# 5 Die Anwendernorm DIN EN 62061 (VDE 0113-50) aus Sicht der Anwender

Sicherheit von Maschinen – Funktionale Sicherheit sicherheitsbezogener elektrischer, elektronischer und programmierbarer elektronischer Steuerungssysteme.

## 5.1 Welche Norm ist anzuwenden: DIN EN ISO 13849-1 oder DIN EN 62061 (VDE 0113-50)?

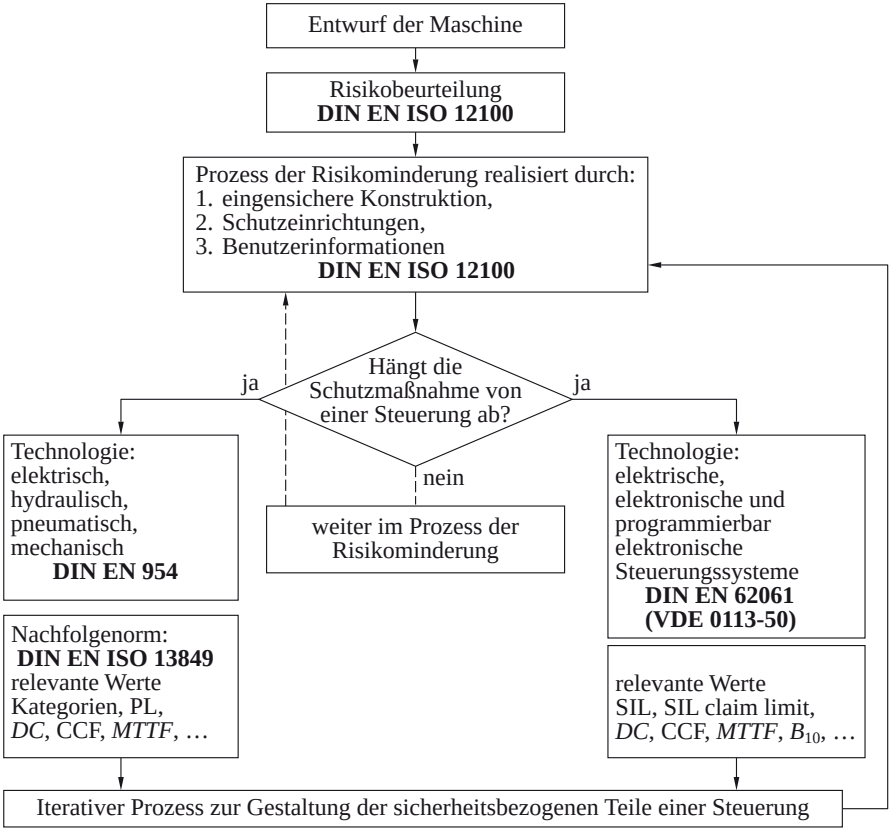


**Bild 5.1** Funktionale Sicherheit – zwei Normen

Und? 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 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 62061 (**VDE 0113-50**) sehr wohl auch für andere Technologien verwendbar sind – der Anwendungsbereich verdeutlicht dies (**Bild 5.2**).

„ …
– legt keine Anforderungen für die Leistungsfähigkeit von nicht elektrischen (z. B. hydraulischen, pneumatischen) Steuerungselementen für Maschinen fest;

Anmerkung 4 Obwohl die Anforderungen in dieser Norm spezifisch für elektrische Steuerungssysteme sind, kann der festgelegte Rahmen und die Methodologie für sicherheitsbezogene Teile von Steuerungssystemen anwendbar sein, die andere Technologien verwenden. …“

**Bild 5.2** Anwendungsbereich der DIN EN 62061 (**VDE 0113-50**)

Lassen Sie uns die in **Tabelle 5.1** gezeigte Gegenüberstellung machen und entscheiden Sie selbst, wie wichtig der Begriff der „Kategorien“ ist.

| **DIN EN ISO 13849-1** | **DIN EN 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 5.1** 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.

## 5.2 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 SRECS, 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 SRECS (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 SRECS, 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.

## 5.3 Bestimmung des erforderlichen Sicherheitsintegritätslevels SIL

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 Risikographens.

Dieser zerrissenen Beziehung trägt die DIN EN 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!

| **Schwere der Verletzung** | **S** | **Häufigkeit/ Aufenthaltsdauer** | **F** | **Möglichkeit zur Vermeidung** | **P** |
|---|---|---|---|---|---|
| irreversible Verletzung | S2 | häufig bis dauernd/ lang | F2 | kaum möglich | P2 |
| reversible Verletzung | S1 | selten bis öfter/kurz | F1 | möglich | P1 |

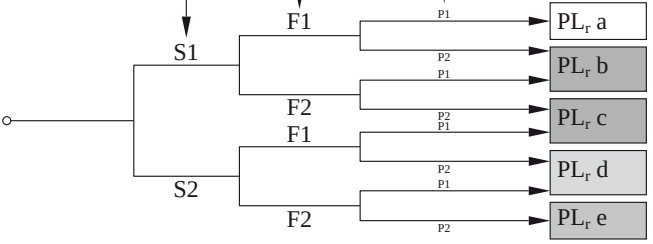


**Bild 5.3** Der Risikograph gemäß DIN EN ISO 13849-1 – Lücken im System

Das größte Manko dieses gewollt symmetrisierten Risikographens (**Bild 5.3**) 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 62061 (**VDE 0113-50**) das Problem an (**Bild 5.4**).