6 DIN EN IEC 62061 (VDE 0113-50) und DIN EN ISO 13849-1

DIN EN IEC 62061, Sicherheit von Maschinen – Funktionale Sicherheit sicherheitsbezogener Steuerungssysteme.

DIN EN ISO 13849-1, Sicherheit von Maschinen – Sicherheitsbezogene Teile von Steuerungen – Teil 1: Allgemeine Gestaltungsleitsätze

Im Prozess der Risikominderung DIN EN ISO 12100 können beide Normen verwendet werden, sobald technische Schutzmaßnahmen auf Basis einer Steuerungslösung verwendet werden sollen.

6.1 Zwei Normen rücken zusammen

Welche Vorliebe haben Sie?

Hört sich seltsam an, aber es ist wirklich so: Wenn ich die Kategorien der EN 954-1 kenne, dann werde ich auch die Nachfolgenorm DIN EN ISO 13849-1 verwenden. Logisch. Wer will schon etwas von Architekturen hören, wenn es Kategorien gibt?

Dass die DIN EN IEC 62061 (**VDE 0113-50**) nichts anderes macht, als Kategorien als einkanalige und zweikanalige Architekturen zu umschreiben, ist jedem Leser der Norm aufgefallen. Würde man diese dann auch noch mit dem Begriff Kategorie in Verbindung bringen, dann würden sich alle Bedenken in Luft auflösen. Dies geschah leider zu selten und somit lebt der Mythos der Kategorie EN 954-1 weiter.

Es wurde schon lange erkannt, dass das kein Kriterium sein darf. Und viele haben erkannt, dass die Grundsätze der Funktionalen Sicherheit der DIN EN IEC 62061 (**VDE 0113-50**) sehr wohl auch für alle Technologien verwendbar sind – der Anwendungsbereich verdeutlicht dies (**Bild 6.2**).

