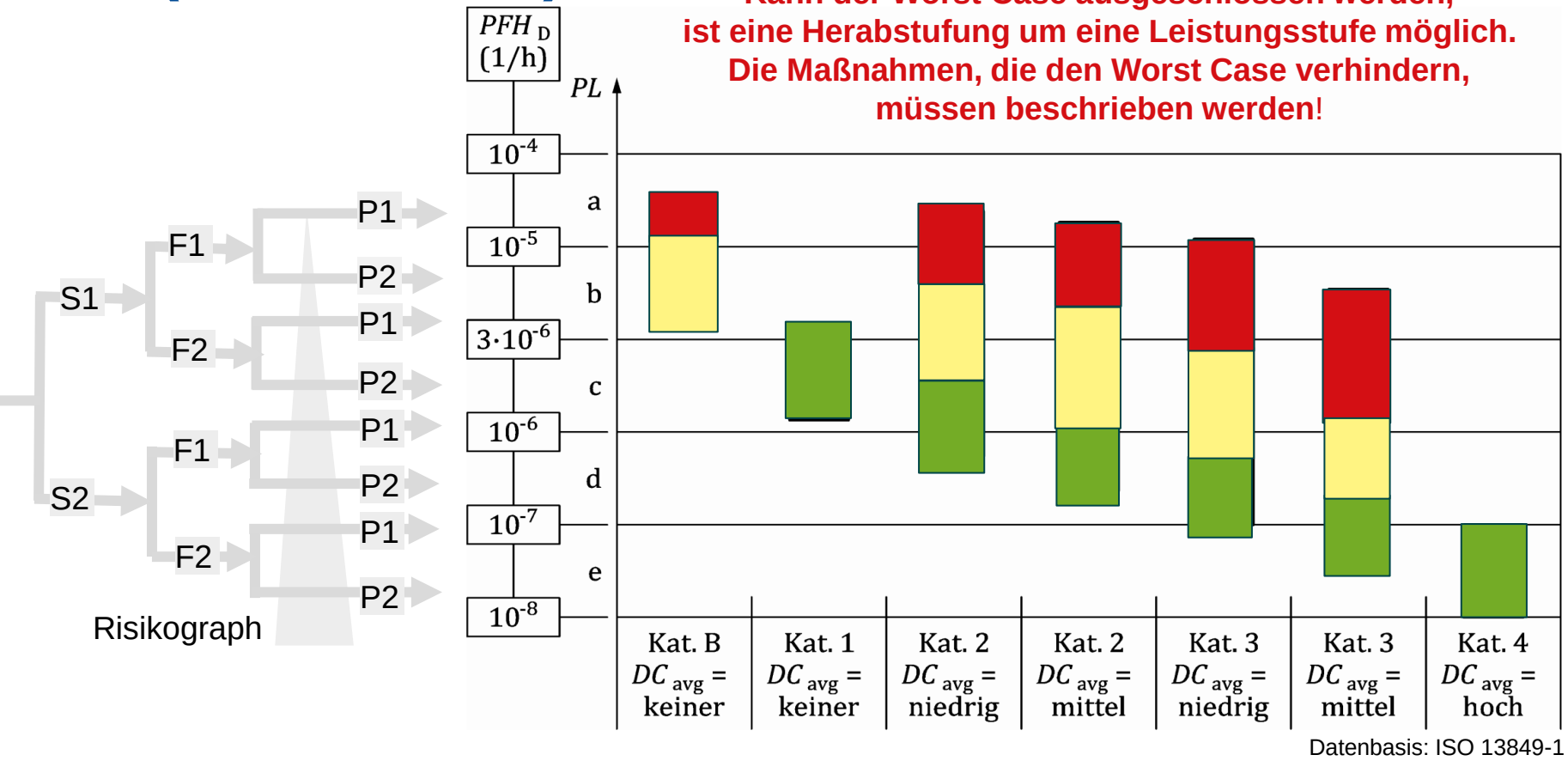
Inhalt

Änderungen der ISO 13849-1 / IEC 62061 und ISO 14119

1. Allgemein
2. Software
3. EMV / EMC
4. Architekturanforderungen
5. Akzeptanz von Teilsystemen
6. Security-Aspekte
7. Validierung
8. Management der funktionalen Sicherheit
9. Unabhängigkeit von Aktivitäten
10. **Risikoeinschätzung**
11. Gerätetypen
12. Sonstiges
13. ISO 14119

