

Safety Integrity Level (SIL) Funktionale Sicherheit in der Anlageninstrumentierung



Mit Veröffentlichung der EN 12952 bzw. 53 im Dezember 2008 wurde auch für den Bereich der Ausrüstung von Dampf- und Heißwasseranlagen erstmals der Begriff SIL in die Regelwerke aufgenommen. So steht z.B. im Absatz 4.3.2 der EN 12953-6: „Für jede Begrenzereinrichtungsfunktion müssen eine Gefährdungsanalyse durchgeführt und angemessene Stufen der funktionalen Sicherheit eingerichtet werden“. In der Anmerkung 1 wird näher ausgeführt: „Typische Anforderungen zum Sicherheits-Integritätslevel (SIL) sind nicht kleiner als 2“.

Was ist SIL (Safety Integrity Level)?

Der Schutz von Kesselanlagen, wie von anderen Prozessen, wird über Sicherheitsfunktionen sichergestellt, die das Risiko von Gefahren für Mensch, Umwelt und Sachwerte minimieren sollen. In den Normen IEC 61508 und IEC 61511 wurden vier unterschiedliche Sicherheitsstufen, welche die Maßnahme zur Risikoreduzierung dieser Komponente beschreiben, festgelegt. Grundsätzlich kann man sagen, je höher der Zahlenwert des SIL ist, desto größer ist die Risikoreduzierung.

Die IEC 61508 beschreibt sowohl die Art der Risikobewertung als auch die Maßnahmen zur Auslegung entsprechender Sicherheitsfunktionen.

Definition von Risiko:

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

Das akzeptierte Risiko ist abhängig von den Faktoren:

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

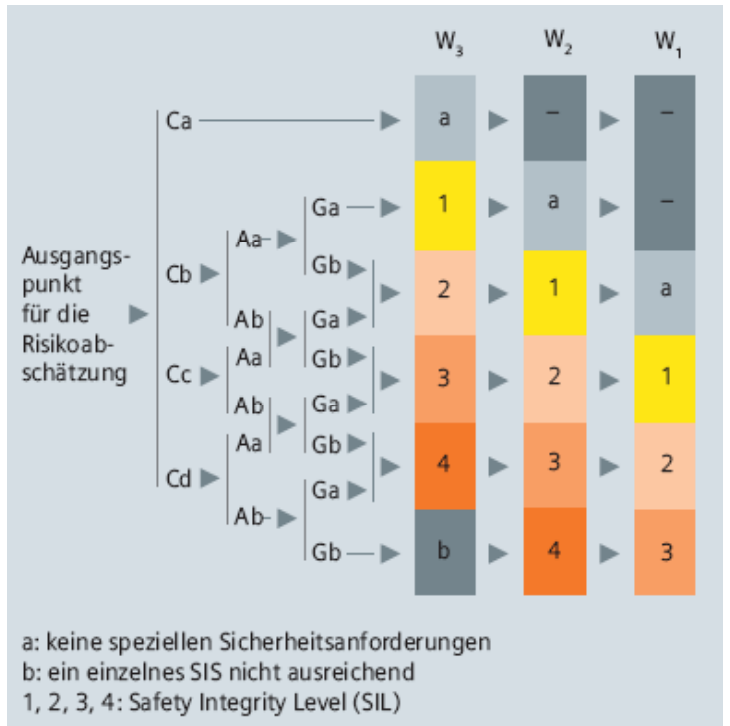
Dieses akzeptierte Risiko muss individuell eingeschätzt werden.

Schadensausmaß	
C _a	leichte Verletzung einer Person, kleinere schädliche Umwelteinflüsse
C _b	schwere Verletzungen oder Tod einer Person
C _c	Tod mehrere Personen
C _d	Tod sehr vieler Personen

Aufenthaltsdauer 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



Sicherheits-Integritätslevel (SIL)	Betriebsart mit niedriger Anforderungsrate PFD _{sys} (Low demand mode).
4	$\geq 10^{-5} \dots < 10^{-4}$
3	$\geq 10^{-4} \dots < 10^{-3}$
2	$\geq 10^{-3} \dots < 10^{-2}$
1	$\geq 10^{-2} \dots < 10^{-1}$

Die Tabelle zeigt die Abhängigkeit des Sicherheits-Integritätslevel von der mittleren Ausfallwahrscheinlichkeit bei Anforderungen einer Sicherheitsfunktion des gesamten sicherheitsbezogenen Systems (PFD_{sys}). Betrachtet wird bei einem Wasserstandbegrenzer die Anforderung „Low demand mode“, d.h. die Anforderungsrate an das sicherheitsbezogene System ist durchschnittlich einmal im Jahr.

