Funktionale Sicherheit mit EN ISO 13849-1 und EN/IEC 62061 realisieren

pilz

Risikobeurteilung und Risikominderung

Risikobeurteilung
nach EN ISO 14121

Folgende Versionen der Normen wurden zitiert:

EN ISO 12100-1	2003
EN ISO 12100-2	2003
EN ISO 13849-1	2008
EN ISO 14121-1	2007
EN/IEC 62061	2005

START

Risikoanalyse
nach EN ISO 14121

Festlegung der Grenzen der Maschine
räumlich, zeitlich, Umgebungsbedingung, Verwendung
EN ISO 14121-1 Kap. 5
EN ISO 12100-1 Kap. 5.2

Identifizierung der Gefährdungen
für alle Lebensphasen und Betriebsarten
EN ISO 14121-1 Kap. 6 und A
EN ISO 12100-1 Kap. 4 und 5.3

Für jedes Risiko separat

Risikoeinschätzung
Schwere, Vermeidbarkeit, Häufigkeit, Dauer
EN ISO 14121-1 Kap. 7
EN/IEC 62061 Anhang A
EN ISO 13849-1 Anhang A (Risikograph)

Risikobewertung
gemäß C-Normen oder Risikoeinschätzung
EN ISO 14121-1 Kap. 8

Wurde das Risiko hinreichend vermindert? — Ja → **ENDE**

Nein

Maßnahmen unabhängig voneinander und nacheinander bewerten

Risikominderung
nach EN ISO 12100-1 Kap. 5.4 +5.5

Kann die Gefährdung **beseitigt** werden? — Ja → Risikominderung durch **inhärent sichere Konstruktion** (EN ISO 12100-2 Kap. 4) → Ist die vorgesehene Risikominimierung erreicht? — Ja

Nein → Kann das Risiko durch **inhärent sichere Konstruktion** vermindert werden? — Ja → Risikominderung durch **inhärent sichere Konstruktion**

Nein → Kann das Risiko durch **trennende und andere Schutzeinrichtungen** vermindert werden? — Ja → Risikominderung durch **technische Schutzmaßnahme** Einbeziehung **ergänzender Schutzmaßnahme** (EN ISO 12100-2 Kap. 5) → Ist die vorgesehene Risikominimierung erreicht? — Ja

Nein → Können die **Grenzen erneut festgelegt** werden? — Nein → Risikominderung durch **Benutzerinformation** (EN ISO 12100-2 Kap. 6) → Ist die vorgesehene Risikominimierung erreicht? — Nein → Ja

Nein → Wurden andere Gefährdungen erzeugt? — Ja → Ja

Realisierung Sicherheitsfunktion SRCF/SRP/CS
EN ISO 13849-1/EN/IEC 62061

EN ISO 13849-1

Einsetzbar für elektrische/elektronische/ programmierbar elektronische/hydraulische/ pneumatische/mechanische Systeme

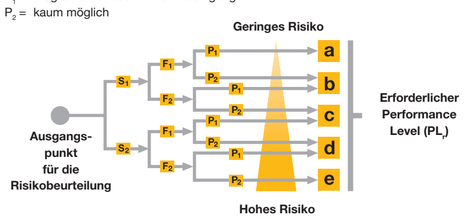
EN/IEC 62061

Einsetzbar für elektrische/elektronische/ programmierbar elektronische Systeme

Risikoeinschätzung

Bestimmung des erforderlichen Performance Levels (PL_r)

- **S – Schwere der Verletzung**
  S_1 = leichte Verletzung (normalerweise reversibel)
  S_2 = schwere Verletzung, einschließlich Tod (normalerweise irreversibel)
- **F – Häufigkeit und/oder Dauer der Gefährdungsexposition**
  F_1 = selten bis öfters und/oder kurze Dauer
  F_2 = häufig bis dauernd und/oder lange Dauer
- **P – Möglichkeiten zur Vermeidung der Gefährdung**
  P_1 = möglich unter bestimmten Bedingungen
  P_2 = kaum möglich



Bestimmung des erforderlichen Safety Integrity Levels (SIL)

Häufigkeit und Dauer	F > 10 Min	F ≤ 10 Min
≤ 1 Std.	5	5
> 1 Std. – ≤ 1 Tag	5	4
> 1 Tag – ≤ 2 Wo.	4	3
> 2 Wo. – ≤ 1 Jahr	3	2
> 1 Jahr	2	1

Wahrscheinlichkeit gef. Ereignis	W
häufig	5
wahrscheinlich	4
möglich	3
selten	2
vernachlässigbar	1