Bestimmung des erforderlichen Performance Levels (ISO 13849-1)

**Kann der Worst Case ausgeschlossen werden,
ist eine Herabstufung um eine Leistungsstufe möglich.
Die Maßnahmen, die den Worst Case verhindern,
müssen beschrieben werden!**



Datenbasis: ISO 13849-1

Legende:

- $MTFF_D$ = niedrig; 3 bis10 Jahre
- $MTFF_D$ = mittel; 10 bis 30 Jahre
- $MTFF_D$ = hoch; 30 bis 100 Jahre (bei Kat. 4 max. 2500 Jahre)

DC_{avg} niedrig 60% - 90%
DC_{avg} mittel ≥ 90% < 99%
DC_{avg} hoch ≥ 99%

Anmerkung: DC Begrenzung bei Monitoring durch den Arbeitsprozess

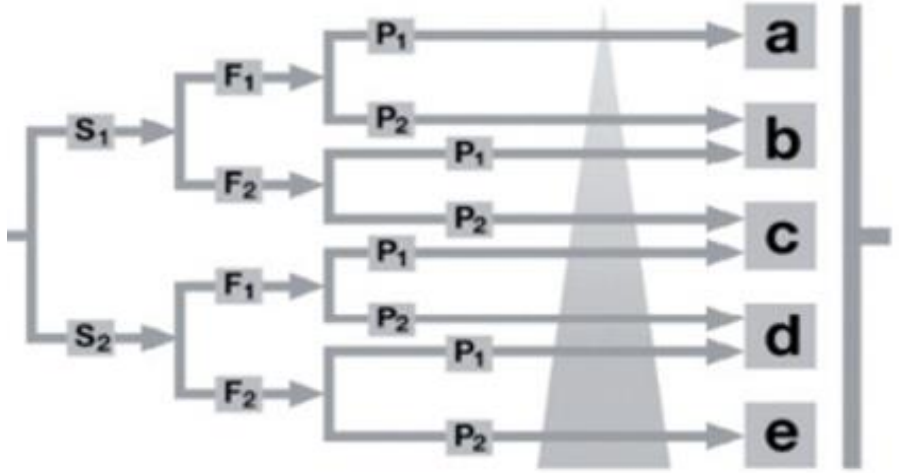
r_t/r_d=1 ➡ DC_{Max} = 60%
r_t/r_d=10 ➡ DC_{Max} = 90%
r_t/r_d=100 ➡ DC_{Max} = 99%

Das Verhältnis der Testrate (r_t) zur Anforderungsrate (r_d) begrenzt den DC

Bestimmung des erforderlichen Performance Levels (ISO 13849-1)

Erforderliche Parameter:

- Schweregrad der Verletzung
  - **S1** = leichte, reversible Verletzungen
  - **S2** = schwere, irreversible Verletzungen sowie der Tod



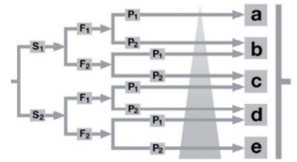
Quelle: In Anlehnung an ISO 13849-1

- Häufigkeit und / oder Expositionszeiten gegenüber der Gefährdung
  - **F1** bei 1/20 der Gesamtbetriebszeit beträgt und maximal einmal in 15 Min.
  - **F2** sollte gewählt werden, wenn eine Person häufig oder ständig der Gefährdung ausgesetzt ist.

Ein allgemein gültiger Zeitraum kann für F1 oder F2 nicht angegeben werden.