Anteil ungefährlicher Fehler (SFF)	Fehlertoleranz der Hardware (HFT) für Typ B		
	0	1	2
< 60 %		SIL 1	SIL 2
60 % - < 90 %	SIL 1	SIL 2	SIL 3
90 % - < 99 %	SIL 2	SIL 3	SIL 4
$\geq 99 \%$	SIL 3	SIL 4	SIL 4

Die Tabelle gibt den erreichbaren Sicherheits-Integritätslevel in Abhängigkeit vom Anteil der ungefährlichen Ausfälle (SFF) und der Fehlertoleranz der Hardware (HFT) für sicherheitsbezogene Systeme an.

Welche Systeme sind von der IEC 61508 betroffen?

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

- ▶ Elektrische Geräte
- ▶ Elektronische Geräte
- ▶ Programmierbare Geräte

Die Norm betrachtet mögliche Risiken, die durch den Ausfall von Sicherheitsfunktionen verursacht werden. Neben der vollständigen Bewertung der Hard- und Software nach IEC 61508, bei der alle Fehlervermeidungs- und Fehlerbeherrschungsmaßnahmen während der Entwicklung, Fertigung und des Betriebes betrachtet werden, diese gilt für alle neu zu entwickelnden Produkte, so auch für die neuen GESTRA Systeme, gibt es noch die Möglichkeit der Betriebsbewährung nach IEC 61508/61511.

Letzteres dient zur Bewertung bereits entwickelter und gefertigter Komponenten hinsichtlich einer Eignungsaussage auf der Basis der Betriebsbewährung eines Gerätes einschließlich dessen Software und des dazugehörigen Änderungs-wesens. Zur Minimierung des Risikos schreiben sowohl die IEC 61508 als auch die IEC 61511 im Wesentlichen folgende Schritte vor:

- ▶ Risikodefinition und -bewertung nach detaillierten Versagenswahrscheinlichkeiten über die gesamte Lebensdauer der Komponenten
- ▶ Festlegung und Umsetzung der Maßnahmen zur Restrisikominimierung
- ▶ Einsatz geeigneter Geräte (bewertet oder zertifiziert)
- ▶ Wiederkehrende Prüfung der korrekten Einhaltung der Sicherheitsfunktion

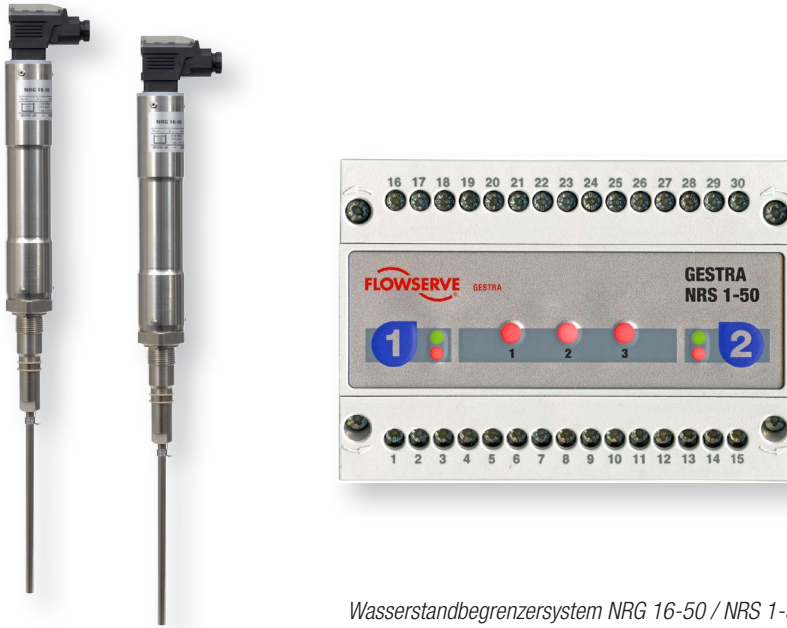
Wen betrifft die SIL-Zertifizierung?

