SIEMENS

Funktionale Sicherheit

Funktionale Sicherheit in der Prozessinstrumentierung mit Einstufung SIL

Fragen, Beispiele, Hintergründe

siemens.de/prozessinstrumentierung

Inhalt

Vorwort

Seit dem Inkrafttreten der IEC 61508 ist das Thema "Funktionale Sicherheit" in der Prozessindustrie sehr stark in den Vordergrund getreten. Oftmals wird nur der Ausdruck SIL verwendet. Was aber genau ist eigentlich SIL?

In dieser Broschüre möchten wir einen ersten Überblick über das Thema geben - und das ganz mit dem Schwerpunkt der Instrumentierung für die Prozesstechnik. Wir möchten das grundlegende Verständnis darstellen und dabei nicht zu sehr die Normensprache benutzen. Für den Experten mögen daher manche Beschreibungen möglicherweise zu ungenau oder zu oberflächlich erscheinen

Diese Broschüre kann nur eine Einleitung in das Thema sein.

Wer genauere Informationen benötigt, sollte sich mit entsprechender Literatur und den einschlägigen Normen auseinandersetzen. Die hier gezeigten Berechnungsbeispiele sind daher nur als prinzipielles Vorgehen zu verstehen und können nicht für "echte" Berechnungen herangezogen werden.

Die Angaben in dieser Broschüre wurden nach bestem Wissen zusammengestellt. Trotzdem können sich dabei Fehler eingeschlichen haben. Eine sich daraus abzulei-tende Verantwortung wird daher nicht übernommen.

Gefahren und Risiken

Im täglichen Leben sind wir ständig den verschiedensten Gefahren ausgesetzt. Die Bandbreite dieser Gefahren reicht bis hin zu schweren Katastrophen, die schwere Schäden an Gesundheit und Umwelt zur Folge haben können. Nicht immer haben wir die Möglichkeit, einer Gefahr und den damit verbundenen Risiken aus dem Wege zu gehen. So lebt beispielsweise eine hohe Anzahl der Weltbevölkerung mit den Gefahren von Erdbeben oder Überschwemmungen. Schutzmaßnahmen gegen die Ereignisse gibt es nicht; Schutzmaßnahmen für die drohenden Folgen von solchen Ereignissen allerdings schon (z. B. Dämme und Deiche oder erdbebensichere Gebäude).

Definition von Risiko

Risiko =
Wahrscheinlichkeit des Eintritts eines gefährlichen Ereignisses X
Konsequenzen (Kosten) eines gefährlichen Ereignisses.

Das akzeptierte Restrisiko ist von folgenden Faktoren abhängig:

- Region/Land
- Gesellschaft der jeweiligen Region / Land
- Gesetze
- Kosten

Dieses akzeptierte Restrisiko muss individuell eingeschätzt werden. Was für den Einen akzeptabel ist, ist für den Anderen bereits inakzeptabel.

Risikoreduzierung

Somit werden im Alltag viele Gefahren nach ihrem Risiko beurteilt und entsprechend akzeptiert - oder nicht akzeptiert. Plant jemand eine weite Strecke zurückzulegen, kann er durch gezielte Auswahl des Verkehrsmittels das Risiko eines Unfalls beeinflussen. Der Reisende kann die Gefahr auf ein für ihn akzeptables Restrisiko reduzieren. Es verbleibt jedoch immer ein Restrisiko.

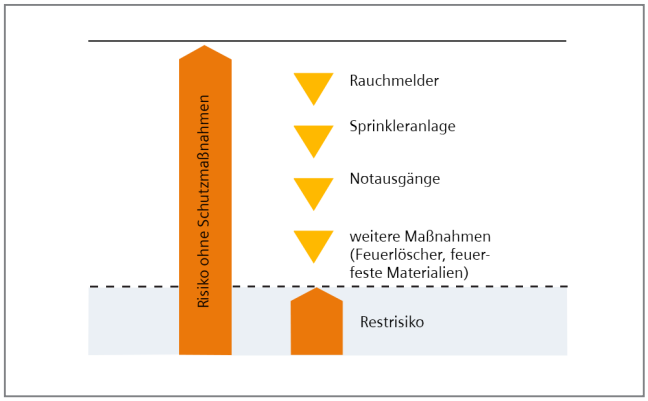
Schutzmaßnahmen

Wir können uns durch Reduzierung der Eintrittswahrscheinlichkeit einer Gefahr oder durch Begrenzung ihrer Auswirkung schützen.

In unserer mehr und mehr technisch dominierten Welt haben wir die Möglichkeit, Gefahren mit elektronischen Systemen zu erkennen und Risiken für Mensch und Umwelt zu reduzieren.

Ein einfaches Beispiel

Um das Schadensrisiko eines Brandes zu reduzieren, können in einem Gebäude verschiedene Schutzmaßnahmen getroffen werden.

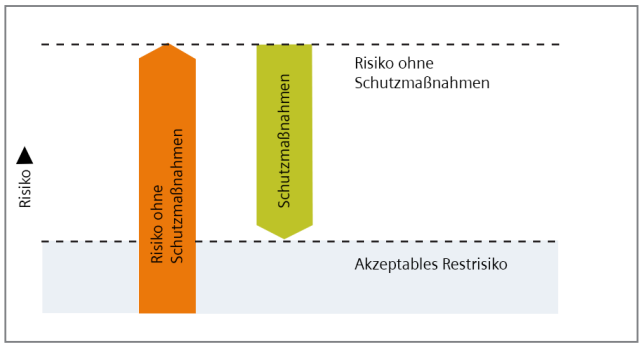


So können bereits beim Entwurf des Gebäudes entsprechende Notausgänge und Fluchtwege vorgesehen werden. Rauchsensoren können einen Alarm auslösen, der den inner- und außerhalb des Gebäudes befindlichen Personen eine Gefahrenmeldung signalisiert. Der Einbau von Brandabschlusstüren und die Verwendung von feuerfesten Materialien verhindert ein weiteres Ausbreiten eines Brandes.

Automatische Sprinkleranlagen bekämpfen die Flammen, Feuerlöscher stehen ebenfalls zur Brandbekämpfung bereit. Dieses Beispiel zeigt, dass es eine Vielzahl an Möglichkeiten der Risikoreduzierung gibt. Dabei werden die Schutzmaßnahmen den jeweiligen Anforderungen angepasst, denn eine Lagerhalle hat andere Risiken als ein Wohngebäude.

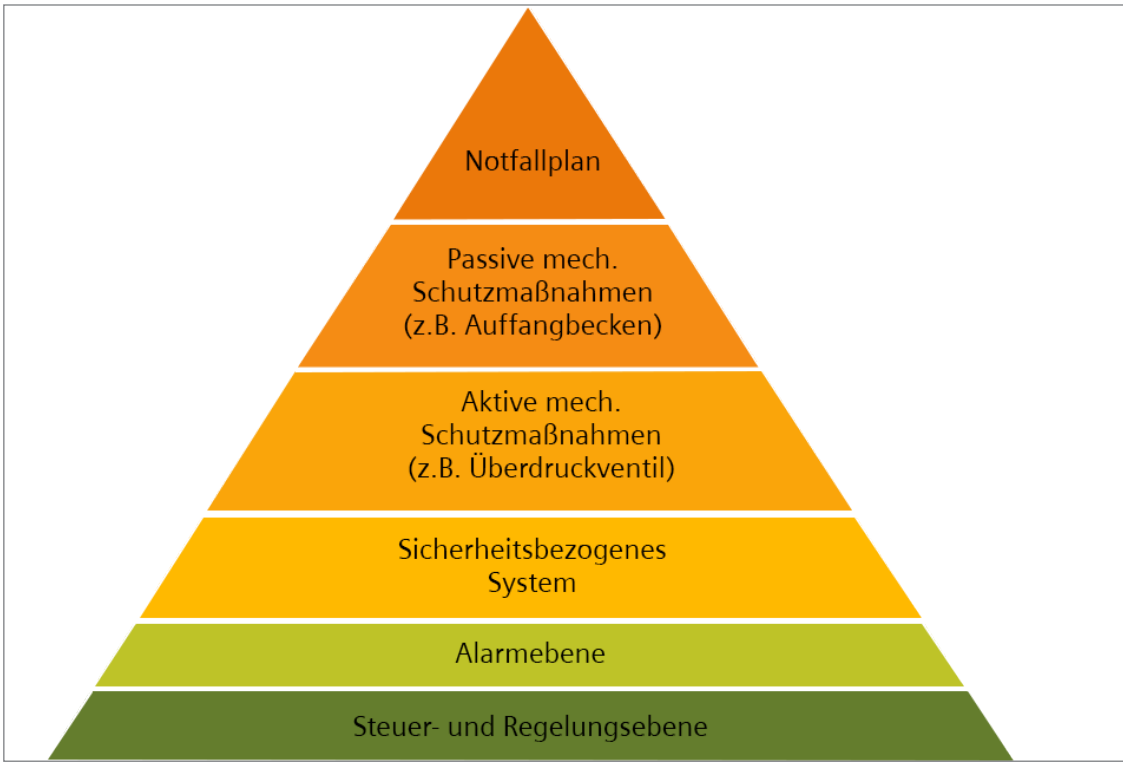
Schutzmaßnahmen in der Industrie

In der Industrie gibt es sehr viele Maschinen und Anlagen, die unterschiedliche Gefahrenpotenziale besitzen. Um Mensch und Umwelt, aber auch die Maschinen und Anlagen vor Schäden zu schützen, werden Risiken ermittelt und anschließend mit geeigneten Schutzmaßnahmen reduziert.