Bestimmung des P- Parameter

Bestimmung des Parameters P auf der Grundlage von fünf Faktoren			
Faktor	C	B	A
1. Nutzung der Maschine durch		Ungelernte Person	Befähigte Person (Fachmann)
2. Geschwindigkeit des Teils der Maschine, der ein gefährliches Ereignis auslösen kann (abhängig von der spezifischen Maschine)	Ereignis bei hoher Geschwindigkeit (z.B. über 1 000 mm/s, Zeit bis zur Gefährdung < 1 s)	Ereignis bei mittlerer Geschwindigkeit (z.B. 251 mm/s bis 1 000 mm/s, Zeit bis zur Gefährdung < 3 s)	Ereignis bei niedriger oder sehr niedriger Geschwindigkeit (z.B. max. 250 mm/s, Zeit bis zur Gefährdung ≥ 3 s)
3. Möglichkeit die Gefährdung zu vermeiden	Nicht möglich	In weniger als 50 % der Fälle möglich	In mehr oder gleich 50 % der Fälle möglich
4. Möglichkeit der Wahrnehmung der Gefährdung	Nicht möglich (z.B. Instrumentierung notwendig, der menschliche Sinn ist nicht in der Lage, die Gefahr wahrzunehmen, Umweltbedingungen verdecken die Wahrnehmung)	In weniger als 50 % der Fälle möglich	In mehr oder gleich 50 % der Fälle möglich
5. Komplexität der Operationen (menschliche Interaktion im Hinblick auf die Anzahl der Operationen und/oder die für diese Operationen verfügbare Zeit)		Hohe Komplexität (z.B. Fehlerbehebung) oder Mittlere Komplexität (z.B. Verwendung der Hold-To-Run-Steuerung zum Einrichten eines Teils der Maschine)	Geringe Komplexität (z.B. Einstellen der Werkstückspanner) oder Sehr geringe Komplexität / oder keine Interaktion (z.B. ein Werkstück in die Maschine einlegen)



ISO13849-1
Risikograph

Ergebnis

Auswahl des Parameters P1 oder P2		
Gesamtpunktzahl		Parameter "P"
ein oder mehrere "C"		P2
kein "C", drei oder mehr "B"		P2
kein "C", zwei "B", der Rest "A"		P1 oder P2 je nach Spezifikation der Maschine
kein "C", ein oder kein "B", der Rest "A".		P1

Quelle: In Anlehnung an ISO 13849-1

Inhalt

Änderungen der ISO 13849-1 / IEC 62061 und ISO 14119

1. Allgemein
2. Software
3. EMV / EMC
4. Architekturanforderungen
5. Akzeptanz von Teilsystemen
6. Security-Aspekte
7. Validierung
8. Management der funktionalen Sicherheit
9. Unabhängigkeit von Aktivitäten
10. Risikoeinschätzung
11. **Gerätetypen**
12. Sonstiges
13. ISO 14119

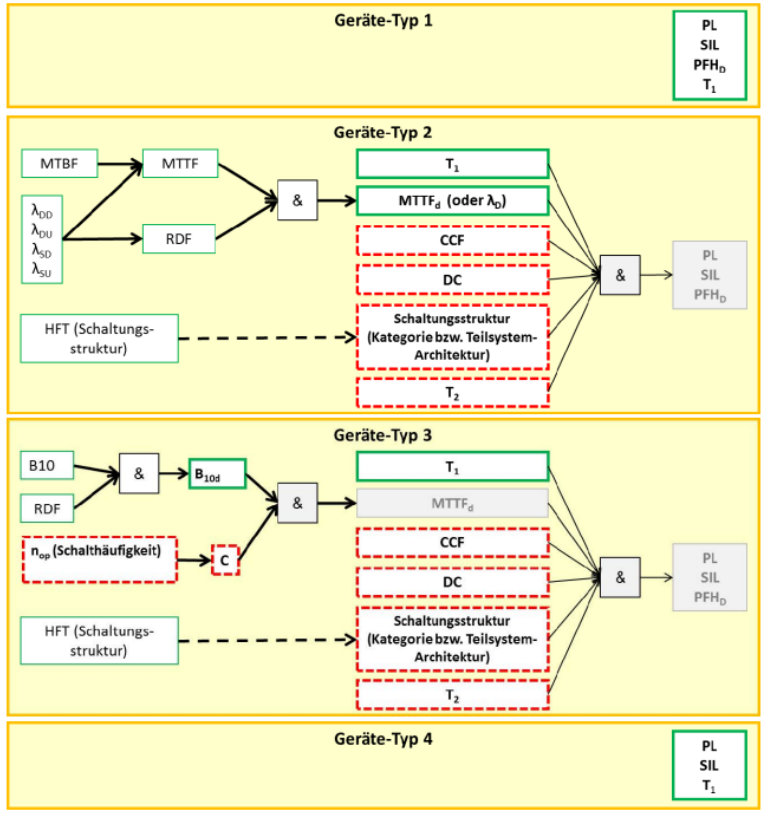
Geräte-Typen (ISO 13849-1 Anhang O)

- **Geräte-Typ 1:**
  gekapselte Subsysteme mit SIL oder PL (Pre-designed)

- **Geräte-Typ 2:**
  für Subsysteme mit vorgesehenen Architekturen (Kategorien) nach ISO 13849 oder IEC 62061 unabhängig von der Schalthäufigkeit (Not pre-designed)

