



# Funktionale Sicherheit und Explosionsschutz

## Grundlagen der funktionalen Sicherheit nach IEC 61508 und ihre Verbindung zu Anwendungen in explosionsgefährdeten Bereichen

von André Fritsch

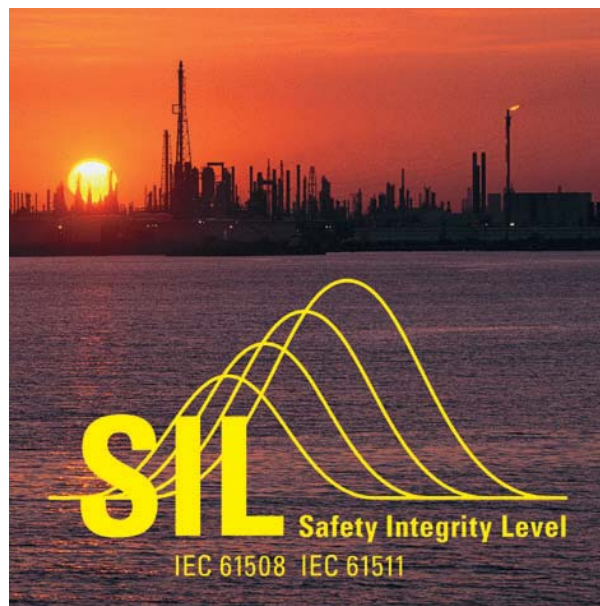


Bild 1: Funktionale Sicherheit SIL

Legt man die Normen und Vorschriften dieser beiden Fachgebiete nebeneinander und vergleicht die Inhalte, könnte man leicht zu dem Ergebnis kommen, dass diese beiden Themen nichts miteinander zu tun haben und ohne jeden Zusammenhang nebeneinander stehen. Dass dies nicht so ist und dass häufig sogar beides untrennbar miteinander verknüpft ist, wird so mancher Betreiber und Planer aus eigener Erfahrung bestätigen.

Von den Herstellern explosionsgeschützter Betriebsmittel wurde der Zusammenhang schon früh erkannt und der notwendige Wissensaufbau ging parallel mit Produktentwicklungen und Zertifizierungen einher. Daher liefern mittlerweile viele Hersteller explosionsgeschützter Betriebsmittel auch die für Stromkreise funktionaler Sicherheit spezifizierten Komponenten und Systeme zusammen mit dem dafür notwendigen Fachwissen.

## Wer hat's erfunden?

Wie kam es eigentlich zu der ›Funktionalen Sicherheit? Man sollte davon ausgehen, dass die Sicherheit des Personals eigentlich keiner speziellen Gesetzgebung bedarf, sondern im Interesse des Betreibers liegt und mit hoher Priorität behandelt wird. Leider ist dem nicht immer so und, wie häufig in der Historie, wird erst etwas unternommen, wenn etwas geschieht. Dieser Zeitpunkt war vor ca. 29 Jahren, genau am 10. Juli 1976 im norditalienischen Ort Seveso. Ein Giftgasunfall setzte hochgiftiges Dioxin (TCDD) frei, ausgelöst durch eine unkontrollierte Überhitzungsreaktion, die durch Überdruck eine Sicherung zerstörte. Der betreffende Reaktor hatte keinerlei automatische Kühlsysteme; in der Anlage existierten weder Warnsysteme noch Alarmpläne. Eine Benachrichtigung der Bevölkerung erfolgte nach 9 Tagen. Glücklicherweise befand sich zum Zeitpunkt des Störfalls kein Fachpersonal im Werk und durch einen Zufall wurde der Austritt der Giftstoffmenge beschränkt. Trotzdem gelangten ca. 2 kg hochgiftiges Dioxin in die Umwelt und verursachten Krankheiten, Sterben von Tieren und gravierende Umweltschäden.

Als Konsequenz aus diesem Unfall wurde die Verschärfung der Gesetze und Verordnungen zum Schutz von Mensch, Lebewesen und Umwelt beschlossen.