Darstellung der Risikoreduzierung

Welche Arten von Schutzmaßnahmen typischerweise existieren und in welcher Reihenfolge sie einzuordnen sind, ist aus dem rechts abgebildeten Ebenenmodel ersichtlich:



Maßnahmen, um ein Risiko zu reduzieren, können teilweise sehr einfach - aber auch sehr komplex sein.

Beispiele:

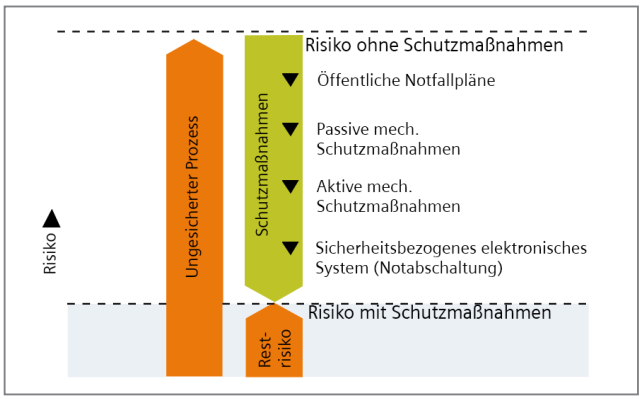
- Bauliche Maßnahmen (z. B. Betonmauern um Produktionsanlagen bauen)
- Gefahrenverteilung
- Evakuierungspläne
- Sicherheitsgerichtete Steuerungs- und Schutzeinrichtungen
- ...und viele andere mehr

Wie aus diesen Beispielen zu ersehen ist, sind Maßnahmen, die das Risiko verringern, teilweise völlig unterschiedlichen Ansätzen zuzuordnen. Diese Ansätze werden auch als Schutzebenen bezeichnet. Diese Schutzebenen sind hierarchisch aufgebaut und jeweils unabhängig voneinander zu betrachten. Versagt eine Schutzebene, greift automatisch die nächst höhere Schutzebene zur Schadensbegrenzung oder Vermeidung ein.

Welche Arten von Schutzmaßnahmen typischerweise existieren und in welcher Reihenfolge sie einzuordnen sind, ist aus dem oben groß abgebildeten Ebenenmodel ersichtlich.

Die Schutzebenen sind in ihrer Funktion voneinander unabhängig. Daher dürfen Geräte für die Steuer- und Regelungstechnik aus der untersten Ebene in der Regel nicht gleichzeitig für Sicherheitsanwendungen einer übergeordneten Ebene verwendet werden.

Die gesamte Risikoreduzierung ergibt sich aus den Maßnahmen der einzelnen Schutzebenen und muss letztendlich ein akzeptables Restrisiko ergeben.



Welche Maßnahmen letztendlich ergriffen werden, hängt damit zusammen, wie hoch das noch akzeptierbare Restrisiko sein darf - und welcher Aufwand (auch finanzieller Art) dafür betrieben werden muss. Sicherheitsgerichtete Steuerungs- und Schutzeinrichtungen können dabei in Maschinen und Anlagen erheblich zur Risikoreduzierung beitragen.

Was bedeutet Funktionale Sicherheit?

Systeme der Automatisierungstechnik übernehmen immer mehr sicherheitsrelevante Aufgaben. So werden heute Prozesse, von denen eine Gefahr für Mensch und Umwelt ausgeht, von Sicherheitssystemen überwacht. Diese greifen im Störfall in den Prozess ein und können das Risiko eines gefährlichen Zustandes reduzieren. Die Funktionale Sicherheit ist das korrekte Funktionieren dieser Einrichtungen.

Bisher gab es nationale Standards für die Planung, den Bau und den Betrieb von sicherheitsbezogenen Systemen (SBS). So konnten sich beispielswiese für den deutschen Markt Hersteller und Betreiber solcher Anlagen auf die Sicherheitsnormen DIN/VDE 19250, DIN/VDE 19251 und DIN/VDE 801 beziehen.

Da viele Länder unterschiedliche Normen für das korrekte Funktionieren von sicherheitsgerichteten Einrichtungen hatten, wurde 1998 eine weltweit gültige IEC-Basisnorm für funktionale Sicherheit verabschiedet. Aus dieser heraus entstanden eine Reihe von Normen, in denen organisatorische und technische Anforderungen an sicherheitsbezogene Systeme und deren Umsetzung definiert wurden.

2003 wurde ein einheitlicher Standard für Anlagen in der Prozessindustrie verabschiedet. Für die Prozessinstrumentierung sind dabei folgende zwei Normen von Bedeutung:

- **IEC 61508** (Basisnorm):
  Gilt weltweit als Basis für Spezifikationen, Entwurf und Betrieb von sicherheitsbezogenen Systemen (SBS).
- **IEC 61511** (anwendungsspezifische Norm für Prozessindustrie): Umsetzung der IEC 61508 für die Prozessindustrie.

Internationale Normen für funktionale Sicherheit.

Sicherheitsbezogenes System (SBS)

Für wen ist die IEC 61508 relevant?

Anhand einer Gefährdungs- und Risikoanalyse können die Gefahren ermittelt werden, die von einer Anlagen und deren zugehörigen Steuerungssystemen ausgehen. Dadurch wird analysiert, ob funktionale Sicherheit erforderlich ist, um einen angemessenen Schutz gegen mögliche Gefährdungen zu gewährleisten. Sollte das der Fall sein, müssen die zugehörigen Konzepte in angemessener Art und Weise in die Entwicklung dieser Anlage mit einfließen.

Die IEC 61508 definiert angemessene Methoden, um funktionale Sicherheit für betroffenen Systeme zu erreichen.

Welche Systeme sind von der IEC 61508 betroffen?

Die IEC 61508 ist auf sicherheitsbezogene Systeme anzuwenden, wenn diese eine oder mehrere der folgende Geräte enthält:

- elektrische Geräte (E)
- elektronische Geräte (E)
- programmierbare elektronische Geräte (PE)

Die Norm betrachtet mögliche Risiken, die durch den Ausfall von Sicherheitsfunktionen verursacht werden. Nicht abgedeckt werden Gefährdungen durch die E/E/PE-Geräte selbst, wie z. B. elektrischer Schlag. Die Norm ist allgemein auf sicherheitsbezogene E/E/PE-Systeme anwendbar, unabhängig von der jeweiligen Applikation.

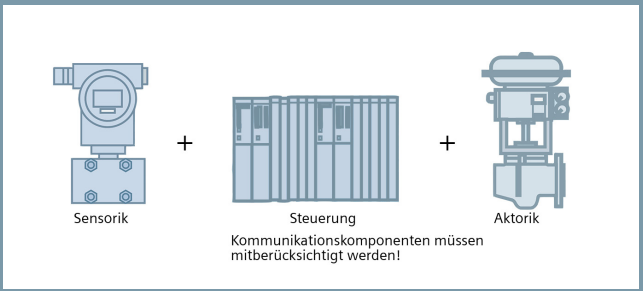
Sicherheitsbezogenes System (SBS)

Ein SBS wird eingesetzt, um einen gefährlichen Prozess abzusichern und das Risiko eines Unfalls zu reduzieren.