Vermeidung	P
unmöglich	5
möglich	3
wahrscheinlich	1

Auswirkungen und Schwere	S	Klasse K = F+W+P 3-4	5-7	8-10	11-13	14-15
Tod, Verlust eines Auges oder Armes	4	SIL 2	SIL 2	SIL 2	SIL 3	SIL 3
permanent, Verlust von Fingern	3		AM	SIL 1	SIL 2	SIL 3
reversibel, medizinische Behandlung	2			AM	SIL 1	SIL 2
reversibel, Erste Hilfe	1				AM	SIL 1

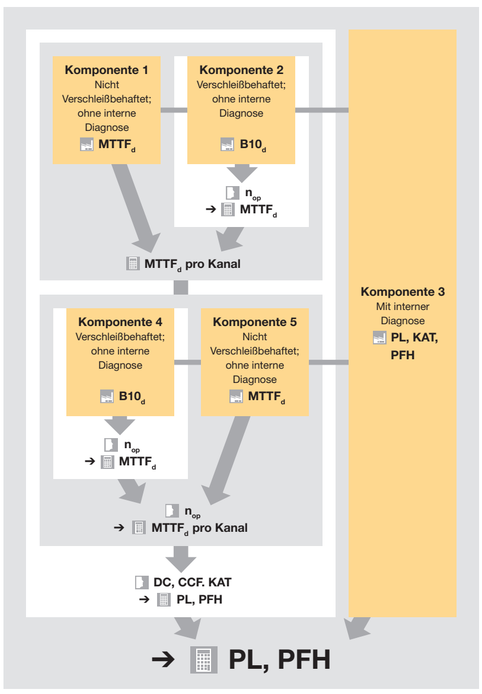
AM = andere Maßnahmen empfohlen

Bewertung der Sicherheitsfunktion

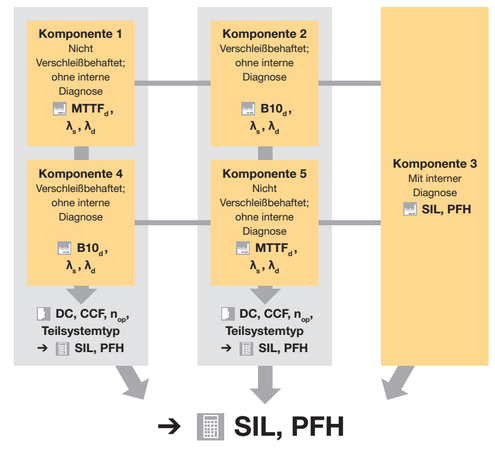
Erforderliche Sicherheitskenndaten

EN ISO 13849-1		Gerätetyp			EN/IEC 62061	
PL Kategorie T1	-	**Geräte mit interner Diagnose**		Sicherheitssteuerung, Sicherheits-schaltgeräte	PFH SIL T1	-
$MTTF_d$	DC, CCF, Kategorie	**Geräte ohne interne Diagnose**	**Ohne** verschleißbehaftete Komponenten	Sensoren	$MTTF_d$ λ_d λ_s	DC, CCF, Teilsystemtyp
$B10_d$	DC, CCF, Kategorie, n_{op}		**Mit** verschleißbehafteten Komponenten	NOT-AUS, Relais, Schalter	$B10_d$ λ_d λ_s	DC, CCF, Teilsystemtyp, n_{op}

Berechnung EN ISO 13849-1

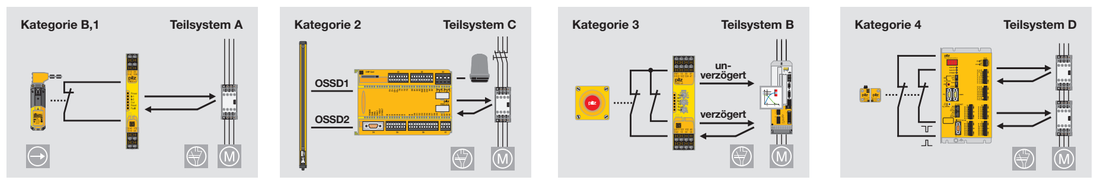


Berechnung EN/IEC 62061



Berechnung erfolgt gemäß Grafik von Innen nach Außen mit Quelle der Daten:
- Daten vom Hersteller
- Daten aus der Anwendung
- Berechnung laut Norm

Spezifikation der Kategorien /Teilsystemtypen



Verifikation der Sicherheitsfunktion

Wahrscheinlichkeit eines gefahrbringenden Ausfalls pro Stunde – Vergleich PL/SIL

Performance Level (PL) nach EN ISO 13849-1	Wahrscheinlichkeit eines gefahrbringenden Ausfalls pro Stunde [1/h]	Safety Integrity Level (SIL) nach EN/IEC 62061
a	$10^{-5} \le PFH < 10^{-4}$	keine spezielle Sicherheitsanforderung
b	$3 \times 10^{-6} \le PFH < 10^{-5}$	1 (1 Versagen in 100000 h)
c	$10^{-6} \le PFH < 3 \times 10^{-6}$	
d	$10^{-7} \le PFH < 10^{-6}$	2 (1 Versagen in 1000000 h)
e	$10^{-8} \le PFH < 10^{-7}$	3 (1 Versagen in 10000000 h)