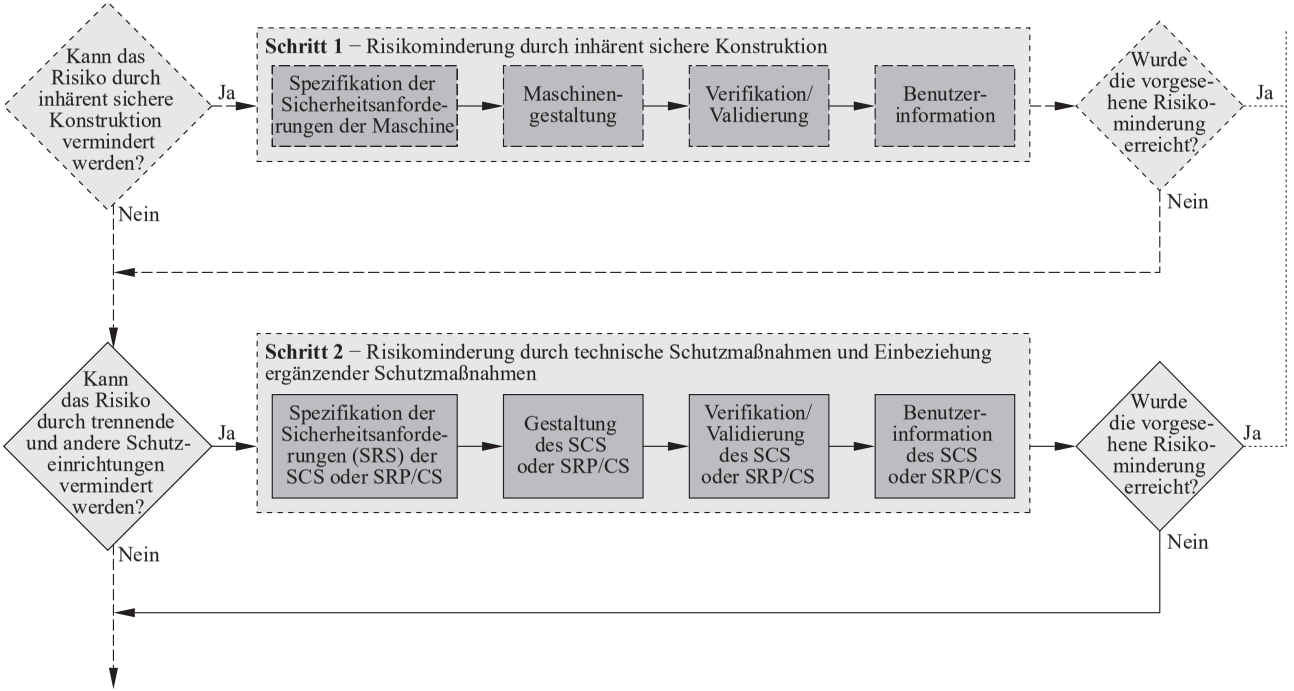

Bild 6.1 Risikominderung durch SCS oder SRP/CS

Diese internationale Norm legt Anforderungen fest und gibt Empfehlungen für den Entwurf, die Integration und die Validierung von sicherheitsbezogenen Steuerungssystemen (SCS) für Maschinen. Sie ist auf Steuerungssysteme anwendbar, die entweder einzeln oder in Kombination zur Ausführung von Sicherheitsfunktionen an Maschinen verwendet werden, die während der Arbeit nicht von Hand getragen werden, einschließlich einer Gruppe von Maschinen, die koordiniert zusammenarbeiten.

Bild 6.2 Anwendungsbereich der DIN EN IEC 62061 (**VDE 0113-50**)

Lassen Sie uns die in **Tabelle 6.1** gezeigte Gegenüberstellung machen und entscheiden Sie selbst, wie wichtig der Begriff der „Kategorien" ist.

DIN EN ISO 13849-1	**DIN EN IEC 62061 (VDE 0113-50)**			**DIN EN ISO 13849-1**
Kategorie	**Fehlertoleranz der Hardware 0 = einkanalig, 1 = zweikanalig**	***SFF* = DC_{avg}**	**Maximal erreichbarer SIL**	**Maximal erreichbarer PL**
1	0	< 60 %	SIL 1	PL c
2	0	60 % … 90 %	SIL 1/2	PL c/d
3	1	< 60 %	SIL 1	PL c
	1	60 % … 90 %	SIL 2	PL d
4	1	> 90 %	SIL 3	PL e

Tabelle 6.1 Vereinfachte sinnvolle Anwendung und Zuordnung von Kategorien zu PL und SIL

Eine Kategorie 2 Anwendung mit einem erreichbaren PL d oder SIL 2 ist mit Vorsicht zu genießen.

Kategorie 4 verlangt immer einen Diagnosedeckungsgrad $DC > 99$ % (±5 %). Da Kategorie 3 bis 90 % (±5 %) definiert ist, macht die Vereinfachung $DC > 90$ % für Kategorie 4 Sinn.

In der Praxis gibt es aus Anwendersicht nur 99 % oder mehr. Somit wären 99 % ohne ±5 % realistisch.

6.2 Plan der funktionalen Sicherheit

Management für alle – kein Nachteil für den Einzelnen

In diesem Plan (en: safety plan) sollen alle notwendigen Aktivitäten erfasst und dokumentiert werden, damit die notwendige Funktionale Sicherheit einer SCS bzw. SRP/CS, also die entscheidenden Teile einer Sicherheitsfunktion, sichergestellt ist. Der Begriff „Managementaktivitäten" in der Norm meint all die Aktivitäten, die diesbezüglich sowohl technisch als auch organisatorisch einzuhalten sind.

Warum sollte man das tun? Schauen wir uns dazu die Inhalte, die zu dokumentieren sind, etwas genauer an.

- *Welche Eingangsparameter gibt es, wer ist verantwortlich dafür?*
  - Die Verfahren und Ressourcen der relevanten Informationen für die Funktionale Sicherheit eines SCS bzw. SRP/CS (z. B. Risikobeurteilung, Sicherheitsmaßnahmen bzw. Einrichtungen, verantwortliche Organisation).
- *Wie wird die Funktionale Sicherheit erreicht?*
  - Erfassen der relevanten Aktivitäten in den Abschnitten 5 bis 9 der Norm,
  - Vorgehensweise zum Erreichen der festgelegten Anforderungen zur Funktionalen Sicherheit,
  - Anwendungssoftware und Strategie zum Erreichen der funktionalen Sicherheit bei Entwicklung, Integration, Verifikation und Validierung.
- *Wer macht was?*
  - Verantwortliche Personen, Abteilungen oder andere Einheiten und Ressourcen für die festgelegten Aktivitäten.
- *Wie können die Resultate verifiziert und überprüft werden?*
  - Verifikationsplan
    - Zeitpunkt der Verifikation,
    - Einzelheiten zu den Personen, Abteilungen oder Einheiten, die die Verifikation ausführen müssen,
    - Verifikationsstrategien und Verifikationstechniken,
    - Testeinrichtungen,
    - Verifikationsaktivitäten,
    - Akzeptanzkriterien,
    - verwendete Mittel zur Bewertung der Verifikationsergebnisse.