Prozessinstrumente sind Bestandteil eines sicherheitsbezogenen Systems . Dieses besteht aus den wesentlichen Komponenten einer gesamten sicherheitsrelevanten Prozesseinheit:

- Sensor
- fehlersichere Verarbeitungseinheit
- Aktor

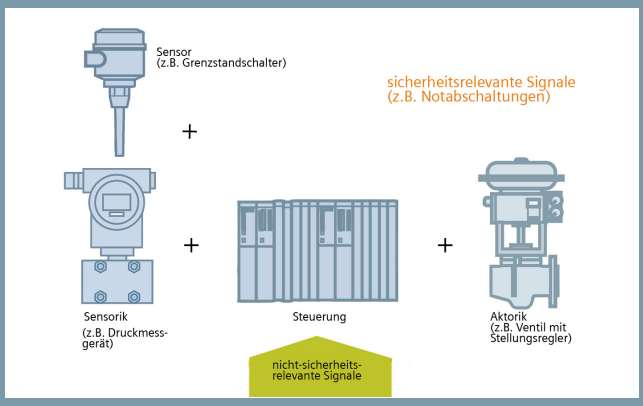
Alle Einheiten zusammen ergeben ein sicherheitsbezogenes System. Um ein SBS auf seine funktionale Sicherheit hin bewerten zu können, muss deshalb die gesamte Verarbeitungskette (vom Sensor bis zum Aktor) betrachtet werden.



Darstellung eines SBS

Innerhalb eines sicherheitsbezogenen Systems können mehrere Sensoren, Aktoren oder Steuerungskomponenten zum Einsatz kommen.

Innerhalb einer Anlage können unter Umständen sicherheits- und nicht-sicherheitsrelevante Komponenten miteinander verbunden sein. Für das SBS werden dabei nur die sicherheitsrelevanten Komponenten betrachtet.



In einer Anlage zu verarbeitende Signale

Ermittlung des erforderlichen SIL

Von Anlagen oder Anlagenteilen gehen unterschiedliche Risiken aus. Somit steigern sich mit zunehmendem Risiko auch die Anforderungen an die Fehlersicherheit des sicherheitsbezogenen Systems (SBS). Die Normen IEC 61508 und IEC 61511 definieren dabei vier unterschiedliche Sicherheitsstufen, welche die Maßnahmen zur Risikobeherrschung dieser Komponenten beschreiben. Diese vier Sicherheitsstufen sind die sogenannten **Safety Integrity Level - SIL.**

Je höher der Zahlenwert des Safety Integrity Level (SIL) ist, desto größer ist die Risikoreduzierung. Der SIL ist somit das Maß für die Wahrscheinlichkeit, dass das Sicherheitssystem die geforderten Sicherheitsfunktionen für einen bestimmten Zeitraum korrekt erfüllen kann.

Um den erforderlichen SIL einer Anlage oder eines Anlagenteiles zu ermitteln, gibt es unterschiedliche Ansätze. In den Normen IEC 61508 und IEC 61511 (Anwendung der IEC 61508 für die Prozessindustrie) sind zur Festlegung des SIL verschiedene Methoden aufgeführt. Da die Thematik sehr komplex ist, soll sie hier nur zum grundlegenden Verständnis aufgezeigt werden.

Eine quantitative Methode

Das Risiko eines gefährlichen Prozesses ist bestimmt durch die Wahrscheinlichkeit, mit der ein gefährlicher Vorfall (ohne vorhandene Schutzmaßnahmen) auftreten könnte, multipliziert mit der Auswirkung des gefährlichen Vorfalls. Es ist zu ermitteln, wie hoch die Wahrscheinlichkeit ist, die zu einem gefährlichen Zustand führen kann. Diese Wahrscheinlichkeit kann unter Anwendung quantitativer Risikobeurteilungsmethoden abgeschätzt werden und mit einen numerischen Grenzwert festgelegt werden.
Die Wahrscheinlichkeit kann bestimmt werden durch:

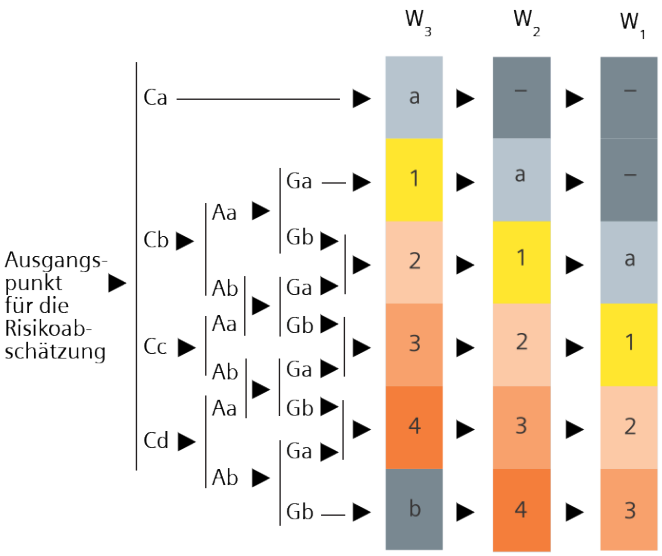
- Analyse der Ausfallraten in vergleichbaren Situationen
- Daten aus relevanten Datenbanken
- Berechnung mithilfe angemessener Vorhersagemethoden

Die genauen Berechnungsmethoden können hier nicht weiter behandelt werden und sind bei Bedarf in der IEC 61508 in Teil 5 näher beschrieben.

Eine qualitative Methode

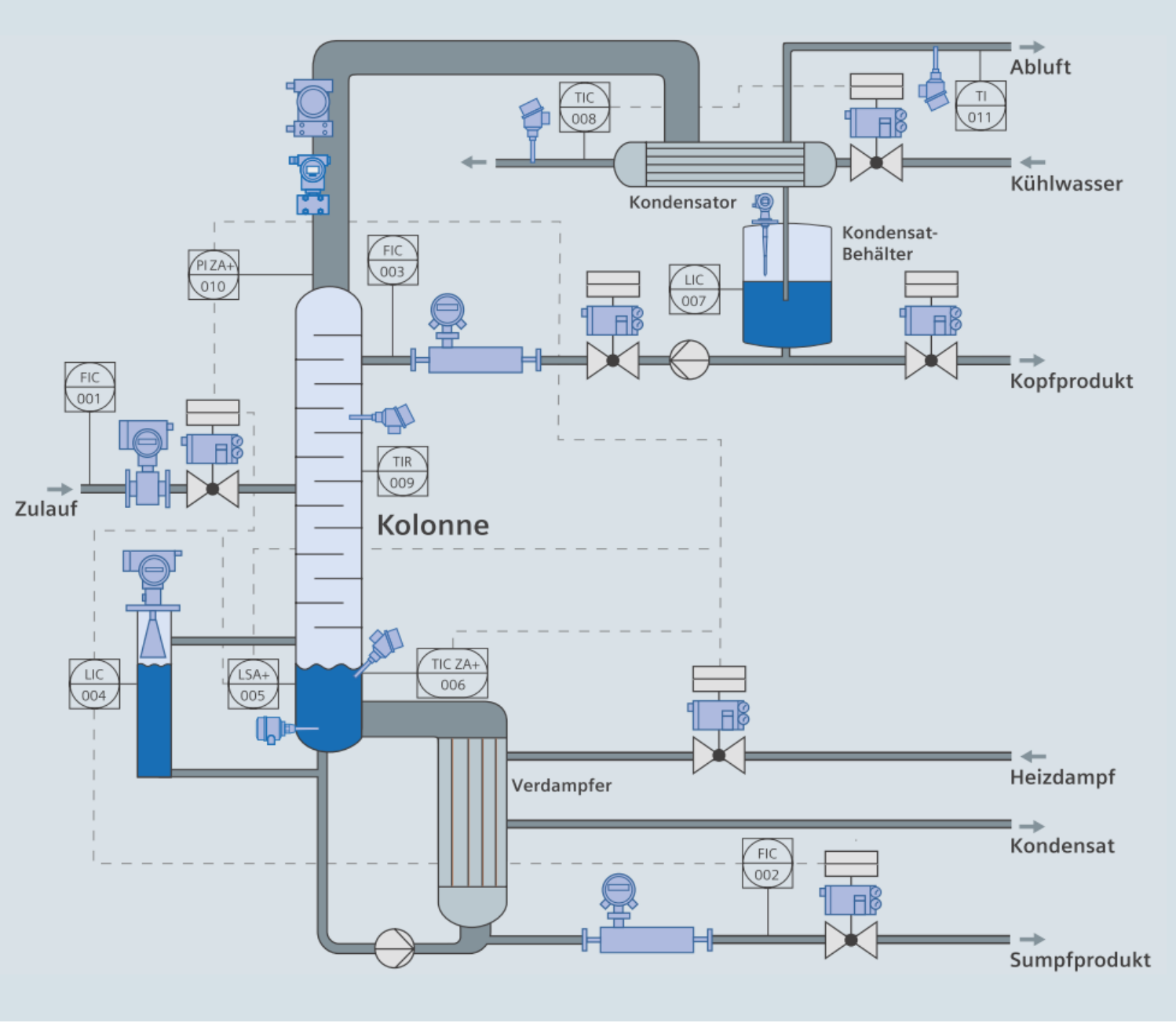
Die qualitative Methode ist ein vereinfachtes Modell, das sehr gut aufzeigt, bei welchen Gefahren welcher SIL gefordert ist.