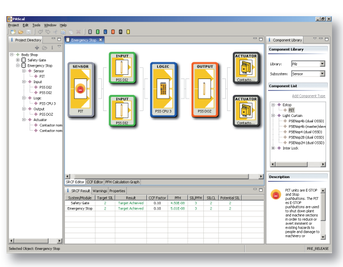
erreichter PL ≥ PL_r? — **erreichter SIL ≥ erforderlicher SIL?**

Lexikon

- **B_{10d}**
  Lebenszeit von Produkten bis 10 % des Produktspektrums „gefährlich" ausfallen
- **β**
  Beta-Faktor bzw. Common Cause-Faktor; Maß für den CCF; Anteil von Ausfällen, die eine gemeinsame Ursache haben
- **Bestimmungsgemäße Verwendung einer Maschine**
  Verwendung einer Maschine in Übereinstimmung mit den in der Benutzerinformation bereitgestellten Informationen
- **CCF**
  Ausfall infolge gemeinsamer Ursache
- **Diagnosedeckungsgrad (DC)**
  Maß für die Wirksamkeit der Diagnose, der bestimmt werden kann als Verhältnis der Ausfallrate der bemerkten gefährlichen Ausfälle und der Ausfallrate der gesamten gefährlichen Ausfälle
- **DC_{avg}**
  Durchschnittlicher Diagnosedeckungsgrad
- **Diagnose-Testintervall**
  Zeitraum zwischen Online-Prüfungen, um Fehler in einem sicherheitsbezogenen System mit spezifiziertem Diagnosedeckungsgrad zu entdecken
- **Diversität**
  Ungleichartige Mittel zur Ausführung einer geforderten Funktion
- **d_{op}**
  Mittlere Betriebszeit in Tagen je Jahr
- **Fehler**
  Zustand einer Einheit charakterisiert durch die Unfähigkeit, eine geforderte Funktion auszuführen, ausgenommen der Unfähigkeit während vorbeugender Wartung oder anderer geplanter Handlungen, oder aufgrund des Fehlens externer Mittel
- **Gebrauchsdauer (T_M)**
  Zeitraum, der die vorgegebene Verwendung der SRP/CS abdeckt
- **h_{op}**
  Mittlere Betriebszeit in Stunden je Tag
- **Kategorie (KAT)**
  Einstufung der sicherheitsbezogenen Teile einer Steuerung bezüglich ihres Widerstandes gegen Fehler und ihres nachfolgenden Verhaltens bei einem Fehler, das erreicht wird durch die Struktur der Anordnung der Teile, die Fehlererkennung und/oder ihre Zuverlässigkeit
- **λ**
  Durchschnittliche Wahrscheinlichkeit eines Ausfalls
- **λ_D**
  Rate gefährlicher Ausfälle
- **λ_S**
  Rate sicherer Ausfälle
- **$MTTF_d$**
  Mittlere Zeit bis zum gefährlichen Ausfall
- **n_{op}**
  Mittlere Betätigungshäufigkeit pro Jahr
- **PAScal**
  Berechnungssoftware zur Verifikation funktionaler Sicherheit
- **Performance Level (PL)**
  Diskreter Level, der die Fähigkeit von sicherheitsbezogenen Teilen einer Steuerung spezifiziert, eine Sicherheitsfunktion unter vorhersehbaren Bedingungen auszuführen
- **Performance Level, erforderlicher (PL_r)**
  Performance Level (PL), um die erforderliche Risikominderung für eine Sicherheitsfunktion zu erreichen
- **$PFH = PFH_d$**
  Wahrscheinlichkeit eines gefährlichen Ausfalls pro Stunde bei kontinuierlicher Nutzung
- **Redundanz**
  Vorhandensein von mehr als den notwendigen Mitteln, damit eine Funktionseinheit eine geforderte Funktion ausführt oder damit Daten eine Information darstellen können
- **Restrisiko**
  Verbleibendes Risiko nachdem Schutzmaßnahmen ergriffen wurden
- **Risiko**
  Kombination der Wahrscheinlichkeit des Eintritts eines Schadens und seines Schadensausmaßes
- **Risikoanalyse**
  Kombination aus Festlegung der Grenzen der Maschine, Identifizierung der Gefährdung und Risikoeinschätzung
- **Risikobeurteilung**
  Gesamtheit des Verfahrens, das eine Risikoanalyse und Risikobewertung umfasst
- **Risikobewertung**
  Auf der Risikoanalyse beruhende Beurteilung, ob die Ziele zur Risikominderung erreicht wurden
- **Sicherheitsfunktion**
  Funktion einer Maschine, wobei ein Ausfall der Funktion zur unmittelbaren Erhöhung des Risikos (der Risiken) führen kann
- **Sicherheitsintegrität**
  Wahrscheinlichkeit, dass ein sicherheitsbezogenes System die geforderten Sicherheitsfunktionen unter allen festgelegten Bedingungen innerhalb eines festgelegten Zeitraumes anforderungsgemäß ausführt
- **Safety Integrity Level (SIL)**
  Diskrete Stufe (eine von vier möglichen) zur Spezifizierung der Sicherheitsintegrität der Sicherheitsfunktionen, die dem E/E/PE-System zugeordnet werden, wobei der SIL 3 (SIL 4 in der Prozessindustrie) die höchste Stufe und der SIL 1 die niedrigste ist
- **SIL-Anspruchsgrenze (SILCL)**
  Maximaler SIL der für ein SRECS-Teilsystem in Bezug auf strukturelle Einschränkungen und systematische Sicherheitsintegrität beansprucht werden kann
- **SRCF – Sicherheitsbezogene Steuerungsfunktion**
  Von einem SRECS ausgeführte Steuerungsfunktion mit einem festgelegten Integritätslevel, die dazu vorgesehen ist, den sicheren Zustand der Maschine aufrechtzuerhalten oder einen unmittelbaren Anstieg des Risikos zu verhindern.
- **SRECS**
  Elektrisches Steuerungssystem an einer Maschine, dessen Ausfall zu einer unmittelbaren Erhöhung des Risikos führt
- **SRP/CS – Sicherheitsbezogenes Teil einer Steuerung**
  Teil einer Steuerung, das auf sicherheitsbezogene Eingangssignale reagiert und sicherheitsbezogene Ausgangssignale erzeugt
- **Teilsystem**
  Einheit des Architekturentwurfs des SRECS auf oberster Ebene, wobei ein Ausfall irgendeines Teilsystems zu einem Ausfall der sicherheitsbezogenen Steuerungsfunktion führt
- **T_1**
  (→ Wiederholungsprüfung)
- **T_M**
  (→ Gebrauchsdauer)
- **t_{Zyklus}**
  Mittlere Zeit zwischen dem Beginn zweier aufeinander folgenden Zyklen des Bauteils (z. B. Schalten eines Ventils) in Sekunden je Zyklus
- **Validierung**
  Bestätigen aufgrund einer Untersuchung und durch Bereitstellung eines Nachweises, dass die besonderen Anforderungen für eine spezielle beabsichtigte Verwendung erfüllt worden sind
- **Verifikation**
  Bestätigen aufgrund einer Untersuchung und durch Bereitstellung eines Nachweises, dass die Anforderungen erfüllt worden sind
- **Wahrscheinlichkeit eines gefahrbringenden Ausfalls pro Stunde**
  (→ PFH)
- **Wiederholungsprüfung (T_1)**
  Wiederkehrende Prüfung zur Aufdeckung von Ausfällen in einem sicherheitsbezogenen System, so dass nötigenfalls das System in einen „Wie-Neu"-Zustand gebracht oder so nah wie unter praktischen Gesichtspunkten möglich an diesen Zustand herangebracht werden kann. Technisch ist eine Wiederholungsprüfung für die meisten Geräte nicht realisierbar