- **Geräte-Typ 3:**
  wie Geräte-Typ 2, Ausfallverhalten abhängig von der Schalthäufigkeit (Not pre-designed)

- **Geräte-Typ 4:**
  gekapseltes Subsystem mit $PFH_D = 0$ (Fehlerausschluss oder nur sichere Fehler, z. B. selbstüberwachtes pneumatisches PSV)



Quelle: In Anlehnung an VDMA 66413

Inhalt

Änderungen der ISO 13849-1 / IEC 62061 und ISO 14119

1. Allgemein
2. Software
3. EMV / EMC
4. Architekturanforderungen
5. Akzeptanz von Teilsystemen
6. Security-Aspekte
7. Validierung
8. Management der funktionalen Sicherheit
9. Unabhängigkeit von Aktivitäten
10. Risikoeinschätzung
11. Gerätetypen
12. **Sonstiges**
13. ISO 14119

ISO 13849-1 (weitere Änderungen)

- **Kategorie 2**: **Verhältnis** von **Testrate** zu **Anforderungsrate** der Sicherheitsfunktion (Faktor 100) und $MTTF_D$ des **Testkanals** sind nun **Teil** der **Kategorie- 2- Anforderungen**

- **Kategorie 4**: neue Anmerkung: **Unerkannte Fehler** mit **sehr niedriger Wahrscheinlichkeit** müssen bei der **Fehlerakkumulation** (z. B. FMEA) **nicht berücksichtigt** werden.

- **Anforderungen** zur Nutzung von **Remote- Zugängen** (5.2.4)

- **alternatives Verfahren** zur Bestimmung von **PL und PFH_D ohne $MTTF_D$** ausgeweitet auf **Eingang, Logik** und **Ausgang** (beschränkt auf Teilsysteme in Mechanik, Hydraulik, Pneumatik, Elektrohydraulik und -pneumatik, **nur nutzbar** wenn **Zuverlässigkeitsdaten** fehlen)

ISO 13849-1 (weitere Änderungen)

- **quantitative Limitierung** bestimmter **Diagnosemaßnahmen** (Anhang E)
- **CCF-Maßnahmen detaillierter beschrieben** (F.3)
- **Beispiel Sicherheitsbezogene Embedded-Software (SRESW) Realisierung** ergänzt (Anhang J)
- **Beispiel** für **Softwarevalidierung** (Anhang N.2)
- mittlere **Häufigkeit** eines **gefahrbringenden Ausfalls je Stunde** (PFH)

IEC 62061 (weitere Änderungen)

- **Umstellung** von **"SILCL"** auf **"maximaler SIL"** eines Teilsystems
- **Architektur C**: Übersicht über verschiedene **Konstellationen** für **Fehlerdiagnose** und **-reaktion** (intern / extern) in Anhang H
- **Beispielwerte** für Komponenten und Beispiele für DC **aus ISO 13849-1** übernommen (Anhänge C & D)
- **Leitfaden** für **SW Level 1** mit Beispiel in Anhang F
- **Beispiele** für **Sicherheitsfunktionen** in Anhang G

Blick in die Zukunft

- **Revision** der **ISO 13849-2** gestartet

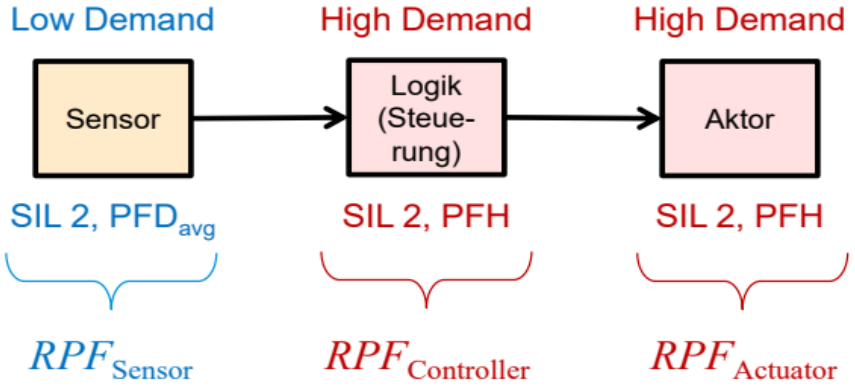
- **ISO TR 23849** – PFH-Formeln nach ISO 13849-1 in Vorbereitung

- **IEC TS 63394** – Guidelines on functional safety of safety-related control system (2023-02)
  Anwendung von **IEC 62061** und **ISO 13849**
  - Neu **“rarely activated”** (selten aktiv) **Sicherheitsfunktionen**
  - Enthält Vorschlag wie **low demand** und **high demand Teilsysteme** in **einer Sicherheitsfunktion** bewertet werden können.
  - **Berechnung** des quantitativen **Ausnutzungsgrad** des **Ziel-SIL**
    RPF (Ratio of Probability of Failures).