Ermittlung des SIL nach der "Qualitativen Methode":



a: keine speziellen Sicherheitsanforderungen
b: ein einzelnes SIS nicht ausreichend
1,2,3,4: Safety Integritiy Level (SIL)

Schadensausmaß	
C_a	leichte Verletzung 1 Person, kleine schädliche Umwelteinflüsse
C_b	schwere Verletzungen oder Tod einer Person
C_c	Tod mehrere Personen
C_d	Tod sehr vieler Personen
Aufenhaltsdauer einer Person im gefährlichen Bereich	
A_a	selten bis häufig
A_b	häufig bis dauernd
Gefahrenabwendung	
G_a	möglich unter bestimmten Bedingungen
G_b	kaum möglich
Eintrittswahrscheinlichkeit	
W_1	sehr gering
W_2	gering
W_3	relativ hoch



Schema der Trennkolonne.

Ein kleines Beispiel...

...wie es zu einer Einstufung einer Sicherheitsintegritätsstufe (SIL) kommen kann:

In einem Chemiebetrieb soll eine neue Produktionsanlage gebaut werden. Das zur Herstellung des chemischen Produktes angewandte Verfahren gibt den konstruktiven Aufbau der Anlage weitestgehend vor. Da grundsätzlich mit dem Betrieb einer solchen Anlage eine Gefahr für Mensch und Umwelt ausgehen kann, müssen mögliche Risiken und Auswirkungen betrachtet und gegebenenfalls angemessene Schutzmaßnahmen in das Projekt einfließen. Exemplarisch soll hier als Anlagenteil eine Trennkolonne betrachtet werden.

Zum Betrachten der Sicherheitsrisiken, die durch den Betrieb der Trennkolonne ausgehen können, wird eine HAZOP Analyse (Hazard and Operability Study) erstellt. Um möglichst viele unterschiedliche Aspekte des Sicherheitsrisikos der Anlage zu betrachten, wird die Betrachtung von den verschiedensten Experten, wie Verfahrentechnikern, Betriebsingenieuren, Arbeitsschutzexperten, Technikern, Bedienpersonal, Betriebsleitung usw. erstellt. Gemeinsam wird von den jeweils verschiedenen Sichtweisen eine Gefahrenanalyse (Störungsbetrachtung) erstellt und daraus abgeleitet, welche Schutz- bzw. Gegenmaßnahmen erforderlich sind.

Safety Integrity Level

Aus der Gefahrenanalyse ergibt sich eine Störungsbetrachtung, die hier auszugsweise dargestellt wird:

Nr.	Störung	Ursache(n)	Auswirkung(en)	Gegenmaßnahme(n)
1	Falsche oder verunreinigte Eingangsprodukte in die Kolonne	Änderung der Gemisch-zusammensetzung des Zulauf-stroms aus vorgeschalteten Anlagenteilen	Temperatur-/Druckanstieg in der Kolonne	• Änderungen in der Zulauf-zusammensetzung gesche-hen nicht plötzlich sondern schleichend und werden bei den regelmäßigen Qualitäts-analysen bemerkt.
2	Stromausfall	Lokaler oder werksseitiger elektrischer Defekt	Ausfall Kühlung und Heizung sowie der Pumpen, ggf. Druck- und Temperaturanstieg	• Alle Armaturen gehen in Sicherheitsstellung • Die Kolonne geht selbsttätig in einen sicheren Zustand (wenn Heizung abgeschaltet und der Zulauf geschlossen wird)
3	Überfüllung im Kolonnensumpf	Versagen der Füllstands-regelung LIC 004	Fluten der unteren Kolonnen-böden mit der Gefahr der Zer-störung der Böden	• Überfüllsicherung LSA+ 005 schließt Heizdampf- und Zulauf-Ventil
4	Überfüllung des Kondensat-Sammelbehälters	Versagen der Füllstands-regelung LIC 007	Fluten des Kondensators und Verlust der Kühlleistung, An-stieg der Temperatur in der Kolonne	• Siehe Temperatur in Ko-lonne zu hoch
5	Temperatur in Kolonne zu hoch	Ausfall des Kühlwassers am Kopfkondensator	Druckanstieg und Durchschlag des Leichtsiederdampfes in die Abluft, Fall A) Mit Sicherheitsventil: An-sprechen des Sicherheits-ventils und Stofffreisetzung in die Umgebung Fall B) Ohne Sicherheitsventil: Überschreiten des maximal zu-lässigen Drucks der Kolonne mit Integritätsverlust	• Drucküberwachung PI ZA+ 010 schließt Heizdampf- und Zulauf-Ventile • Viele Temperaturmess-stellen zur schnellen Reak-tion des Bedienpersonals bei ungewöhnlichem Temperaturanstieg.
6	Temperatur im Sumpf zu hoch	Regelungsfehler in der Heizdampfzufuhr	Überhitzung des Sumpfprodu-ktes über die maximal zulässige Temperatur, Zersetzungs-reaktion mit Gasproduktion, Druckanstieg über den maxi-mal zulässigen Behälterdruck	• Temperaturüberwachung TIC ZA+ 006 schließt Heizdampf

Als Sicherheitsrelevant wurde die Messstelle Drucküberwachung am Kolonnenkopf (010) und die Temperaturüberwachung am Kolonnenboden (006) identifiziert. Dabei wurde insbesondere noch auf das Vorhandenseins eines Sicherheitsventils der Drucküberwachung eingegangen.

In Verbindung mit der Graphik zur Ermittlung des erforderlichen SIL auf Seite 10, ergeben sich bei der Trennkolonne für die Druck- und Temperaturüberwachung die entsprechenden Einstufungen.

	Drucküberwachung		Temperatur
	mit Sicherheits-ventil	ohne Sicherheits-ventil	
Schadensausmaß	C_b	C_c	C_c
Aufenthaltsdauer in Gefahrenzone	A_b	A_b	A_b
Möglichkeit der Gefahren-abwendung	G_b	G_b	G_b
Eintrittswahr-scheinlichkeit des Ereignisses	W2	W2	W1
Safety Integritiy Level	**SIL2**	**SIL3**	**SIL2**

Low und High Demand Mode

Da sich die Anwendungen in der Prozess- und Fertigungsindustrie wesentlich unterscheiden, werden auch unterschiedliche Anforderungen an das sicherheitsbezogene System (SBS) gestellt. Aus diesem Grund gibt es für jede dieser beiden Industriezweige ein unterschiedliches System, in dem die Anforderungsrate an das SBS festgelegt ist. Dabei unterscheidet man die Systeme anhand der Wahrscheinlichkeit bei Fehlern auf Anforderung des SBS (PFD, Probability of Failure on Demand).

Low Demand

Betriebsart mit niedriger Anforderungsrate an das Sicherheitssystem. Das Sicherheitssystem darf nicht häufiger als einmal pro Jahr angefordert werden.

SIL	PFD	Max. akzeptierter Ausfall des SBS
SIL 1	$10^{-2} \leq PFD < 10^{-1}$	ein gefährlicher Ausfall in 10 Jahren
SIL 2	$10^{-3} \leq PFD < 10^{-2}$	ein gefährlicher Ausfall in 100 Jahren
SIL 3	$10^{-4} \leq PFD < 10^{-3}$	ein gefährlicher Ausfall in 1.000 Jahren
SIL 4	$10^{-5} \leq PFD < 10^{-4}$	ein gefährlicher Ausfall in 10.000 Jahren

Ausfallgrenzwerte für eine Sicherheitsfunktion, die in der Betriebsart mit niedriger Anforderungsrate betrieben wird (Low Demand)

High Demand

Betriebsart mit hoher Anforderungsrate oder kontinuierlicher Anforderung an das Sicherheitssystem. Das Sicherheitssystem arbeitet kontinuierlich oder wird häufiger als einmal pro Jahr angefordert.