Die hier beschriebenen Maßnahmen stellen eine Vereinfachung dar und dienen zur Übersicht der beiden Normen EN ISO 13849-1 und EN/IEC 62061. Für eine Validierung von Steuerkreisen sind die Kenntnis und korrekte Anwendung der einschlägigen Normen und Richtlinien erforderlich. Für die Vollständigkeit der Angaben können wir daher keine Haftung übernehmen.

Safety Calculator PAScal – Berechnungssoftware zur Verifikation funktionaler Sicherheit



Der Safety Calculator PAScal berechnet den PFH_D-Wert von Sicherheitsfunktionen in Maschinen und Anlagen. Das Ergebnis wird mit dem vorgegebenen Performance Level (PL) nach EN ISO 13849 bzw. Safety Integrity Level (SIL) nach EN/IEC 62061 verifiziert. Durch die grafische Darstellung erkennen Sie den Einfluss der einzelnen Komponenten auf die Gesamtsicherheit.

Ihre Vorteile:
- Zeitersparnis durch einfache Handhabung
- umfangreiche Komponenten-Datenbank
- einfache Import- und Updatefunktion
- Reportgenerator als Dokumentationsnachweis

Aktuelle Version herunterladen:

www.pilz.com Webcode 0971

Internationale Hotline +49 711 3409-444