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

- ▶ **Anlagenbetreiber**
Stellen die Anforderungen an die Lieferanten der sicherheitstechnischen Komponenten. Sie müssen den Nachweis über das verbleibende Risikopotential erbringen
- ▶ **Kesselhersteller / Anlagenbauer**
Müssen die Anlage entsprechend den Betreiberanforderungen bzw. den Regelwerken auslegen.
- ▶ **Lieferanten**
Bestätigen die Klassifizierung der Produkte
- ▶ **Versicherungen, Behörden**
Fordern den Nachweis für eine ausreichende Reduzierung des Restrisikos der Anlage

Welche Vorteile bringt die Normierung

- ▶ Internationale harmonisierte Vorgehensweise bei der Beurteilung von Schutzeinrichtungen
- ▶ Bewertung von PLT-Geräten in Hinblick auf systematische Fehler und statistisch belegbare Angaben von zufälligen Fehlern.
- ▶ Definiertes „Life-Cycle-Management“, d.h. Dokumentation aller funktionsrelevanten Entwicklungsschritte.
- ▶ Komplette Bewertung der gesamten Schutzeinrichtung



Wasserstandbegrenzersystem NRG 16-50 / NRS 1-50

Kenngrößen des Begrenzersystems:

Sicherheitstechnische Kenngrößen	SIL	Architektur	Lifetime (a)	Proof-Test-Intervall (a)
Allgemeine Werte	3	1oo2(D)	20	20
	SFF	PFDav	PFHav	λ DU
Niveauschalter NRS 1-50 allein	98,54%	$1,18 \times 10^{-4}$	$3,73 \times 10^{-8}$	$7,33 \times 10^{-8}/h$
Niveauschalter NRS 1-50 in Kombination mit einer Niveauelektrode NRG 1..-50, NRG 16-36	98,17%	$1,69 \times 10^{-4}$	$4,54 \times 10^{-8}$	$9,33 \times 10^{-8}/h$
Niveauschalter NRS 1-50 in Kombination mit zwei Niveauelektroden NRG 1..-50	97,80%	$1,17 \times 10^{-4}$	$3,76 \times 10^{-8}$	$7,38 \times 10^{-8}/h$

Bedeutung der Sicherheitstechnischen Kenngrößen:

Betrachtet man das gesamte Kesselschutzsystem so ist hierfür der sog. SIS (Safety Instrumented System) zu berechnen. Hierbei kann als Ergebnis herauskommen, dass trotz ausschließlicher Verwendung von SIL 3 Geräte der SIS lediglich SIL 2 entspricht.

Beispiel:



$$\begin{aligned}
 PFD_{\text{Sys}} &= PFD_{\text{S}} + PFD_{\text{S}} + PFD_{\text{L}} + PFD_{\text{A}} \\
 PFD_{\text{Sys}} &= 5,8 * 10^{-4} + 4,9 * 10^{-4} + 1,3 * 10^{-4} + 5,0 * 10^{-4} \\
 PFD_{\text{Sys}} &= 1,7 * 10^{-3} \gg (\text{SIL } 2)
 \end{aligned}$$

Mit einem geringen PFD für die Sensoren ergibt sich folgendes Bild:

$$\begin{aligned}
 PFD_{\text{Sys}} &= 1,17 * 10^{-4} + 2,5 * 10^{-4} + 1,3 * 10^{-4} + 5,0 * 10^{-4} \\
 PFD_{\text{Sys}} &= 9,97 * 10^{-4} \gg (\text{SIL } 3)
 \end{aligned}$$

Es wird deutlich, dass man für die Berechnung des PFD_{Sys} unbedingt die sicherheitstechnischen Kenngrößen benötigt. Bestehen Sie zur Durchführung der Berechnung bei SIL-Geräten auf diese Kenngrößen!

