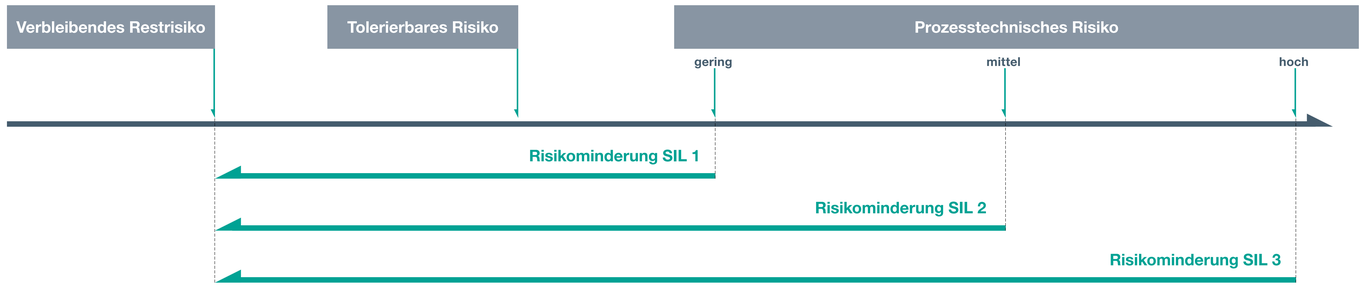
Funktionale Sicherheit in der Prozessindustrie

www.pepperl-fuchs.com/functional-safety

Risikobasierter Ansatz



Möglichkeiten zur Gerätequalifikation
Herstellererklärung
Betriebsbewährung
Fehleraussschluss
Baumusterprüfung
Vollständige Diagnose

Phasen des Sicherheitslebenszyklus

Bestimmung der erforderlichen Risikominderung

Management und Beurteilung der funktionalen Sicherheit und Audits

Aufbau und Planung des Sicherheitslebenszyklus

Gefährdungs- und Risikobeurteilung

Zuordnung der Sicherheitsfunktionen zu Schutzebenen

Spezifikation der Sicherheitsanforderungen an die PLT-Schutzeinrichtung

Realisierung der Risikominderung

Entwurf und Planung der PLT-Schutzeinrichtung

Entwurf und Planung anderer Maßnahmen zur Risikoreduzierung

Montage, Inbetriebnahme und Validierung

Betrieb und Instandhaltung

Änderung

Außerbetriebsetzung

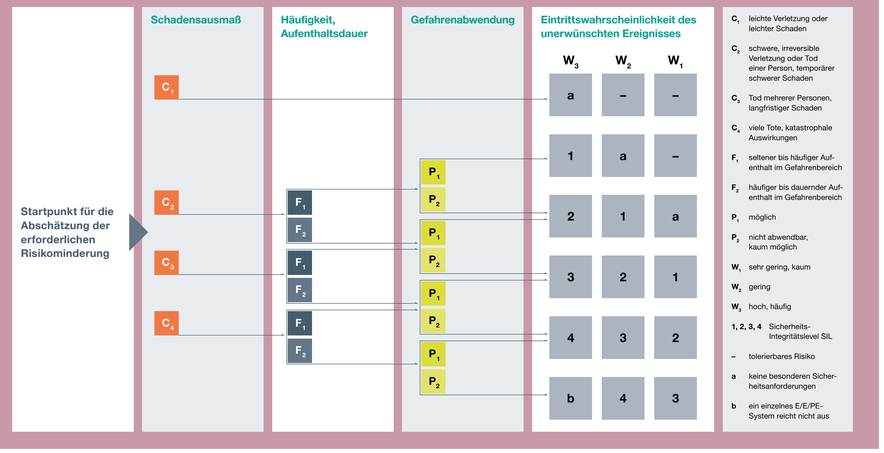
Verifikation

Gefahrenquellen identifizieren

HAZOP/PAAG (IEC 61882)