Mitte der 80er Jahre verabschiedete die Europäische Union die Seveso I Richtlinie für ›Anlagen mit großem Gefahrenpotential. Diese wurde später durch die Seveso II Richtlinie 96/82/EU ›Beherrschung der Gefahren bei schweren Unfällen mit gefährlichen Stoffen‹ ersetzt. Die deutsche Umsetzung dieser Richtlinie in nationales Recht erfolgte durch die Störfallverordnung im Bundesimmissionschutzgesetz 12. BImSchV ›Verordnung zur Umsetzung EG-rechtlicher Vor-

schriften betreffend die Beherrschung der Gefahren bei schweren Unfällen mit gefährlichen Stoffen‹ vom 26.04.2000. Diese Störfallverordnung verwies auf die DIN V 19250 ›Grundlegende Sicherheitsbetrachtung für MSR-Schutzeinrichtungen‹ und DIN V 19251 ›Leittechnik – MSR-Schutzeinrichtungen – Anforderungen und Maßnahmen zur gesicherten Funktion‹, in denen u.a. die bekannten Anforderungsklassen AK1-8 definiert werden. Nach diesen Anforderungsklassen wurden seit Jahren Anlagen und Systeme konzipiert. Im Jahr 1998 erschien die IEC 61508 ›Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer programmierbarer elektronischer Systeme‹, die seit August 2002 als EN 61508 europaweite Gültigkeit erlangt hat. Diese neue Sicherheitsnorm definiert zum ersten Mal umfassend die Sicherheitsanforderungen in der Automatisierungstechnik, unabhängig von der Anwendung, und berücksichtigt dabei auch moderne, Mikroprozessor basierende Systeme. Die IEC 61508 hat weltweite Akzeptanz gefunden und wird bzw. wurde in vielen Ländern in nationales Recht bzw. nationale Normen und Vorschriften umgesetzt (z. B. Australien AS 61508, Großbritannien BS IEC 61508, USA NFPA 79-2002, Japan JIS C 0508). Nach der Umsetzung in eine deutsche Norm DIN EN 61508 (VDE 0803) liefen am 31. Juli 2004 die DIN V 19250 und DIN V 19251 aus, so dass nur noch eine verbindliche Vorschrift existiert.

Während sich die IEC 61508 in erster Linie an die Hersteller von Komponenten für Schutzeinrichtungen wendet, wird mit der IEC 61511 ›Funktionale Sicherheit – Sicherheitstechnische Systeme für die Prozessindustrie‹ der Betreiber und Planer von Schutzeinrichtungen adressiert. Die IEC 61511 gibt Empfehlungen und Vorgaben zur Beurteilung des Schadensrisikos von Anlagen und

unterstützt bei der Auswahl geeigneter, sicherheitsgerichteter Komponenten. Im Teil 3 Anhang D der IEC wird als Verfahren zur Risikobeurteilung der Risikograph eingeführt, der ähnlich wie VDI/VDE 2180 ›Sicherung von Anlagen der Verfahrenstechnik mit Mitteln der Prozessleittechnik (PLT)‹ oder NAMUR Empfehlung NE 31 ›Anlagensicherung mit Mitteln der Prozessleittechnik‹ den Betreiber und Planer bei der Auslegung unterstützt. Die in 2003 erschienene IEC 61511 ist noch nicht in europäisches bzw. nationales Recht umgesetzt sondern befindet sich im Entwurfstadium (Entwurf DIN IEC 61511 VDE 1810; Stand Februar 2004). Weitere anwendungsspezifische Normen auf Grundlage der IEC 61508 sind z. B. die DIN IEC 61513 ›Kernkraftwerk – Leittechnik für Systeme mit sicherheitstechnischer Bedeutung‹ oder der Entwurf DIN IEC 62061 ›Sicherheit von Maschinen – Funktionale Sicherheit von elektrischen, elektronischen und programmierbaren Steuerungen von Maschinen‹.

## Fachchinesisch?

Beschäftigt man sich näher mit dem Thema ›Funktionale Sicherheit‹ und liest z. B. einen entsprechenden Prüfbericht, so wird man schnell auf einige Begriffe und Abkürzungen stoßen, die bei Weitem nicht selbsterklärend sind. Daher soll im Folgenden kurz auf die Terminologie und Fachausdrücke eingegangen werden, die zum Verständnis unabdingbar sind.