SIL	PFH (pro Stunde)	Max. akzeptierter Ausfall des SBS
SIL 1	$10^{-6} \leq PFH < 10^{-5}$	ein gefährlicher Ausfall in 100.000 Std
SIL 2	$10^{-7} \leq PFH < 10^{-6}$	ein gefährlicher Ausfall in 1.000.000 Std
SIL 3	$10^{-8} \leq PFH < 10^{-7}$	ein gefährlicher Ausfall in 10.000.000 Std
SIL 4	$10^{-9} \leq PFH < 10^{-8}$	ein gefährlicher Ausfall in 100.000.000 Std

Ausfallgrenzwerte für eine Sicherheitsfunktion, die in der Betriebsart mit hoher oder kontinuierlicher Anforderungsrate betrieben wird (High Demand)

In der Fertigungstechnik wird meist der High Demand Mode (continuous mode) angewandt. Hier ist oft eine kontinuierliche Überwachung der Arbeitsprozesse notwendig, um die Sicherheit von Mensch und Umwelt gewährleisten zu können.
In der Prozessindustrie findet sich typischerweise der Low Demand Mode (on demand). Ein typisches Beispiel sind Notabschaltsysteme, die erst dann aktiv werden, wenn der Prozess außer Kontrolle gerät. Dies tritt normalerweise immer seltener als einmal im Jahr auf. Aus diesem Grund ist für die Prozessinstrumentierung der High Demand Mode in den meisten Fällen bedeutungslos.

Die Betrachtungen in dieser Broschüre beziehen sich daher ausschließlich auf Low-Demand-Systeme.

Vergleich zwischen SIL und AK

DIN 19250/19251 und DIN 0801 waren deutsche Industrienormen und wurden als Basis zur Bewertung sicherer Produkte angewendet, bevor der internationale Standard IEC 61508 eingeführt wurde.

DIN 19250 definierte Anforderungsklassen (AK) anstelle der Sicherheitsintegritätsstufen (SIL1-4) der neuen internationalen Norm IEC61508. Das Grundprinzip bei der Anwendung von Anforderungsklassen (AK) beruhte darauf, dass durch den ausschließlichen Einsatz von Geräten einer Anforderungsklasse, auch das gesamte System diese Anforderungsklasse erfüllte. Zudem wurden ausschließlich die Rechnerkomponenten eines sicherheitsbezogenen Systems (SBS) betrachtet.

Bei der Anwendung mit SIL werden zwei Betrachtungen gemacht:

1. Betrachtung der systematischen Fehler
Hier gilt, wie bei der Anwendung mit AK, dass das Verknüpfen aller wichtigen Komponenten einer SIL-Klasse das Gesamtsystem auch den Anforderungen an die SIL-Einstufung erfüllt.

2. Betrachtung der zufälligen Fehler
Hier wird das gesamte SBS gerechnet. Dabei kann es vorkommen, dass trotz der Einstufung aller Geräte in eine SIL-Klasse, die Anforderungen nicht erfüllt werden.

SIL

Das SBS wird in seiner Gesamtheit betrachtet. Die Ausfallwahrscheinlichkeit und damit die Sicherheitsintegritätsstufen muss errechnet werden. Dazu werden die einzelnen Ausfallwahrscheinlichkeiten aller eingesetzen Komponenten des SBS aufaddiert. Es kann also passieren, dass trotz ausschließlichem Einsatz von SIL 2-Komponenten SIL 2 in einem SBS nicht erreicht wird! Zusätzlich müssen die systematischen Fehler des gesamten SBS mitbetrachtet werden.

AK

In einem SBS werden nur die Rechnerkomponenten betrachtet. Um Beispielsweise eine Anlage AK4-gerecht auszulegen, mussten alle entsprechenden Komponenten auch mindestens AK4 entsprechen.
Die folgende Tabelle zeigt eine Gegenüberstellung der Anforderungsklassen AK mit dem Safety Integrity Level.

DIN 19250 Anforderungsklasse	IEC 61508 Safety integrity level
AK 1	not defined
AK 2 / AK 3	SIL 1
AK 4	SIL 2
AK 5 / AK 6	SIL 3
AK 7 / AK 8	SIL 4

Gegenüberstellung AK (DIN 19250) und SIL (IEC 61508)
(kann in wenigen Fällen nicht übereinstimmend sein)

Safety Integrity Level

Wen betrifft die SIL-Klassifizierung?

Bei Anlagen, die sicherheitstechnische Auflagen erfüllen müssen, sind die Beteiligten aus unterschiedlichen Gründen betroffen:

- **Anlagenbetreiber**
  Stellen die Anforderung an die Lieferanten der sicherheitstechnischen Komponenten. Sie müssen einen Nachweis über das verbleibende Risikopotenzial erbringen.
- **Anlagenbauer**
  Müssen die Anlage entsprechend auslegen.
- **Lieferanten**
  Bestätigen die Klassifizierung ihrer Produkte.
- **Versicherungen, Behörden**
  Fordern den Nachweis für eine ausreichende Reduzierung des Restrisikos der Anlage.

Welche Geräte werden bei welchem SIL eingesetzt?

Um ein Level (SIL 1 - 4) erreichen zu können, muss das gesamte sicherheitsbezogene Syszem (SBS) die Forderungen für die systematischen Fehler (insbesondere Software) und die zufälligen Fehler (Hardware) erfüllen. Somit muss das Berechnungsergebnis des gesamten SBS dem geforderten SIL entsprechen.

In der Praxis ist das vor allem abhängig vom konzeptionellen Aufbau der Anlage bzw. des Messkreises. So können in einer SIL 3-Anlage auch SIL 2-Geräte eingesetzt werden. Mit SIL 1-Geräten werden die Anforderungen in der Regel nicht mehr erfüllt.

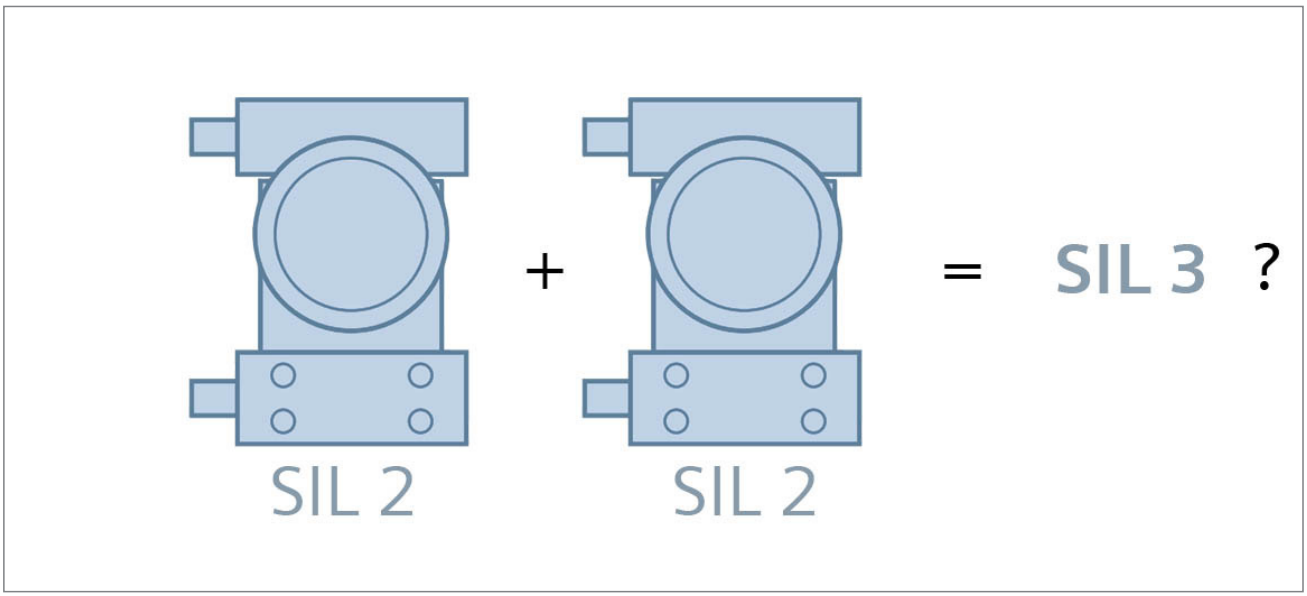
In vielen Fällen ist es vorteilhafter, zwei Sensoren einzusetzen, da der Anlagenbetreiber aus Verfügbarkeitsgründen Redundanz fordert. Ein kleiner positiver Nebeneffekt dabei ist, dass die Kosten für zwei SIL 2-Geräte meist günstiger sind als die eines SIL 3-Gerätes.