Leitwort	Bedeutung
Nein (nicht/kein/keine)	Vollständige Verneinung des Entwurfsziels
Mehr	Quantitative Zunahme
Weniger	Quantitative Abnahme
Sowohl als auch	Qualitative Änderung/Zunahme
Teilweise	Qualitative Änderung/Abnahme
Umkehrung	Sinngemäßer Gegensatz zum Entwurfsziel
Anders als	Vollständiger Austausch/Ersatz
Zu früh	Relativ zur Uhrzeit
Zu spät	Relativ zur Uhrzeit
Davor	Relativ zur Reihenfolge oder zum Ablauf
Danach	Relativ zur Reihenfolge oder zum Ablauf

Erforderliche Risikominderung quantifizieren



SIL IEC/EN 61508 → IEC/EN 61511 → VDI/VDE 2180

Anforderungen an den Entwurf

Mindest-Hardware-Fehlertoleranz (HFT) abhängig vom SIL

SIL	HFT
SIL 1 – Jede Betriebsart	0
SIL 2 – Betriebsart mit niedriger Anforderung	0
SIL 2 – Betrieb mit hoher/kontinuierlicher Anforderung	1
SIL 3 – Jede Betriebsart	1
SIL 4 – Jede Betriebsart	2

Hinweis: Geräte müssen nachweislich für die Anwendung geeignet sein.

Ausfallwahrscheinlichkeit pro Stunde bei hoher Anforderungsrate (> 1 Anforderung pro Jahr)

SIL	PFH [1/h]	Max. akzeptierter Ausfall des SIS
SIL 1	≥ 10^{-6} bis < 10^{-5}	max. 1 gefährlicher Ausfall pro 100 000 Stunden
SIL 2	≥ 10^{-7} bis < 10^{-6}	max. 1 gefährlicher Ausfall pro 1 000 000 Stunden
SIL 3	≥ 10^{-8} bis < 10^{-7}	max. 1 gefährlicher Ausfall pro 10 000 000 Stunden
SIL 4	≥ 10^{-9} bis < 10^{-8}	max. 1 gefährlicher Ausfall pro 100 000 000 Stunden

Ausfallwahrscheinlichkeit bei niedriger Anforderungsrate (≤ 1 Anforderung pro Jahr)

SIL	PFD	Max. akzeptierter Ausfall des SIS
SIL 1	≥ 10^{-2} bis < 10^{-1}	max. 1 gefährlicher Ausfall pro 10 Anforderungen
SIL 2	≥ 10^{-3} bis < 10^{-2}	max. 1 gefährlicher Ausfall pro 100 Anforderungen
SIL 3	≥ 10^{-4} bis < 10^{-3}	max. 1 gefährlicher Ausfall pro 1000 Anforderungen
SIL 4	≥ 10^{-5} bis < 10^{-4}	max. 1 gefährlicher Ausfall pro 10 000 Anforderungen

Realisierung

HFT	Zuverlässigkeitsblockdiagramm	Anlagensicherheit	Anlagenverfügbarkeit	PFD (nach VDI/VDE 2180)
0	A	o	o	$\lambda_{du} \cdot \frac{T_1}{2}$
0	2oo2 (A, B)	-	+	$\lambda_{du} \cdot T_1$
1	1oo2 (A, B)	+	-	$\frac{\lambda_{du}^2 \cdot T_1^2}{3} + \beta \cdot \lambda_{du} \cdot \frac{T_1}{2}$
1	2oo3 (A, B, C)	+	+	$\lambda_{du}^2 \cdot T_1^2 + \beta \cdot \lambda_{du} \cdot \frac{T_1}{2}$
2	1oo3 (A, B, C)	++	-	$\frac{\lambda_{du}^3 \cdot T_1^3}{4} + \beta \cdot \lambda_{du} \cdot \frac{T_1}{2}$