Funktionale Sicherheit nach IEC 61508 • Erklärung der Begriffe

Begriff	Bezeichnung	Erklärung
1oo2(D)	1 out of 2	Zweikanalige Struktur, bei der jeder Kanal (unabhängig von dem jeweils anderen) eine sichere Abschaltung herbeiführen kann. Die zusätzliche Bezeichnung (D) gibt noch an, dass eine interne Diagnose stattfindet, die das Gerät in den sicheren Zustand versetzen kann, sofern ein Fehler auftritt.
	Proof-Test-Intervall	Zeitraum in dem das Gerät betrieben werden kann, ohne dass ein manueller Test notwendig ist. In der Regel ist hiermit die gesamte Lebensdauer gemeint, sofern das Gerät nicht zwischenzeitlich gewartet oder repariert wird.
SFF	Safe Failure Fraction	Prozentualer Anteil der Ausfälle, die in den sicheren Zustand führen. Ein Gerät besteht in der Regel aus zahlreichen Bauteilen. Diese können ausfallen (durch Alterung oder durch rein zufällige physikalische Vorgänge). Ein Großteil dieser Ausfälle hat zur Folge, dass die Geräte nicht mehr betriebsfähig, aber sehr wohl noch sicher ist (es ist dann abgeschaltet, aber nicht mehr verfügbar). Diese Ausfälle werden als „sichere Ausfälle“ betrachtet. Ein Anteil der gesamten Ausfälle kann das Gerät auch in den gefährlichen Zustand versetzen. Sofern man diese erkennt, besteht keine unmittelbare Gefahr, da man das zweikanalige Gerät rechtzeitig abschalten kann. Lediglich ein kleiner Anteil der Ausfälle, die gefährlich, aber nicht erkennbar sind, können fatale Folgen nach sich ziehen (hier kann das Gerät einen gefährlichen Zustand einnehmen und es wird nicht erkannt). Der SFF-Wert gibt den Anteil der Ausfallraten an, die sich aus den „sicheren Ausfällen und den „gefährlichen aber erkennbaren Ausfällen“ im Bezug zu den gesamten Ausfällen berechnet. Wenn der Wert für SFF 100% ist, so bleiben keine „gefährlichen und unentdeckten Fehler“ mehr übrig. Je höher der SFF-Wert ist, desto immuner ist das Gerät gegenüber eventuellen Ausfällen (Maximalwert ist 100%).
PFD	Probability Failure per Demand	Mittlere Ausfallwahrscheinlichkeit der Versagensrate bei einer Anforderung. Bei der Angabe des PFD-Wertes wird in der Regel davon ausgegangen, dass man etwa einmal pro Jahr eine Sicherheitsanforderung an das Gerät hat. Ein PFD-Wert von 10^{-4} gibt dann beispielsweise an, dass die Anforderung mit einer maximalen Versagensrate von 10^{-4} möglich ist. Also bei 10.000 Anforderungen kann es höchstens einmal dazu kommen, dass die Anforderung nicht angenommen wird. Statistisch kann man auch die Aussage machen, dass man bei 10.000 Geräten, die alle eine Anforderung entgegennehmen, nur ein einziges Gerät versagt. Der PFD-Wert hängt direkt mit dem SIL-Wert zusammen. So muss beispielsweise für SIL 1 der PFD-Wert kleiner als 10^{-1} und für SIL 3 kleiner als 10^{-3} sein. Je niedriger der PFD-Wert ist, desto besser reagiert das Gerät auf Sicherheitsanforderungen.
PFH	Probability Failure per Hour	Ausfallwahrscheinlichkeit pro Stunde (gefahrlos). Geräte, die ununterbrochen Zustände überwachen, bezeichnet man als „kontinuierlich arbeitende Geräte“. Hier ist es sinnvoll, die Ausfallwahrscheinlichkeit nicht nur für den Anforderungsfall (PFD) anzugeben. PFH ist daher eine zusätzliche Angabe, welche die Ausfallwahrscheinlichkeit im Bezug auf eine Stunde angibt. Zwischen den PFD-Wert und dem PFH-Wert liegen etwa 4 Zehnerpotenzen, da ein Jahr etwa 10.000 Stunden hat. Auch der PFH-Wert hängt direkt mit dem SIL-Wert zusammen. So muss bei SIL 1 der Wert kleiner als 10^{-4} und bei SIL 3 kleiner als 10^{-7} sein. Je niedriger der PFH-Wert ist, desto sicherer reagiert das Gerät auf laufende Sicherheitsfunktionen.
λ_{DU}		Rate unerkannter gefährlicher Fehler (pro Stunde) Diese Rate ist die bereits in der SFF-Erklärung genannte Ausfallrate, die weder sicher noch erkennbar ist. Diese Ausfälle können fatale Zustände nach sich ziehen, die zur Gefahr werden. Auch mit diesem Wert ist der SIL-Wert direkt verknüpft. Er orientiert sich an dem PFH-Wert. Je niedriger der λ_{DU} -Wert ist, desto sicherer reagiert das Gerät auf laufende Sicherheitsfunktionen.
HFT	Hardware Failure Tolerance	Immunität gegenüber Fehlern. Die Hardware Fehler Toleranz gibt an, wie viele Fehler in einem Gerät (an beliebiger Stelle) auftreten können, ohne dass es unsicher wird. Wenn der HFT-Wert 0 ist, dann kann bereits ein Fehler zum Totalversagen der Sicherheit führen. Bei einem HFT-Wert von 1 kann an jeder beliebigen Stelle ein Fehler auftreten, und das Gerät verliert nicht die Sicherheitsfunktion.

Der Hersteller muss ein Functional Safety Management (FSM) eingerichtet haben. Nach erfolgreicher Einführung des FSM sowie der Überprüfung der Produktion ist der Hersteller berechtigt diese durch das TÜV-Oktagon zu dokumentieren.

GESTRA AG

Münchener Straße 77
D-28215 Bremen
Telefon +49 (0) 421-35 03-0
Telefax +49 (0) 421-35 03-393
E-Mail gestra.ag@flowserve.com
Internet www.gestra.de