SIL 4 ist mit herkömmlichen Geräten nicht realisierbar.

Wenn zwei SIL-2-Geräte redundant betrieben werden, habe ich dann automatisch SIL 3?

Nein. Grundsätzlich gilt, dass die Ausfallwahrscheinlichkeit des gesamten SBS rechnerisch zu SIL 3 führen muss. Durch den redundanten Betrieb von SIL-2-Geräten lässt sich die Ausfallwahrscheinlichkeit für zufällige Fehler verringern. Ob es allerdings für SIL 3 reicht, muss durch das Betrachten von systematischen und zufälligen Fehlern ermittelt werden. Bezüglich systematischer Fehler (z. B. Software) muss das gesamte System ebenfalls den Anforderungen für SIL 3 genügen.

Diese Vorgehensweise gilt analog auch für andere Sicherheitsintegritätsstufen.



Fehlerarten

Man unterscheidet in einem sicherheitsbezogenen System (SBS) sowohl die systematischen Fehler als auch die **zufälligen** Fehler. **Um ein gefordertes SIL zu erfüllen, müssen beide Fehlerarten jeweils für sich betrachtet werden.**

Zufällige Fehler

Zufällige Fehler existieren nicht zum Lieferzeitpunkt. Sie ergeben sich aus Fehlern der Hardware und treten zufällig während des Betriebs auf. Beispiele für zufällige Fehler sind: Kurzschluss, Unterbrechung, Wertedrift eines Bauelements, etc. Die Fehler- und damit verbunden die Höhe der Ausfallwahrscheinlichkeit sind berechenbar. Berechnet werden die einzelnen Hardwarekomponenten eines SBS. Die daraus resultierenden Ergebnisse werden durch den PFD-Wert (average probability of failure on demand) ausgedrückt und sind Berechnungsgrundlage zur Ermittlung des SIL-Wertes.

Systematische Fehler

Systematische Fehler existieren bereits zum Lieferzeitpunkt in jedem gelieferten Gerät. Typischerweise sind es Entwicklungsfehler oder Fehler im Aufbau oder der Projektierung. Beispiele sind Softwarefehler, falsche Dimensionierung, falsche Auslegung des Messgerätes, etc. Den größten Anteil an systematischen Fehlern haben Fehler in der Gerätesoftware. Die grundlegende Überlegung bei systematischen Softwarefehlern ist, dass Fehler in der Programmierung auch zu einem Fehler im Prozess führen können.

Common-Cause-Fehler

Besondere systematische Fehler sind "Common-Cause-Fehler". Dies sind Fehler, die durch äußere Einflüsse, wie z. B. elektromagnetische Störungen (EMV) oder sonstige Umwelteinflüsse, wie z. B. Temperatur oder mechanische Beanspruchung, verursacht werden. Sie wirken gleichzeitig auf alle Komponenten eines "sicherheitsbezogenen Systems".

Systematische Fehler müssen durch besondere Maßnahmen während der Entwicklung vermieden werden. Dazu gehören z. B. qualitative Anforderungen der IEC Norm an den Entwicklungsprozess, den Änderungsprozess und die HW/SW-Architektur des Gerätes.

Die Gerätehersteller müssen Angaben über die SIL-Einstufung bezüglich der systematischen Fehler liefern. Diese Angaben finden sich in der Regel in der Konformitätserklärung der einzelnen Geräte. In Abhängigkeit vom SIL erfolgen die Angaben auch über Zertifikate von externen unabhängigen Organisationen wie dem TÜV oder Bescheinigungen von auf Prüfungen spezialisierten Firmen.

Diese Angaben sind keine Werte für weitere Berechnungen sondern lediglich eine Angabe über die SIL-Einstufung des Gerätes in Bezug auf die systematische Fehler.

Um die Forderungen bei einem bestimmten SIL (z. B. SIL 3) an die systematischen Fehler zu erfüllen, muss das gesamte SBS entsprechend ausgelegt sein. Die einfachste Betrachtung ist in diesem Fall, dass sämtliche Komponenten eine SIL-3-Einstufung für systematische Fehler besitzen.

Diversitäre Redundanz bei systematischen Fehlern

Jedoch gibt es auch die Möglichkeit SIL-2 Komponenten einzusetzen, wenn Maßnahmen ergriffen wurden, die einen systematischen Fehler nicht auf SIL-2-Niveau belassen. Sollen beispielsweise SIL-2 Druckmessgeräte in einem SIL-3-SBS eingesetzt werden, muss dafür gesorgt werden, das unterschiedliche Gerätesoftware zum Einsatz kommt. Dies erreicht man z.B. durch den Einsatz von zwei unterschiedlichen Geräten, am besten unterschiedlicher Hersteller (diversitäre Redundanz, siehe auch Bild Seite 18). Als diversitäre Redundanz kann auch gelten, wenn statt unterschiedlicher Geräte unterschiedliche Technologien (sofern sinnvoll) eingesetzt werden, beispielsweise mit einem Druckmessgerät und einem Temperaturmessgerät.

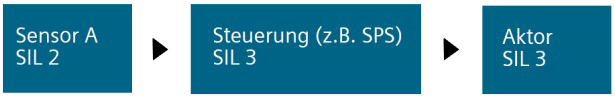
Berechnungsbeispiele
(zufällige Fehler)

Berechnung eines sicherheitsbezogenen Systems (SBS) mit einem SIL-2-Sensor

Gegebene Werte:

PFD Sensor A	$1.5 * 10^{-3}$	(geeignet für SIL 2)
PFD Steuerung	$1.3 * 10^{-4}$	(geeignet für SIL 3)
PFD Aktor	$7.5 * 10^{-4}$	(geeignet für SIL 3)

Beispiel für ein 1oo1 Sensor
1 Einheit zur Funktion erforderlich von 1 verfügbaren Einheiten



$PFD_{Sys} = PFD_S + PFD_L + PFD_A$

$PFD_{Sys} = 1.5 * 10^{-3} + 1.3 * 10^{-4} + 7.5 * 10^{-4}$

$PFD_{Sys} = 2.38 * 10^{-3}$ (SIL 2)

Durch die Verwendung dieser Komponenten erreicht das SBS die PFD für SIL 2.

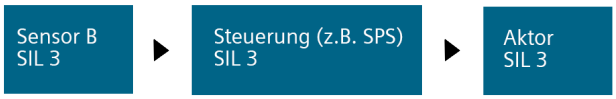
SIL	PFD
SIL 1	$10^{-2} \leq PFD < 10^{-1}$
SIL 2	$10^{-3} \leq PFD < 10^{-2}$
SIL 3	$10^{-4} \leq PFD < 10^{-3}$
SIL 4	$10^{-5} \leq PFD < 10^{-4}$

Berechnung eines sicherheitsbezogenen Systems (SBS) mit ausschließlich SIL-3-Komponenten

Gegebene Werte:

PFD Sensor B	$6.09 * 10^{-4}$	(geeignet für SIL 3)
PFD Steuerung	$1.3 * 10^{-4}$	(geeignet für SIL 3)
PFD Aktor	$5.0 * 10^{-4}$	(geeignet für SIL 3)

Beispiel für ein 1oo1 Sensor
1 Einheit zur Funktion erforderlich von 1 verfügbaren Einheiten



$PFD_{Sys} = PFD_S + PFD_L + PFD_A$

$PFD_{Sys} = 6.09 * 10^{-4} + 1.3 * 10^{-4} + 5.0 * 10^{-4}$

$PFD_{Sys} = 1.24 * 10^{-3}$ (SIL 2)

Durch die Verwendung dieser Komponenten erreicht das SBS die PFD für SIL 2.

Dieses Beispiel zeigt deutlich, dass trotz Einsatz von ausschließlich SIL-3-Komponenten das SBS die PFD für SIL 3 nicht erreicht.