  - Validierungsplan
    - Zeitpunkt der Validierung,
    - Betriebsarten der Maschine (z. B. Normalbetrieb, Einrichten),
    - Anforderungen der SCS bzw. SRP/CS, die zu prüfen bzw. zu validieren sind,
    - technische Validierungsstrategien (Tests),
    - Akzeptanzkriterien,
    - auszuführende Aktionen bei Nichterreichen der Akzeptanzkriterien.
- *Wie werden Änderungen verfolgt?*
  - Konfigurationsmanagement, Modifikation.

    Festgelegt wird also eine Strategie für ein Konfigurationsmanagement unter Berücksichtigung der relevanten organisatorischen Aspekte. Dazu gehören z. B. autorisierte Personen und interne Strukturen der Organisation.

All diese Informationen liegen bereits heute beim Hersteller von Maschinen vor.

Mit dem Plan der Funktionalen Sicherheit soll letztendlich die Vorgehensweise bis zur endgültigen Lösung strukturiert dokumentiert werden.

Damit stellt eine mögliche Nachweispflicht kein Problem dar.

Validierung und Verifikation werden bereits heute schon in der DIN EN ISO 13849-2 gefordert und stellen für den Anwender der EN 954-1 nichts Neues dar.

Das Konfigurationsmanagement ist insofern wichtig, weil Änderungen nicht mehr „unbemerkt“ gemacht werden können, und somit auch nicht mehr undokumentiert bleiben. Insbesondere bei der Erstellung und Verwaltung der Anwendersoftware ist diese Systematik zwingend notwendig geworden.

Fazit

Wer bisher die EN 954-1 korrekt verwendet hatte, der findet sich von allein im Plan der Funktionalen Sicherheit wieder: Das Kind hat einen Namen bekommen und orientiert sich an allen Aktivitäten, die in jedem erfolgreichen Projekt notwendig sind. Aus Alt mach Neu wäre die richtige Umschreibung.

6.3 Bestimmung der erforderlichen Sicherheitsintegrität

Den Risikograph der EN 954-1 hatte jeder irgendwie im Kopf, dieses harmonisch wirkende Bild (und so schön symmetrisch aufgebaut) hatte man doch lieb gewonnen. Gleichwohl wurde geflucht und geschimpft: Was ist denn nun „selten bis weniger häufig" oder „häufig bis dauernd" und warum nur zwei Schweregrade für das Schadensausmaß? Es gleicht einer Hassliebe – bis heute noch. Und zugleich sind das die stärksten Kritikpunkte des so sympathisch wirkenden Risikographen.

Dieser zerrissenen Beziehung trägt die DIN EN IEC 62061 (**VDE 0113-50**) Rechnung und versucht einen gewagten und doch charmanten Ansatz: Alle Risikoelemente der Risikoeinschätzung werden verwendet und genauer präzisiert. Ein wichtiger Schritt, damit die geforderte Sicherheitsintegrität ermittelt werden kann!

Das größte Manko dieses gewollt symmetrisierten Risikographens (**Bild 6.3**) sind die folgenden Kritikpunkte:

1. Warum nur S1 und S2? Nach RAPEX sind S1 bis S4, also vier Stufen empfohlen.
2. F1 und F2 bieten nicht die notwendige Flexibilität und sind somit nicht mehr zeitgemäß.
3. Wo ist denn der Parameter der Eintrittswahrscheinlichkeit geblieben? Eine Worst-Case-Betrachtung darf nicht vorgeschrieben werden.

Ganz anders geht die DIN EN IEC 62061 (**VDE 0113-50**) das Problem an (**Bild 6.4**).

Entscheiden Sie selbst, was Ihnen am ehesten liegt. Meine Gesprächspartner haben mir sehr oft gesagt, dass dieser Ansatz bevorzugt wird, weil Menschen im Team sehr wohl mit dieser feingranularen Aufteilung zurechtkommen – wichtig ist eine abgestimmte Einstufung des Risikos, das nachweisbar und nachvollziehbar dokumentiert wird.

Skurril wird es nur dann, wenn die Einstufung gemäß der Tabelle in Bild 6.4 gemacht wird und die Anwendung dann nach DIN EN ISO 13849-1 erfolgt. Da beide Methoden, als Tabelle oder Risikograph, nur *informativ* sein können, mögen die Normenexperten Nachsicht mit den Anwendern haben – er sucht nur nach einem Ausweg aus seiner misslichen Lage.