Low - und High demand in einer Sicherheitsfunktion (IEC TS 63394 Anhang J)

- **Keine** verfügbare **High Demand Sensorik** für diesen **Einsatzbereich**
- **Teilsysteme**, für die Betriebsart **hohe / kontinuierliche Betriebsweise** werden in **high demand** quantifiziert
- **SIF low demand** und **SIF high demand** werden auf der **Schnittstellenebene** betrachtet
- **Subsysteme** müssen für **beide Betriebsarten** geeignet sein
- **Anforderungen** an den **Proof-Test** (die nicht in der Logik realisiert werden können) sind in der **BA** zu beschreiben (Anforderungen siehe zugehörige C Norm)
- Die **Teilsysteme** „**High Demand**“ müssen mindestens den **gleichen SIL** haben wie das Subsystem „**Low Demand Sensorik“**
- Bestimmen des **quantitativen Ausnutzungsgrades Ziel-SIL RPF** (Ratio of Probability of Failures)

IEC TS 63394 “Bestimmung des RPF (Ratio of Probability of Failures)”.



Alle drei Komponenten für den geforderten SIL der SF qualifiziert (in diesem Beispiel SIL 2).

Unter der Voraussetzung kann der quantitative Ausnutzungsgrad des Ziel-SIL bestimmt werden
RPF (Ratio of Probability of Failures)

$$RPF_{\text{Sensor}} = \frac{PFD_{\text{avg, Sensor}}}{PFD_{\text{avg, max}}(\text{SIL 2})}$$

$$RPF_{\text{Controller}} = \frac{PFH_{\text{Controller}}}{PFH_{max}(\text{SIL 2})}$$

$$RPF_{\text{Actuator}} = \frac{PFH_{\text{Actuator}}}{PFH_{\text{max}}(\text{SIL 2})}$$

Der Ziel-SIL gilt in quantitativer Hinsicht als erreicht, wenn:

$$RPF_{\text{Sensor}} + RPF_{\text{Controller}} + RPF_{\text{Actuator}} \leq 100\ \%$$

SIL	$PFD_{avg\ max}$	PFH_{max} [h^{-1}]
1	10^{-1}	10^{-5}
2	10^{-2}	10^{-6}
3	10^{-3}	10^{-7}

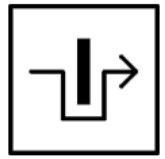
Quelle BGHM

Inhalt

Änderungen der ISO 13849-1 / IEC 62061 und ISO 14119

1. Allgemein
2. Software
3. EMV / EMC
4. Architekturanforderungen
5. Akzeptanz von Teilsystemen
6. Security-Aspekte
7. Validierung
8. Management der funktionalen Sicherheit
9. Unabhängigkeit von Aktivitäten
10. Risikoeinschätzung
11. Gerätetypen
12. Sonstiges
13. **ISO 14119**

ISO 14119 Verriegelungseinrichtungen in Verbindung mit trennenden Schutzeinrichtungen



Quelle: BGHM

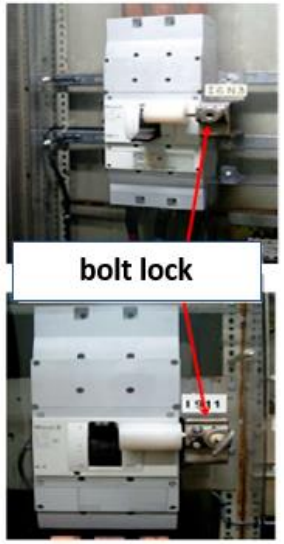
Auszug aus dem **Anwendungsbereich**

… Diese Internationale Norm behandelt **Teile von trennenden Schutzeinrichtungen**, die **Verriegelungseinrichtungen betätigen**, und deckt **Grundsätze** für die Gestaltung, Auswahl und Anwendung von **Verriegelungseinrichtungen** mit **Schlüsseltransfersystem** sowie **Systemen für Maschinenanwendungen** ab, unabhängig von der **Energieart**, die für deren **Steuerung** genutzt wird oder die diese **selbst steuern**.