SIL	PFD
SIL 1	$10^{-2} \leq PFD < 10^{-1}$
SIL 2	$10^{-3} \leq PFD < 10^{-2}$
SIL 3	$10^{-4} \leq PFD < 10^{-3}$
SIL 4	$10^{-5} \leq PFD < 10^{-4}$

Wichtiger Hinweis:
Die gezeigten Berechnungen beziehen sich ausschließlich auf die zufälligen Fehler! Ob ein SBS tatsächlich auch den Anforderungen an einen geforderten SIL erfüllt, muss noch zusätzlich in Bezug auf die systematischen Fehler überprüft werden.

Anmerkung:
Die hier gezeigten Beispiele sind sehr vereinfacht dargestellt und dienen ausschließlich zum grundlegenden Verständnis. Für eine exakte Berechnung können diese Beispiele nicht herangezogen werden!

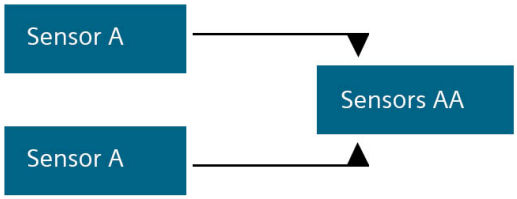
Bei den Berechnungsbeispielen werden folgende Abkürzungen verwendet:

Abkürzung	Erklärung
PFD	mittlere Ausfallwahrscheinlichkeit der Funktion bei Anforderung
PFD_{Sys}	Ausfallwahrscheinlichkeit des Systems (des gesamten SBS)
PFD_S	Ausfallwahrscheinlichkeit des Sensors
PFD_L	Ausfallwahrscheinlichkeit der Logikkomponenten / Steuerung
PFD_A	Ausfallwahrscheinlichkeit des Aktors

Berechnung eines sicherheitsbezogenen Systemss (SBS) mit redundanten Sensoren

Gegebene Werte:

PFD Sensor A	$1.5 * 10^{-3}$	(geeignet für SIL 2)
PFD Sensor A	$1.5 * 10^{-3}$	(geeignet für SIL 2)



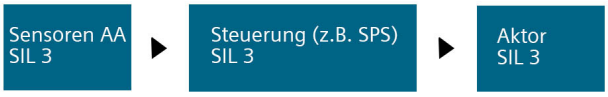
$PFD_S = 1.52 * 10^{-4}$

Die Ermittlung des PFD-Wertes für die redundante Zusammenschaltung der beiden Sensoren ist zu komplex, um sie hier nachvollziehbar wiederzugeben. Der Wert kann sich gravierend unterscheiden, wenn beispielsweise unterschiedliche Technologien, verschiedene Hersteller oder unterschiedliche Gerätebauweisen eingesetzt werden.

PFD Sensor AA	$1.52 * 10^{-4}$	(geeignet für SIL 3)
PFD Steuerung	$1.3 * 10^{-4}$	(geeignet für SIL 3)
PFD Aktor	$6.8 * 10^{-4}$	(geeignet für SIL 3)

Beispiel für ein 1oo2 Sensor

1 Einheit zur Funktion erforderlich von 2 verfügbaren Einheiten



$PFD_{Sys} = PFD_S + PFD_L + PFD_A$

$PFD_{Sys} = 1.52 * 10^{-4} + 1.3 * 10^{-4} + 6.8 * 10^{-4}$

$PFD_{Sys} = 9.62 * 10^{-4}$ (SIL 3)

Durch die Verwendung dieser Komponenten erreicht das SBS die PFD für SIL 3.

Dieses Beispiel zeigt deutlich, dass trotz Einsatz von SIL-2-Komponenten das gesamte SBS die PFD für SIL 3 erreicht.

SIL	PFD
SIL 1	$10^{-2} \leq PFD < 10^{-1}$
SIL 2	$10^{-3} \leq PFD < 10^{-2}$
SIL 3	$10^{-4} \leq PFD < 10^{-3}$
SIL 4	$10^{-5} \leq PFD < 10^{-4}$

Berechnung eines sicherheitsbezogenen Systems (SBS) mit redundanten Sensoren (schlechterer Aktorwert)

Gegebene Werte:

PFD Sensor A	$1.5 * 10^{-3}$	(geeignet für SIL 2)
PFD Sensor A	$1.5 * 10^{-3}$	(geeignet für SIL 2)

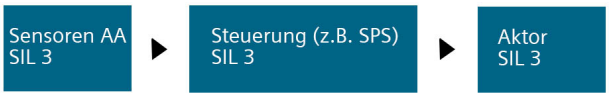
$PFD_S = 1.52 * 10^{-4}$

Die Ermittlung des PFD-Wertes für die redundante Zusammenschaltung der beiden Sensoren ist zu komplex, um sie hier nachvollziehbar wiederzugeben. Der Wert kann sich gravierend unterscheiden, wenn beispielsweise unterschiedliche Technologien, verschiedene Hersteller oder unterschiedliche Gerätebauweisen eingesetzt werden.

PFD Sensor AA	$1.52 * 10^{-4}$	(geeignet für SIL 3)
PFD Steuerung	$1.3 * 10^{-4}$	(geeignet für SIL 3)
PFD Aktor	$7.5 * 10^{-4}$	(geeignet für SIL 3)

Beispiel für ein 1oo2 Sensor

1 Einheit zur Funktion erforderlich von 2 verfügbaren Einheiten



$PFD_{Sys} = PFD_S + PFD_L + PFD_A$

$PFD_{Sys} = 1.52 * 10^{-3} + 1.3 * 10^{-4} + 7.5 * 10^{-4}$

$PFD_{Sys} = 1.03 * 10^{-3}$ (SIL 2)

Durch die Verwendung dieser Komponenten erreicht das SBS die PFD für SIL 2.

Dieses Beispiel zeigt deutlich, dass trotz Einsatz von redundanten SIL-2-Sensoren das SBS die PFD für SIL 3 nicht erreicht.

SIL	PFD
SIL 1	$10^{-2} \leq PFD < 10^{-1}$
SIL 2	$10^{-3} \leq PFD < 10^{-2}$
SIL 3	$10^{-4} \leq PFD < 10^{-3}$
SIL 4	$10^{-5} \leq PFD < 10^{-4}$

Überprüfung und Bescheinigung

Ist ein möglichst hoher SIL vorteilhaft?

Anlagenbetreiber sind für den Nachweis der funktionalen Sicherheit ihrer Anlage verantwortlich. Sie sind sich oft nicht sicher, ob sie einen hohen oder niedrigen SIL für ihre Anlage anstreben sollen. Indem das Restrisikio ermittelt wird, das von der Anlage ausgeht, ergibt sich die Anforderung an einen bestimmten SIL. Grundsätzlich wird ein möglichst niedriger SIL angestrebt. Daraus ergibt sich nicht nur ein erheblicher Kostenvorteil, sondern auch eine weitaus größere Geräteauswahl.

Ein hoher SIL wird nur dann angestrebt, wenn es unvermeidbar ist oder wenn dadurch ein Kostenvorteil an anderer Stelle entsteht, an der die Mehrkosten wieder eingespart werden können (z. B. durch Einsparen von teuren konstruktiven Zusatzmaßnahmen).

Warum ist es für einen Betreiber von Vorteil, eine IEC 61508/61511-gerechte Anlage zu haben?

Die Norm liefert ebenso eine gemeinsame Basis für Hersteller und Anwender, um die Wirksamkeit der Entwicklungsprozesse zu überwachen. Wenn Anwender sichere Geräte auswählen, um den vorgesehenen SIL für ihre Anlagen zu erreichen, können sie sicher sein, dass bei der Entwicklung einheitliche Methoden angewendet wurden.

Dadurch wird dem Anlagenbetreiber der gesetzlich geforderte Nachweis für die Risikoreduzierung erleichtert. Diesen benötigt er, um eine Betriebsgenehmigung für die Anlage zu bekommen. Es ist nicht zwingend erforderlich, dass SIL-klassifizierte Produkte eingesetzt werden. Jedoch wird dadurch die Nachweisführung wesentlich vereinfacht, da bei diesen Produkten das Restrisiko bereits bekannt (und eindeutig) ist.

Wie sicher ist die Bus-Kommunikation?