Risikoelemente:

S Schwere der Verletzung
S1 leichte
(üblicherweise reversible Verletzung)
S2 ernste
(üblicherweise irreversible Verletzung
einschließlich Tod)

F Häufigkeit und/oder Dauer der Gefährdungsexposition
F1 selten bis weniger häufig und/oder die Zeit der Gefährdungsexposition ist kurz
F2 häufig bis dauernd und/oder die Zeit der Gefährdungsexposition ist lang

P Möglichkeit zur Vermeidung der Gefährdung oder Begrenzung des Schadens
P1 möglich unter bestimmten Bedingungen
P2 kaum möglich

O Eintrittswahrscheinlichkeit
O1 gering
O2 hoch

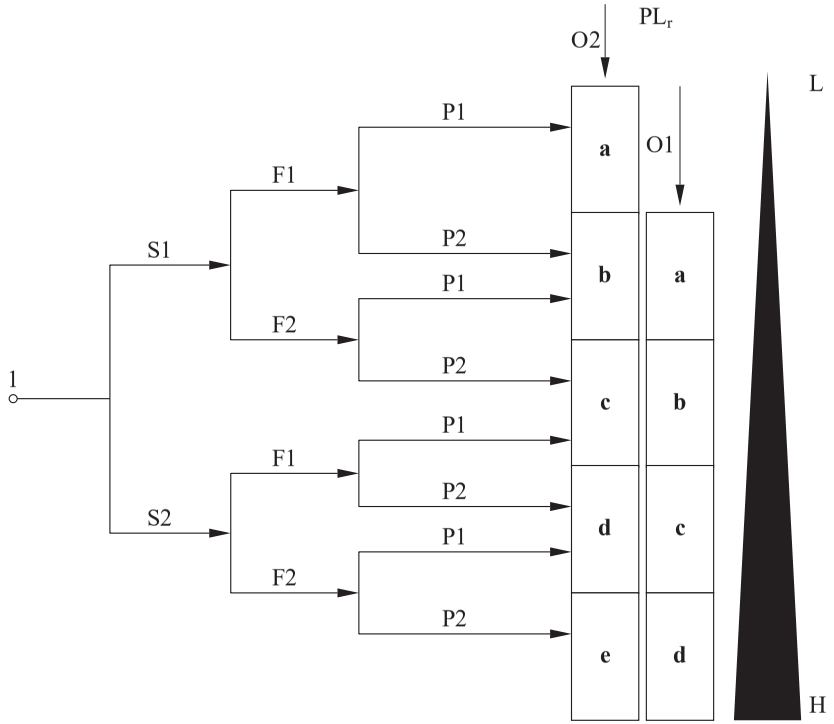

Bild 6.3 Die Ermittlung des geforderten PL gemäß DIN EN ISO 13849-1 – Lücken im System

SIL-Zuweisung (Anhang A der DIN EN IEC 62061 (VDE 0113-50))

Folgen	Schwere *Se*	Klasse *Kl* = *Fr* + *Pr* + *Av*												
		3	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*	*12*	*13*	*14*	*15*
Tod, Verlust eines Auges oder Arms	*4*	**SIL 1**		**SIL 2**			**SIL 2**			**SIL 3**			**SIL 3**	
		PL_r b	PL_r c	PL_r d			PL_r d			PL_r e			PL_r e	
dauerhafte Verletzung, Finger verlieren	*3*			**AM**			**SIL 1**			**SIL 2**			**SIL 3**	
				PL_r a			PL_r b		PL_r c	PL_r d			PL_r e	
reversible Verletzung, medizinische Versorgung	*2*	kein SIL (oder PL) erforderlich					**AM**			**SIL 1**			**SIL 2**	
							PL_r a			PL_r b		PL_r c	PL_r d	
reversible Verletzung, Erste Hilfe	*1*									**AM**			**SIL 1**	
										PL_r a			PL_r b	
AM: andere Maßnahmen (z. B. grundlegende Sicherheitsprinzipien)														

Folgen	Schadensausmaß *Se*
irreversible: Tod, Verlust eines Auges oder Arms	4
irreversible: gebrochene Extremität(en), Verlust eines Fingers (von Fingern)	3
reversibel: erfordert Versorgung durch einen Arzt	2
reversibel: benötigt Erste Hilfe	1