β: 0.15

Glossar

Betriebsbewährt	Eine Komponente ist betriebsbewährt, wenn eine entsprechend dokumentierte Untersuchung ergeben hat, dass Nachweise aus früheren Einsätzen belegen, dass die Komponente für den Einsatz in einem sicherheitstechnischen System geeignet ist.
BCPS – Basic Process Control System (Betriebs- und Überwachungseinrichtungen)	System, das auf Eingangssignale vom Prozess und seinen zugehörigen technischen Einrichtungen, von anderen programmierbaren Systemen und/oder von einem Bediener antwortet und Ausgangssignale erzeugt, die den Prozess und seine zugehörigen technischen Einrichtungen in der gewünschten Weise steuern.
CCF – Common Cause Failure (Ausfall infolge gemeinsamer Ursache)	Ausfall, der das Ergebnis eines oder mehrerer Ereignisse ist, die Ausfälle von 2 oder mehreren getrennten Kanälen in einem mehrkanaligen System verursachen und zu einem Systemausfall führen.
EUC – Equipment Under Control (gesteuerte Einrichtung)	Einrichtung, Maschine, Apparat oder Anlage, die zur Fertigung, Stoffumformung, zum Transport, zu medizinischen oder anderen Tätigkeiten verwendet wird.
Fehlertoleranz	Fähigkeit einer Funktionseinheit, eine geforderte Funktion bei Bestehen von Fehlern oder Abweichungen weiter auszuführen.
Funktionale Sicherheit	Teil der Gesamtsicherheit, der sich auf den Prozess und das BPCS bezieht und der von der bestimmungsgemäßen Funktion des SIS und anderer Sicherheitsebenen abhängt.
Gefahrbringender Ausfall	Ausfall mit dem Potenzial, das sicherheitstechnische System in einen gefahrbringenden oder funktionsunfähigen Zustand zu versetzen.
Lambda du (λ_{du})	Rate der gefahrbringenden unerkannten Ausfälle (pro Stunde) eines Kanals in einem Teilsystem.
MooN-System ("M out of N")	Sicherheitstechnisches System oder Teil davon, das aus „N" unabhängigen Kanälen besteht, die derart miteinander verbunden sind, dass jeweils „M" Kanäle genügen, um die sicherheitstechnische Funktion auszuführen.
Notwendige Risikominderung	Risikominderung, um sicherzustellen, dass das vertretbare Risiko (Grenzrisiko) nicht überschritten wird.
PFD – Probability of Failure on Demand (Wahrscheinlichkeit eines gefahrbringenden Ausfalls im Anforderungsfall)	Sicherheitsbezogene Nichtverfügbarkeit eines sicherheitsbezogenen E/E/PE-Systems, die festgelegte Sicherheitsfunktion auszuführen, wenn von der EUC oder dem EUC-Leit- oder Steuerungssystem eine Anforderung erfolgt.
PFH – Probability of Failure per Hour (Mittlere Häufigkeit eines gefahrbringenden Ausfalls je Stunde)	Mittlere Häufigkeit eines gefahrbringenden Ausfalls eines sicherheitsbezogenen E/E/PE-Systems, die festgelegte Sicherheitsfunktion über einen gegebenen Zeitraum auszuführen.
PLT-Schutzeinrichtung	PLT-Einrichtung, die das Erreichen eines unzulässigen Fehlbereichs durch einen selbsttätigen Eingriff in den Prozess verhindert oder das Bedienpersonal durch eine Meldung zum Eingreifen veranlasst.
Prozessrisiko	Risiko, das sich aus Prozesszuständen ergibt, die durch außergewöhnliche Ereignisse verursacht werden (einschließlich Fehlfunktionen des BPCS).
Risiko	Kombination der Wahrscheinlichkeit des Auftretens eines Schadens und des Schweregrads dieses Schadens.
SFF – Safe Failure Fraction (Anteil sicherer Ausfälle)	Anteil der Gesamtausfallrate für zufällige Ausfälle eines Geräts, die entweder einen ungefährlichen Ausfall oder einen erkannten gefahrbringenden Ausfall zur Folge haben.