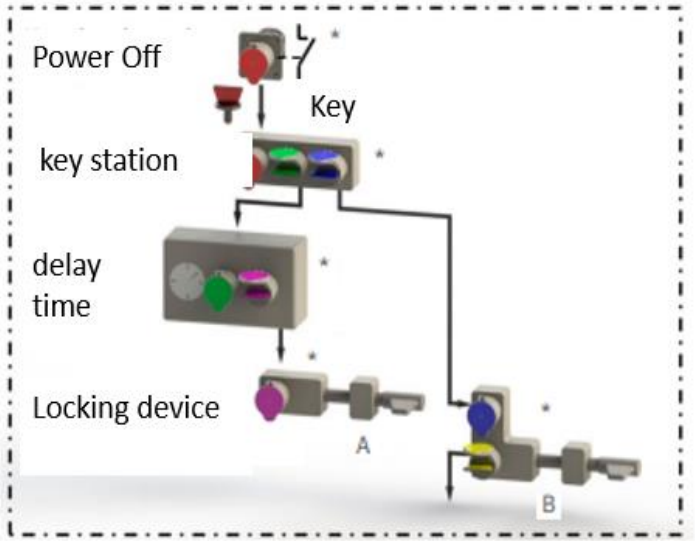
…

ISO 14119 (Stand 9/2023)

- Einarbeitung der Schlüsseltransfersysteme Änderung

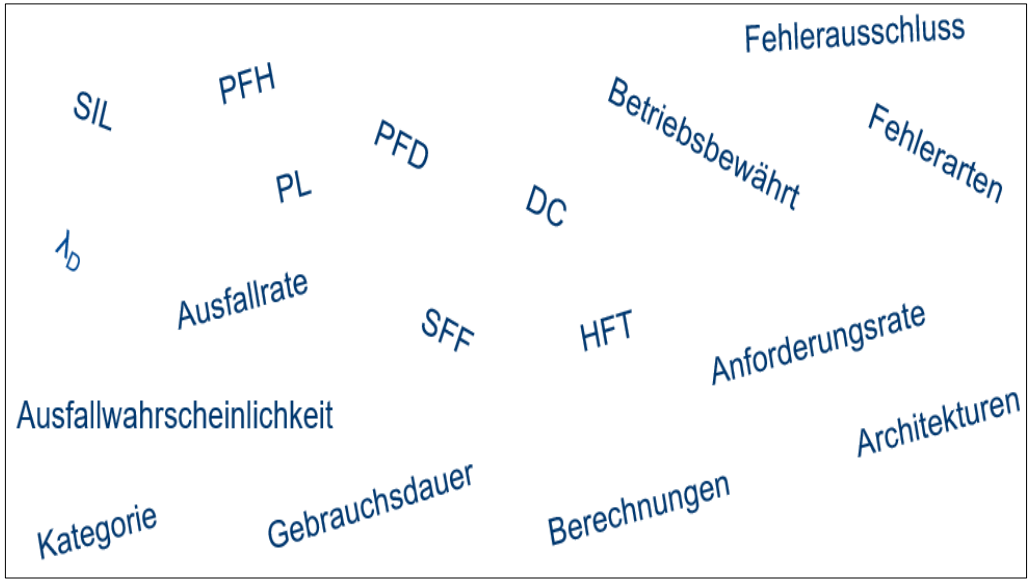


Quelle: BGHM



Quelle: BGHM

- Einarbeitung der Anforderungen aus der ISO 13849-1 und IEC 62061 Änderung



Quelle: BGHM

ISO 14119 (Stand 9/2023)

- Anhang J (normativ) Prüfverfahren

  Neu

  – J.1 Prüfung der Zuhaltekraft
  – J.2 Schlagfestigkeitsprüfung
  – J.3 Durchführung der Prüfung

- Anhang K (normativ) Sicherheit von Maschinen — Verriegelungseinrichtungen in Verbindung mit trennenden Schutzeinrichtungen — Leitsätze für Gestaltung und Auswahl
  Dieser Anhang hat folgende Ziele:

  Neu

  – Leitlinie für Benutzer zur Abschätzung der höchsten DC-Werte und des PL;
  – Leitlinie zur Konstruktion von SRP/CS.

- Anhang L (normativ) Verriegelungseinrichtungen der Bauart 5 — Verriegelungssysteme mit Schüsseltransfersystem

  Neu

Danke für Ihre Aufmerksamkeit