Häufigkeit und Dauer der Exposition (*Fr*)			Wahrscheinlichkeit des Eintritts	Wahrscheinlichkeit *Pr*	Möglichkeit zur Vermeidung oder Begrenzung eines Schadens *Av*	
Häufigkeit der Exposition	Häufigkeit, *Fr*: Dauer der Exposition ≥10 min	Häufigkeit, *Fr*: Dauer der Exposition <10 min				
≥1 pro Stunde	5	5	sehr hoch	5	unmöglich	5
<1 pro Stunde bis ≥1 pro Tag	5	4	wahrscheinlich	4		
<1 pro Tag bis ≥1 pro 2 Wochen	4	3	möglich	3	selten	3
<1 pro 2 Wochen bis ≥1 pro Jahr	3	2	selten	2		
<1 pro Jahr	2	1	vernachlässigbar	1	wahrscheinlich	1

Bild 6.4 Die Ermittlung des geforderten SIL gemäß DIN EN IEC 62061 (**VDE 0113-50**)

Hinweis

„Informativ“ sind meistens Anhänge, die keinen normativen und somit verbindlichen Charakter (im Sinne von Anforderungen) haben, sondern lediglich eine Hilfestellung anbieten wollen. Leider wird seitens der Anwender der Norm oft kein Unterschied gemacht und diese Hilfestellung als quasi verbindlich eingestuft, mangels Alternativen.

Vielleicht sollte bei der Überarbeitung der Norm dieses Bedürfnis an Freiheitsgrad ernst genommen, aufgegriffen und in der Norm verankert werden: Etwas praktikable Hilfe ist nicht verkehrt für den Anwender der Normen und kann z. B. auch nur informativ in einem Anhang platziert werden.

6.4 Spezifikation der Sicherheitsanforderungen

Was wollen wir denn wie erreichen?

Bei der Spezifikation jeder Sicherheitsfunktion sind zwei grundlegende Aspekte zu betrachten:

- die Spezifikation der funktionalen Anforderungen und
- die Spezifikation der Anforderungen zur *Sicherheitsintegrität*, umgangssprachlich auch „Performance“ oder Leistungsfähigkeit genannt.

Diese müssen in der Spezifikation der Sicherheitsanforderungen (SRS, en: safety requirement specification) dokumentiert werden.

Funktionale Anforderungen

Die nachfolgenden Tabellen zeigen die typischen Merkmale, die beschrieben werden sollten, damit die Sicherheitsfunktion funktional (als Zielsetzung oder Schutzziel) verstanden wird, bevor die Suche nach einer technischen Lösung beginnt.

Typische Merkmale sind zum Beispiel

Spezifikation der funktionalen Anforderungen an die Sicherheitsfunktion	
Beschreibung	Wenn … dann … (Ursache/Wirkung)
Bedingung(en)	Betriebsarten
Neustart/Zurücksetzen	manuelle menschliche Eingriffe sind erforderlich, wenn …
Priorität	hohe Priorität im Vergleich zu anderen Sicherheitsfunktionen; die Not-Halt-Funktion wird die höchste Priorität haben
Häufigkeit des Betriebs	*X* mal pro Stunde; *Y* Stunden pro Tag; *Z* Tage pro Jahr
Reaktionszeit	max. 500 ms vom Auslöseereignis (Öffnen der Schutztür) bis zur elektrischen Reaktion …
Schnittstelle(n) zu anderen Maschinenfunktionen	… Informationen zur Verwendung des Komponentenherstellers sind zu referenzieren
Fehler-Reaktionsfunktion	sofortiger Stopp oder Erkennung beim erneuten Start zumindest durch Verhinderung des Wiederanlaufs.
Manipulation/Umgehung	Entwurf der Schutztür und Einbau von Verriegelungseinrichtungen nach DIN EN ISO 14119
Umgebung	Temperatur, Staub, Vibrationen, …
Spezifikation der Anforderungen an die Sicherheitsintegrität der Sicherheitsfunktion	
geforderter SIL oder PL_r	SIL 2 mit zugehörigem Zielwert *PFH*
Architektur Einschränkungen	Verwendung von … Schutzverriegelungen (Positionsschalter) wegen Vibrationen keine Typ-C-Normanforderungen (z. B. geforderte *HFT*)

Tabelle 6.2 Funktionale Beschreibung

Anforderungen zur Sicherheitsintegrität

Mit dieser Sicherheitsintegrität soll sichergestellt werden, dass die notwendig geforderte Risikominderung erreicht werden kann. Diese Einstufung ist hierarchisch zu sehen, ebenso wie der Performance Level PL nach DIN EN ISO 13849-1. Das macht die Sache etwas greifbarer (**Tabelle 6.3**).