Beginnen wir mit einer Begriffsdefinition, die häufig verwechselt und missinterpretiert wird – Sicherheit und Verfügbarkeit. An einem alltäglichen Beispiel wird der maßgebliche Unterschied schnell klar. Eine Bahnüberquerung ist mit einer Schranke gesichert, so dass bei Herannahen eines Zuges →

nicht gleichzeitig ein Fahrzeug über die Schienen fahren kann. Die beiden möglichen Fehlerquellen in diesem Beispiel sind »nicht Öffnen« und »nicht Schließen« der Schranke. Sollte die Schranke nicht mehr öffnen, nachdem der Zug passiert hat, so ist die Verfügbarkeit der Straße nicht mehr gewährleistet. Abhilfe würde hier z. B. ein paralleler Übergang schaffen, da die Wahrscheinlichkeit, dass auch hier die Schranke nicht öffnet, recht gering ist. Aus Sicherheitsaspekten ist dieser natürlich strikt abzulehnen, da die Fehlerwahrscheinlichkeit für das »nicht schließen« von zwei auf vier Schranken verdoppelt wird. Hier ist es wesentlich besser, wenn jeweils zwei Schranken hintereinander gebaut werden, um einen Fehler abzufangen, falls eine der vier Schranken nicht schließt. Dies wirkt aber wiederum der Verfügbarkeit entgegen. Wie kommen wir aus diesem Dilemma heraus und erhöhen sowohl Sicherheit als auch Verfügbarkeit? Es gibt sogar mehrere Lösungen, wie z. B. eine Überführung, die aber alle eines gemeinsam haben, nämlich höhere Kosten. Bei allen Anwendungen und Maßnahmen zur Erhöhung von Sicherheit und bzw. oder Verfügbarkeit sollte der Kostenaspekt nicht aus den Augen verloren werden. Daher macht es keinen Sinn, grundsätzlich die höchste Sicherheitsstufe zu fordern, sondern diese muss anwendungs-

Schutzeinrichtung	Risikoreduzierung der Anlage
SIL 1	10 ... 100
SIL 2	100 ... 1.000
SIL 3	1.000 ... 10.000
SIL 4	10.000 ... 100.000

Tabelle 1: Zusammenhang zwischen SIL und Risikoreduzierung

IEC 61511	DIN V 19250	VDI/VDE 2180
SIL 1	AK1	Risikobereich I (niedrigeres Risiko)
	AK2	
	AK3	
SIL 2	AK4	
SIL 3	AK5	Risikobereich II (höheres Risiko)
	AK6	
SIL 4	AK7	Nicht allein durch PLT-Schutzeinrichtungen abdeckbar
	AK8	

Tabelle 2: Beziehung zwischen IEC 61511, DIN V 19250 und VDI/VDE 2180 (Quelle: E DIN IEC 61511-3; Anlage E VDE 0810 Teil 3)

spezifisch ermittelt und projektiert werden, um auch den ökonomischen Anforderungen zu genügen. Mit dem zuvor genannten Risikographen aus der IEC 61511-3 steht hierfür ein geeignetes Hilfsmittel zur Verfügung, das später noch beschrieben wird.

Die Definition des »sicheren Zustandes« ist wichtiger Bestandteil eines Sicherheitskonzeptes. Je nach Anwendung sind auch hier unterschiedliche Betrachtungen möglich. In einem Prozess, in dem eine Flüssigkeit erhitzt wird, kann der sichere Zustand z. B. durch Abschalten aller Stromkreise inklusive der Heizung erreicht werden, so dass die Flüssigkeit nicht überkocht. Bei einem Fehlerzustand in einem Flugzeug sollte dagegen alles Mögliche getan werden, um alle Systeme in Funktion zu halten. Anhand dieses Beispiels wird auch klar, dass der energielose Zustand eines Systems recht einfach zu erreichen ist und daher möglichst für Sicherheitsfunktionen bevorzugt werden sollte. Sichere Zustände bei Automatisierungskomponenten können z. B. »letzte Position halten«, »Hardware Abschaltung« oder »sicher herunterfahren« sein. Die Definition des sicheren Zustandes ist wichtiger Bestandteil der Prüfberichte von Komponenten mit SIL-Klassifizierung.