Sicherheitshandbuch	Handbuch, das die sichere Anwendung eines Geräts, Teilsystems oder Systems beschreibt.
Sicherheitslebenszyklus	Notwendige Tätigkeiten im Rahmen der Realisierung von sicherheitstechnischen Funktionen während eines Zeitraums, der mit der Konzeptphase eines Projekts beginnt und endet, wenn alle sicherheitstechnischen Funktionen nicht mehr für die Verwendung verfügbar sind.
Sicherheitstechnische Funktion beim High/ Continuous Demand Mode	Funktion für Fälle, in denen bei Ausfall der sicherheitstechnischen Funktion eine mögliche Gefährdung ohne einen weiteren Ausfall eintritt, wenn keine Maßnahme zu ihrer Verhinderung ergriffen wird.
Sicherheitstechnische Funktion in Anforderungsbetriebsarten	Funktion für Fälle, in denen die festgelegte Handlung (z. B. das Schließen eines Ventils) als Antwort auf Prozesszustände oder andere Anforderungen eingeleitet wird. Im Fall eines gefahrbringenden Ausfalls der sicherheitstechnischen Funktion tritt eine mögliche Gefährdung nur im Fall eines Ausfalls des Prozesses oder der BPCS ein.
SIF – Sicherheitstechnische Funktion	Funktion, die von einer oder mehreren Schutzebenen ausgeführt wird, mit dem Ziel, unter Berücksichtigung eines festgelegten gefährlichen Ereignisses einen sicheren Zustand für den Prozess zu erreichen oder aufrecht zu erhalten.
SIL – Sicherheits-Integritätslevel	Eine von 4 diskreten Stufen zur Spezifikation der Anforderungen für die Sicherheitsintegrität der sicherheitstechnischen Funktionen, die dem sicherheitstechnischen System zugeordnet werden, wobei der Sicherheits-Integritätslevel 4 den höchsten Grad der Sicherheitsintegrität, der Sicherheits-Integritätslevel 1 den niedrigsten darstellt.
SIS – Sicherheitstechnisches System	Sicherheitstechnisches System zur Ausführung einer oder mehrerer sicherheitstechnischer Funktionen. Ein SIS besteht aus einem oder mehr Sensoren, Aktoren und einem Logiksystem.
Spezifikation der Sicherheitsanforderung	Spezifikation, die alle Anforderungen an die sicherheitstechnischen Funktionen beinhaltet, die vom sicherheitstechnischen System auszuführen sind.
Schutzebene	Jede unabhängige Maßnahme, die das Risiko durch Regelung oder Steuerung, Schutz- oder Schadensbegrenzungsmaßnahmen vermindert.
Systematischer Ausfall	Systematisches Versagen/Ausfall, bei dem eindeutig auf eine Ursache geschlossen werden kann, die nur durch eine Modifikation des Entwurfs oder des Fertigungsprozesses, der Art und Weise des Betreibens, der Betriebsanleitung oder anderer Einflussfaktoren beseitigt werden kann.
Tolerierbares Risiko	Risiko, das in einem gegebenen Kontext basierend auf den gültigen Wertvorstellungen der Gesellschaft akzeptiert wird.
Ungefährlicher Ausfall	Ausfall ohne das Potenzial, das sicherheitstechnische System in einen gefahrbringenden oder funktionsunfähigen Zustand zu versetzen.
Wiederholungsprüfung	Prüfung zur Aufdeckung verdeckter Fehler in einem sicherheitstechnischen System, so dass das System, wenn nötig, wieder in den Zustand gebracht werden kann, in dem es seine geplante Funktion erfüllt.
Zufälliger Ausfall	Ausfall, der zu einem zufälligen Zeitpunkt auftritt und der aus einem oder mehreren möglichen Mechanismen in der Hardware resultiert, die zu einer Verschlechterung der Eigenschaften von Bauteilen führen.

Your automation, our passion.

PEPPERL+FUCHS