Sicherheitsintegritätslevel (SIL)	**Wahrscheinlichkeit eines Gefahr bringenden Ausfalls pro Stunde (*PFH*)**	**Performance Level (PL)**
1	$10^{-6} \leq PFH < 10^{-5}$	PL b / PL c
2	$10^{-7} \leq PFH < 10^{-6}$	PL d
3	$10^{-8} \leq PFH < 10^{-7}$	PL e

Tabelle 6.3 SIL, PL und Wahrscheinlichkeiten Gefahr bringender Ausfälle

*DIN EN IEC 62061 (**VDE 113-50**) verwendet PFH anstelle von PFH_D* (kommt aus dem Englischen und bedeutet „Probability of Failures per Hour, Dangerous“).

Diese statistischen Grenzwerte (Probabilistik) kann man sich bildhaft wie folgt vorstellen:

- **SIL 1, ein möglicher Ausfall innerhalb von ca. 10 Jahren;**
- **SIL 2, ein möglicher Ausfall innerhalb von ca. 100 Jahren;**
- **SIL 3, ein möglicher Ausfall innerhalb von ca. 1 000 Jahren.**

Anmerkung: Das Jahr hat 365 mal 24 Stunden, also 8 760 Stunden und somit ungefähr 10 000 Stunden, oder $1 \cdot 10^4$ in wissenschaftlicher Schreibweise.

Ebenfalls anzumerken bleibt noch: Wenn die erforderliche Sicherheitsintegrität einer sicherheitsbezogenen Steuerungsfunktion kleiner als SIL 1 ist, dann müssen mindestens die Anforderungen von Kategorie B nach DIN EN ISO 13849-1 erfüllt werden.

Im Lichte der Funktionalen Sicherheit ist auch immer die DIN EN 60204-1 (**VDE 0113-1**) zu beachten. Wenn die Anforderungen geringer als SIL 1 sind, dann treibt nur noch z. B. die DIN EN 60204-1 (**VDE 0113-1**) den Entwurf des elektrischen Steuerungssystems.

Unter Sicherheitsintegrität versteht man aber nicht nur diese statistischen Werte zur Bewertung der Wahrscheinlichkeiten (quantitativen Betrachtungen), sondern auch den qualitativen Entwurf, der sich in den Strukturen und der Systematik widerspiegelt.

Leider wird oft nur das Thema Wahrscheinlichkeit in den Vordergrund gestellt. Dabei sind der strukturelle Ansatz und die gesamte systematische Integrität weitaus wichtiger einzustufen: Hier werden die meisten Fehler gemacht.

Hinweis

Was hilft eine bis in die Nachkommastellen errechnete Lösung, wenn, bezogen auf die Applikation, die falschen Komponenten verwendet werden? Nichts. Leider wird diesen Zahlen mitunter mehr Wert beigemessen als der Auswahl der richtigen Komponenten, also der „systematischen Integrität“.

In der Normensprache wird die Sicherheitsintegrität folgendermaßen umschrieben:

- Sicherheitsintegrität der Hardware, d. h., Architektureinschränkungen (Fehlertoleranz) und Wahrscheinlichkeit zufälliger Gefahr bringender Hardwareausfälle;
- *Systematische Integrität*, d. h., Anforderungen zur Vermeidung und Beherrschung systematischer Fehler.

Systematische Fehler sind grundlegende Entwicklungsfehler, Auswahl falscher Komponenten und Fehler in der Software. Alle Fehler sind nicht nur mit Wahrscheinlichkeiten zu betrachten, sondern haben ihren Ursprung in der Methodik und dem Qualitätssystem: Kontrolle statt Vertrauen ist die einzige Antwort darauf. Diese „verdeckten", nicht aufgespürten Fehler führen irgendwann zu einem Ausfall der Lösung. Daher wird heutzutage auf diesen systematischen Aspekten seitens der Behörden und seitens der Zulassung vermehrt Wert gelegt. Im Grunde ist diese Thematik vergleichbar mit der ISO 9001 – ein gut funktionierendes Managementsystem!

CCF und systematische Ausfälle

Systematische Ausfälle müssen berücksichtigt werden: Bei dem Entwurf eines SCS oder SRP/CS sind diese möglichen Ausfälle insbesondere zu betrachten.

Gefährlicher Ausfall und CCF führen zu einem Ausfall des Teilsystems

Die systematische Integrität wird mathematisch mit dem Faktor Beta β berücksichtigt.

Die Wahrscheinlichkeit eines Ausfalls aufgrund von einer gemeinsamen Ursache wird mit den Werten 10 %, 5 %, 2 % oder 1 % beziffert, besser gesagt angenommen. Welcher Wert der richtige ist, bleibt das Geheimnis jedes Konstrukteurs.