In der Prozessindustrie ist ein klarer Trend erkennbar, dass zwischen den Komponenten immer mehr Daten übertragen werden. Dies geschieht über die verschiedensten Protokolle, wie HART, PROFIBUS oder Foundation Fieldbus - mit entweder auf dem analogen 4 bis 20 mA Signal aufmodulierten digitalen Signalen oder über Buskommunikation mit einem Feldbus.

Aufgrund der Vielfalt von Fehlermöglichkeiten, wie z. B. elektromagnetische Einstrahlung (EMV) und der Komplexität des Bussystems erfolgt die Übertragung der Daten bei herkömmlichen Bussystemen nicht fehlersicher.

Für eine sichere Datenkommunikation über einen Bus oder Feldbus bedarf es daher spezieller Software-Algorithmen, die eine gesicherte Übertragung gewährleisten können. Das einzige Protokoll, das diese Anforderungen derzeit erfüllt ist PROFIBUS mit einem PROFIsafe Profil. In der Fertigungsindustrie hat sich für sicherheitsgerichtete Anwendungen PROFIsafe bereits seit längerer Zeit bewährt. In der Prozessindustrie gewinnt PROFIsafe zunehmend mit der immer größer werdenden Zahl an verfügbaren Feldgeräten an Bedeutung und trägt dazu bei, die Vorteile der Feldbustechnik auch in sicherheitsgerichteten Systemen nutzen zu können.

Was kann beurteilt werden?

Folgende Elemente können beurteilt werden:

- das Gesamtgerät
- zufällige Fehler (nur Hardware)
- systematische Fehler (Hardware und Software)

Neuanlagen – Altanlagen (Bestandsschutz)

Es gilt der Bestandsschutz für bestehende Anlagen. Dies bedeutet aber, dass bei Umbauten oder Erweiterungen der Anlage die neu hinzukommenden Teile nach den neuen Normen beurteilt werden.

Gerätebewertungen der Hersteller

Bewertung nach IEC 61508: Die Vorgaben der IEC 61508 umfassen den kompletten Produktlebenszyklus von der Idee bis zur Abkündigung eines Produktes. Um eine Komponente nach dieser Norm zu entwickeln, müssen entsprechende Vorgehensweisen und zusätzliche technische Maßnahmen von der Entwicklung bis zur Fertigung vorgenommen und überprüft werden. Durch diesen zum Teil zusätzlichen Aufwand ist die Entwicklung eines fehlersicheren Produkts aufwendiger als die einer Standardkomponente ohne SIL-Bescheinigung.

Geräte lassen sich nicht nachträglich nach IEC 61508 klassifizieren.

Bewertung nach IEC 61511 (Betriebsbewährung): Momentan gibt es nur sehr wenige Geräte, die komplett nach der Norm IEC 61508 entwickelt wurden. Um überhaupt eine praktikable Geräteauswahl zu ermöglichen, wurde in der IEC 61511 die Möglichkeit der Betriebsbewährung von Geräten ermöglicht.

In der Praxis sind die älteren Geräte seit vielen Jahren erfolgreich im Einsatz. Daher kann über eine Betrachtung von Ausfallstatistiken unter gewissen Umständen eine Aussage über die funktionale Sicherheit erbracht werden. Das Ziel ist es, zweifelsfrei zu ermitteln, ob die geforderte funktionale Sicherheit auch tatsächlich gegeben ist. Die Nachweisführung muss über eine ausreichende Stückzahl erfolgen und Angaben über die Betriebsdauer und über die Einsatzbedingungen enthalten. Die Mindesteinsatzdauer beträgt 1 Jahr und zusätzlich eine bestimmte Anzahl an Betriebsstunden. Die Betriebsbewährung gilt nur für die Version/Release des Produktes für die der Nachweis erfolgt ist. Alle zukünftigen Änderungen des Produkts müssen anschließend gemäß IEC 61508 durchgeführt werden.

Welche Bescheinigungen sind notwendig - und wer darf sie ausstellen?

Die Anlagenbetreiber benötigen einen Nachweis über die SIL-Klassifizierung der von sicherheitsbezogenen Systemen eingesetzten Komponenten. Nach IEC 61511 sind hierfür Herstellererklärungen völlig ausreichend. Zertifikate sind weder gesetzlich vorgeschrieben noch von der Norm gefordert.

Um eine Herstellererklärung oder ein Zertifikat ausstellen zu können, bedarf es einer technischen Beurteilung der einzusetzenden Sicherheitskomponente. Häufig erfolgt diese Beurteilung durch eine unabhängige Organisation. Der Hersteller kann nach einer erfolgreichen Beurteilung eine Herstellererklärung ausstellen und sich gegebenenfalls auf den Prüfbericht der Beurteilung beziehen.

Im Gegensatz zu Herstellererklärungen dürfen Zertifikate nur von einer akkreditierten Organisation (z. B. TÜV) ausgestellt werden

SIL 1	unabhängige Person
SIL 2	unabhängige Abteilung
SIL 3	unabhängige Organisation
SIL 4	unabhängige Organisation

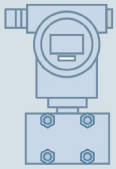
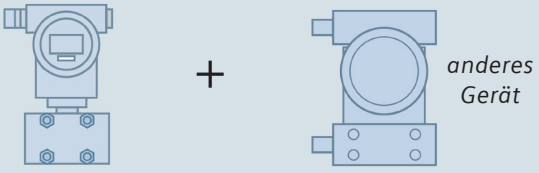
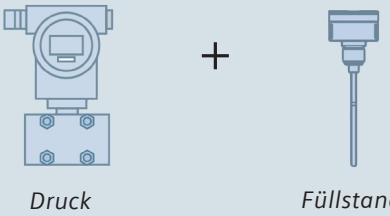
Übersicht, welche Instanz beurteilt

Je höher die geforderte Sicherheit einer Anlage ist, desto unabhängiger muss die Person sein, die eine Beurteilung der funktionalen Sicherheit ausstellt.

Konformitäts-erklärung (Hersteller-erklärung)	Der Hersteller bescheinigt, dass nach seinen Überprüfungen und Berechnungen oder aufgrund von Betriebsbewährung ein bestimmtes SIL erreicht wird. Häufig erfolgt die Überprüfung durch eine Prüfstelle wie z. B. TÜV.
Zertifikat	Wird durch eine unabhängige akreditierte Organisation ausgestellt (z. B. TÜV).

Übersicht der möglichen Bescheinigungen

Aufbaumöglichkeiten
(einkanalig / redundant)

Aufbau einkanalig ein einzelnes Gerät	
Aufbau redundant zweikanalig zwei gleiche Geräte	
Aufbau redundant diversitär zwei unterschiedliche Geräte (Maßnahme, dass ein systematischer Fehler nicht gleichzeitig auftreten kann)	
zwei unterschiedliche Technologien	

Zusammenfassung

Im Folgenden werden noch einmal wichtige Aussagen zum Thema “funktionale Sicherheit” (SIL) dargestellt:

- Der Gerätelieferant hat keinen Einfluss auf die SIL-Einstufung der Anlage
- Um beurteilen zu können, ab wann ein sicherheitsbezogenes System einen geforderten SIL einhält, muss **immer** die Ausfallwahrscheinlichkeit der zufälligen Fehler berechnet werden.
- Letztendlich ist daher der **Wert der Ausfallwahrscheinlichkeit** der eingesetzten Komponenten für den Anlagenbetreiber von Bedeutung. Die SIL-Einstufung des Gerätes kann daher oftmals für die Berechnung nur als Anhaltspunkt betrachtet werden.
- Zusätzlich muss die Verarbeitungskette den Anforderungen an die Vermeidung systematischer Fehler genügen.
- Die Aussage über die Sicherheitsintegritätsstufen eines Gerätes bedeutet nur, dass es prinzipiell für den Einsatz einer Anlage mit entsprechendem SIL geeignet ist.
- Die Norm fordert eine **Beurteilung** der funktionalen Sicherheit. **Zertifikate sind weder von der Norm gefordert noch gesetzlich vorgeschrieben.**
- Für die Prozessindustrie gilt die Anwendungsnorm IEC 61511.

Weitere Informationen finden Sie im Internet:

siemens.de/sil

siemens.de/safety

siemens.de/prozessanalytik

siemens.com/prozesssicherheit

siemens.de/prozessinstrumentierung

Siemens AG
Process Industries and Drives
Östliche Rheinbrückenstr. 50
76181 Karlsruhe
Deutschland

Änderungen vorbehalten