SIL selbst steht als Abkürzung für »Safety Integrity Level« und ist mittlerweile zum Synonym der Funktionalen Sicherheit geworden. Dabei definiert SIL »nur« ein Maß für die sicherheitsbezogene Leistungsfähigkeit oder Zuverlässigkeit einer elektronischen oder elektrischen Steuerungseinrichtung (Tabelle 1) und hat für sich alleine stehend nur eine geringe Aussagekraft.

Da ein SIL anders ermittelt und betrachtet wird als die AK (Anforderungsklasse) aus der DIN V 19250, ist ein direkter Vergleich nicht so einfach möglich. Als Anhaltspunkt gilt, dass ein AK 3 System in etwa einem SIL 1 System oder ein AK 5 System einem SIL 3 entspricht (Tabelle 2).

Im Unterschied zu der AK-Ermittlung steht bei SIL die Bewertung der Sicherheitskette, auch als SIF »Safety Instrumented Function« bezeichnet, im Vordergrund. Diese Sicherheitskette besteht typischerweise aus der Sicherheits-Steuerung, einem Aktor und einem Sensor. Aus einer oder mehrerer Sicherheitsketten entsteht das SIS »Safety Instrumented System«.

Generell werden Sicherheitssysteme gemäß IEC 61508 in »low demand« und »high demand« Systeme aufgeteilt. Hiermit wird

Fehlerarten	Ungefährliche Fehler	Gefährliche Fehler
Erkannte Fehler	$\lambda_{sd}$ (= safe detected)	$\lambda_{dd}$ (= dangerous detected)
Unerkannte Fehler	$\lambda_{su}$ (= safe undetected)	$\lambda_{du}$ (= dangerous undetected)
Fehler von Komponenten, die nicht Teil der Schutzeinrichtung sind	$\lambda_{np}$ (= not part)	

Tabelle 3: Fehlerarten bei Sicherheitssystemen

definiert, wie häufig im Betrieb einer Anlage oder Maschine die Sicherheitsfunktion zum Einsatz kommt. Ist damit zu rechnen, dass die Sicherheitsfunktion mehrmals täglich oder häufiger ansprechen wird, so spricht man von einem »high demand« System. Beispiele hierzu findet man bei Anwendungen im Maschinenbau, wenn z. B. eine Lichtschranke beim Eingriff eines Bedieners die Sicherheitsfunktion auslösen muss und der Bediener kontinuierlich an der Maschine arbeitet. Im Bereich der Prozessautomatisierung ist davon auszugehen, dass die Sicherheitsfunktion nur sehr selten auslöst, typischerweise maximal einmal im Jahr. Dies wird als »low demand« System bezeichnet. Beispiele hierfür sind z. B. Feueralarme oder Not-Abschaltungen. Im Folgenden wird nur auf die »low demand« Anwendungen eingegangen, da

diese im Bereich der Automatisierungslösungen den Schwerpunkt bilden.

Zur Projektierung von Sicherheitssystemen reicht die Aussage über den SIL der einzelnen Komponenten nicht aus. Während in der Vergangenheit die Sicherheitskette genau den niedrigsten AK der Einzelkomponenten erreichen konnte, muss bei SIL eine Berechnung auf Grundlage der Ausfallwahrscheinlichkeiten erfolgen. Hier kommt dem Wert  $PFD_a$  (= Probability of Failure on Demand, average) eine zentrale Bedeutung zu.  $PFD_a$  spezifiziert die durchschnittliche Wahrscheinlichkeit, mit der ein Sicherheitssystem genau in dem Moment ausfällt, in dem diese Sicherheitsfunktion benötigt wird. Bezogen wird der Wert auf einen wählbaren Zeitraum, typischerweise pro Jahr. Ein  $PFD_a$  von z. B.  $3 \cdot 10^{-3}$  besagt also, dass die Sicherheitsfunktion mit hoher Wahrscheinlichkeit einmal in 333 Jahren in dem Moment versagt, wo sie benötigt wird. Was aber nicht bedeutet, dass das System jetzt 333 Jahre ohne Ausfall funktionieren wird. So kann der sicherheitskritische Ausfall bereits nach einem Jahr erfolgen und dann 332 Jahre nicht mehr – das besagt die Wahrscheinlichkeitsrechnung. Die Ermittlung der  $PFD_a$  von Komponenten geschieht in einem recht aufwändigen analytischen Verfahren, der sogenannten FMEDA (Failure Mode Effects and Detectability Analysis), bei der bis hinunter zu den einzelnen Bauteilen analysiert