Wenn ich zwei unterschiedliche Technologien verwende, z. B. Elektromechanik und Elektronik, dann kann 1 % angenommen werden. Bei gleicher Technologie hängt es von der Überdimensionierung ab. Zum Beispiel zwei Leistungsschütze mit max. 50 % Belastung können ein β = 2 % rechtfertigen.

Wer pfiffig ist, rechnet zunächst alles mit 10 %, um einer Diskussion aus dem Weg zu gehen. Sollten die *PFH*-Werte reichen, dann erst recht.

Aber nichtsdestotrotz wird auch mit Recht verlangt, dass CCF nicht einfach mal so schnell bewertet wird, sondern dass Mindestanforderungen zu betrachten sind.

„Tue Gutes und denke systemisch dabei."

Gefährlicher Ausfall aufgrund einer Wahrscheinlichkeit (zufälliger Hardwareausfall) und aufgrund eines systematischen Fehlers: Beide können zum Ausfall eines Teilsystems oder Teilsystem-Elements führen.

Auf Ebene des SCS (als Summe aller Teilsysteme)
Vermeiden, damit nicht im Nachhinein Beherrschen –
wehret den Anfängen.

Die wichtigsten Aspekte dabei sind:

- Verwendung des SCS innerhalb der Spezifikation des Herstellers (falls ein SCS vollständig erworben wird und eine Sicherheitsfunktion abbildet),
- die richtige Auswahl, Kombination, Anordnung, Montage und Installation von Teilsystemen,
- Anwendung der DIN EN 60204-1 (**VDE 0113-1**),
- Betriebsarten müssen dokumentiert sein,
- Betrachtungen des vorhersehbaren Missbrauchs, der Umweltveränderungen oder jeglicher Modifikation(en),
- Verdrahtung von Teilsystemen (ein- oder zweikanalig) – das kann spezielle Fehlerbetrachtungen und Fehlerausschlüsse zur Folge haben,
- Herstelleranweisungen (einschließlich z. B. Anwendungsbeispiele) beider miteinander verbundenen Teilsysteme.

Zusätzlich kann gelten:

- SCS Hardware Design Review (z. B. durch Inspektion oder Begehung), zwecks Aufdeckung von Diskrepanzen zwischen der Spezifikation und der Implementierung
- ggf. Simulation oder Analyse: Durchführung einer systematischen und vollständigen Simulation eines SCS-Entwurfs (Dimensionierung und Interaktion der Teilsysteme).

Auf Ebene des SCS (als Summe aller Teilsysteme)
Beherrschen, wenn Vermeiden nicht möglich ist.

Die wichtigsten Aspekte dabei sind:

- Verwendung der Energieabschaltung des SCS, sodass sicherer Zustand der Maschine erreicht oder aufrechterhalten wird,
- Maßnahmen zur Beherrschung der Auswirkungen vorübergehender Ausfälle des Teilsystems, wie z. B. Energieversorgungsschwankungen oder Auswirkungen elektromagnetischer Interferenzen,
- Maßnahmen zur Beherrschung der Auswirkungen von Fehlern aufgrund von Datenübertragungsverfahren,
- Betrachtungen von gefährlichen Fehlern an einer Schnittstelle eines Teilsystems (insbesondere bei einkanaligen Strukturen oder zweikanaligen, die aber einkanalig werden können).

EMV ist tückisch und kann zu einem systematischen Ausfall führen

Das SCS muss die geltenden Anforderungen der DIN EN 61000-1-2 (**VDE 0839-1-2**) erfüllen, dabei sind die entsprechenden Störfestigkeitspegel für industrielle Umgebungen in DIN EN 61326-3-1 (**VDE 0843-20-3-1**) oder DIN EN 61000-6-7 (**VDE 0839-6-7**) angegeben.

Bei Teilsystemen, die nach einer sicherheitsbezogenen Produktnorm entworfen wurden, z. B. nach DIN EN IEC 61496-1 (**VDE 0113-201**) usw., oder nach DIN EN 61326-3-1 (**VDE 0843-20-3-1**) oder DIN EN 61000-6-7 (**VDE 0839-6-7**), kann es möglich sein, dass mit dem Teilsystem Informationen geliefert werden, die die Verifizierung der Anforderungen auf Systemebene des SCS durch Analyse erleichtern können.

Somit ist die Anwendung von Produkten nach Herstellerangabe, als Teilsystem-Elemente oder Teilsysteme, ein wichtiger Faktor, der eine Gesamtbewertung durch Analyse erlaubt, und nicht zwangsläufig zu umfangreichen EMV-Tests führen muss, was für eine Maschine, je nach Ausdehnung, oder Aufstellungsort quasi unmöglich sein kann.