wird, was bei welchem Fehler passiert und wie dies entdeckt werden kann. Grundlage der Analyse bilden Datensammlungen über die Ausfallraten von elektronischen Bauelementen, wie z. B. der Siemens-Standard SN 29500 oder, recht konservativ, das MIL-Handbuch 217F, aber auch eigene Statistiken der Hersteller über das Ausfallverhalten ihrer Komponenten. Mögliche Fehler in Komponenten lassen sich in fünf verschiedene Fehlerarten unterteilen, die unterschiedliche Auswirkungen auf den  $PFD_a$  haben (Tabelle 3).

Bei den hier betrachteten »low demand« Systemen spielt nur der gefährliche, unerkannte Fehler  $\lambda_{du}$  eine maßgebliche Rolle, und zwar bezogen auf ein definiertes Zeitintervall, welches als  $T_{proof}$  (Prüfintervall) bezeichnet wird. Ziel dieser Prüfungen ist es, den gefährlichen Fehler, der also zum Versagen der Sicherheitsfunktion führen würde, durch Prüfungen zu entdecken und zu eliminieren. Daraus ergibt sich im Umkehrschluss, dass sich durch eine Veränderung des Zeitintervalls für die Prüfungen die Versagenswahrscheinlichkeit im Bedarfsfalle ändert. Jeder Autofahrer kennt dieses Verfahren, wenn er alle drei Jahre sein Fahrzeug dem TÜV vorstellt. Natürlich würde ein jährlicher oder gar halbjährlicher TÜV die Sicherheit des Fahrzeuges erhöhen, was aber wiederum auch eine Erhöhung der Kosten bedeutet. Manchmal ist aber die Verkürzung der Prüfzeit  $T_{proof}$  die einzige Methode, ein gefordertes SIL zu erreichen.

Der ermittelte Werte  $PFD_a$  erlaubt die Zuordnung des Gerätes zu einem SIL (Tabelle 4). Mit zwei weiteren Parametern wird die Sicherheitsqualität eines Gerätes beschrieben. Die SFF (Safe Failure Fraction) sagt aus, wie groß der Anteil der ungefährlichen Fehler zu den gesamt möglichen Fehlern ist. Ein ungefährlicher Fehler ist definiert →

$PFD_a$ (Fehler bei Anforderung; low demand Systeme)	SIL
$\geq 10^{-2} \dots < 10^{-1}$	SIL 1
$\geq 10^{-3} \dots < 10^{-2}$	SIL 2
$\geq 10^{-4} \dots < 10^{-3}$	SIL 3
$\geq 10^{-6} \dots < 10^{-4}$	SIL 4

Tabelle 4: Ausfallwahrscheinlichkeit und erreichbarer SIL

als ein Fehler, der zwar für die Sicherheit relevant ist, der aber entweder erkannt wird oder das System in den sicheren Zustand überführt. Einfaches Beispiel hierfür wäre eine Gerätesicherung, die bei einer Überspannung das Gerät in den sicheren Aus-Zustand bringt – sofern dies der sichere Zustand ist. Ein SFF von z. B. 90% besagt, dass nur 10% der möglichen Fehler in einer Sicherheitseinrichtung nicht erkannt werden können und zu einem gefährlichen Zustand führen würden. Der zweite Parameter, der hier relevant ist, ist die HFT (Hardware Failure Fraction). Mit dem HFT wird die Redundanz-Tolerance des Gerätes bzw. Systems beschrieben. Systeme ohne Redundanz, bei denen also durch einen Ausfall die Sicherheitsfunktion nicht mehr gewährleistet ist, haben eine HFT = 0. Bei einfacher Redundanz beträgt die HFT = 1 und bei doppelter Redundanz die HFT = 2. Die Verbindung der beiden Parameter SFF und HFT ergibt dann den SIL eines Gerätes. Hier-

bei wird noch unterschieden zwischen einfachen Typ A Geräten, bei denen alle Fehler bekannt und beschreibbar sind (Tabelle 5), und komplexeren Typ B Geräten, wenn nicht alle Fehler bekannt und beschreibbar sind, wie es meist bei Mikroprozessor-Systemen bzw. Software der Fall ist (Tabelle 6).