Maßnahmen zur Reduzierung von EMV-Einflüssen:

- ✓ Die Installation von Überspannungsschutzgeräten und/oder Filtern für Geräte.
- ✓ Leitende Ummantelungen (z. B. Armierungen, Abschirmungen) von Kabeln sollten mit dem Schutzleiter System verbunden sein.
- ✓ Induktionsschleifen vermeiden durch die Wahl gemeinsamer Wege für die Verdrahtung von Leistungs-, Signal- und Datenleitungen unter Beibehaltung der Trennung der Stromkreise.
- ✓ Energiekabel sollen von Signal- oder Datenleitungen getrennt verlegt werden.
- ✓ Wo es notwendig ist, dass sich Leistungs- und Signal- oder Datenleitungen kreuzen, sollten diese rechtwinklig gekreuzt werden Verwendung von Leitungen mit konzentrischen Leitern zur Verringerung der in den Schutzleiter induzierten Ströme.
- ✓ Verwendung von symmetrischen mehradrigen Leitungen (z. B. abgeschirmte Leitungen mit getrennten Schutzleitern) für die elektrischen Verbindungen zwischen Motoren und Umrichtern.
- ✓ Wenn geschirmte Signal- oder Datenkabel verwendet werden, sollte darauf geachtet werden, dass der Stromfluss durch die Schirme von Signal- oder Datenkabeln, die geerdet sind, reduziert wird. Es kann erforderlich sein, einen Bypass-Leiter zu installieren.

Zusammenfassend können die Vermeidung und Beherrschung von Fehlern bzw. Ausfällen wie in **Tabelle 6.4** dargestellt werden.

Vermeidung von systematischen Fehlern	
Maßnahme	**Anmerkung/Beispiele**
richtige Auswahl, Kombination, Anordnung, Montage	Die richtige Komponente für die Anwendung und in der richtigen Form verwendet (Benutzerinformation des Komponentenherstellers): Für diese Anwendung Positionsschalter verwendbar?
Verkabelung, Verbindungen	Siehe Benutzerinformation des Komponentenherstellers; Maßnahmen gegen Kurzschlussausfälle
korrekte Dimensionierung und Formgebung	Elektrische Überdimensionierung: Belastung der Schütze korrekt?
Überprüfung des HW-Entwurfs	Plausibilitätsanalyse und Berücksichtigung der Benutzerinformation des Komponentenherstellers
Beherrschung von systematischen Fehlern	
Maßnahme	**Anmerkung/Beispiele**
Spannungsschwankungen und Unterbrechungen	Hardwareentwurf gemäß DIN EN 60204-1 (**VDE 0113-1**)
Auswirkungen der physikalischen Umgebung und der EM-Störfestigkeit	Hardwareentwurf gemäß DIN EN 60204-1 (**VDE 0113-1**); siehe Benutzerinformation des Komponentenherstellers
Auswirkungen von Temperaturanstieg oder -abfall	Siehe Benutzerinformation des Komponentenherstellers; ggf. einschließlich relevanter Hinweise für die Verwendungsinformationen der Sicherheitsfunktion
Verwendung der Stromabschaltung	Abschalten des Motors durch Betätigen der Positionsschalter
bewährte Sicherheitsprinzipien	
• Fehlererkennung durch automatische Tests,	Überwachung von zwei Positionsschaltern und zwei Schützen; Kurzschlusserkennung
• Betrieb im Positiv-Modus,	Zwangsgeführte Kontakte der Positionsschalter
• mechanisch verbundene Kontakte	Schütze mit Spiegelkontakten

Tabelle 6.4 Systematische Fehler

Historisch

Die EN 954-1 hat international zugunsten der ISO 13849-1:2006 Platz gemacht. 2005 bereits erschien die IEC 62061:2005 als Anwendernorm der IEC 61508:1999.

Die probabilistischen Betrachtungen der ISO 13849-1 sind aus dem europäischen Projekt „European Project STSARCES – Standards for Safety Related Complex Electronic Systems, Annex 6“, im Jahr 2001 hervorgegangen.

Hinweis

Die ISO 13849-1 muss sich den Vorwurf gefallen lassen, dass das im Anhang K hinterlegte Markov-Modell, das in dem europäischen Projekt seine Wurzeln hat, nicht offengelegt wurde. Ferner trifft dieses Modell die Annahme, dass alle Komponenten in die Modellierung eingebunden werden. Werden jedoch bereits vorgeprüfte Komponenten verwendet, z. B. Sicherheitsschaltgeräte, dann ist dies nicht berücksichtigt worden.