In der IEC 61511 ist der Begriff der »Betriebsbewährtheit« definiert. Kann der Hersteller die Betriebsbewährtheit seiner Komponenten oder Systeme nachweisen, lässt sich der erreichbare SIL erhöhen. In den Tabellen 5 und 6 wird dies mit »HFT = 0<sup>1)</sup>« bzw. »1<sup>1)</sup>« bezeichnet. Grundlage für diesen Nachweis bildet die Anzahl der im Markt befindlichen Geräte und die systematische Auswertung von sicherheitsrelevanten Fehlern bei diesen Geräten während ihrer Einsatzdauer. Dieser Nachweis der Betriebsbewährtheit ist bei komplexeren Systemen, die häufig mit Mikroprozessoren ausgestattet sind, die einzige effektive Möglichkeit, eine SIL-Bewer-

tung durchzuführen. Aus den beiden, eventuell unterschiedlichen SIL, die sich aus der PFD<sub>a</sub> und aus der SFF und HFT ergeben, wird der niedrigste Wert als SIL des Gerätes oder Systems angenommen.

Anders als z. B. beim Explosionsschutz existiert bei der Funktionalen Sicherheit keine Zertifizierungspflicht. Gemäss IEC 61508 reicht für SIL 2 Anwendungen eine Herstellerprüfung, die allerdings von einer unabhängigen Abteilung im Unternehmen durchzuführen ist. Ab SIL 3 empfiehlt die Norm, dass ein Fremdunternehmen die Analyse durchführt.

### Was macht der Anwender?

Glücklicherweise muss sich der Anwender nicht um die aufwändige und teilweise komplexe Ermittlung der Einzelparameter kümmern. Dies wird durch den Gerätehersteller durchgeführt und in Prüfberichten und einem Sicherheitshandbuch dokumentiert. Unbenommen bleibt aber die Verantwortung des Betreibers, seine Anlage richtig einzustufen und die richtigen Komponenten unter den richtigen Randbedingungen einzusetzen. Aus Erfahrungsberichten geht hervor, dass ca. 44% aller Fehler bereits in der Spezifikationsphase auftreten.

Der Ablauf zur Erlangung einer Genehmigung ist in der Bundesrepublik Deutschland wie in anderen Ländern gesetzlich geregelt. Hierzu stellt der Betreiber einen »Antrag auf Genehmigung der sicherheitsgerichteten Anlage« bei der staatlichen Genehmigungsbehörde (Gewerbeaufsicht). Diese beauftragt das Landesumweltamt (LUA) als Gutachter und Berater mit der Prüfung der Anlage. Das LUA führt diese Prüfung selber durch oder beauftragt einen sogenannten §29a Sachverständigen (gemäss §29a des Bundesimmissionsschutzgesetzes), z. B. vom TÜV.

SFF (Safe Failure Fraction)	HFT (Hardware Failure Tolerance)		
	0	1 / 0 <sup>1)</sup>	2 / 1 <sup>1)</sup>
< 60%	SIL 1	SIL 2	SIL 3
60 ... 90%	SIL 2	SIL 3	SIL 4
90 ... 99%	SIL 3	SIL 4	SIL 4
> 99%	SIL 3	SIL 4	SIL 4

Tabelle 5: Zusammenhang der SFF und HFT bei einfachen Geräten (Typ A2) 0<sup>1)</sup> bzw. 1<sup>1)</sup> bei Nachweis der Betriebsbewährtheit nach IEC 61511

SFF (Safe Failure Fraction)	HFT (Hardware Failure Tolerance)		
	0	1 / 0 <sup>1)</sup>	2 / 1 <sup>1)</sup>
< 60%	—	SIL 1	SIL 2
60 ... 90%	SIL 1	SIL 2	SIL 3
90 ... 99%	SIL 2	SIL 3	SIL 4
> 99%	SIL 3	SIL 4	SIL 4

Tabelle 6: Zusammenhang der SFF und HFT bei komplexeren Geräten (Typ B) 0<sup>1)</sup> bzw. 1<sup>1)</sup> bei Nachweis der Betriebsbewährtheit nach IEC 61511

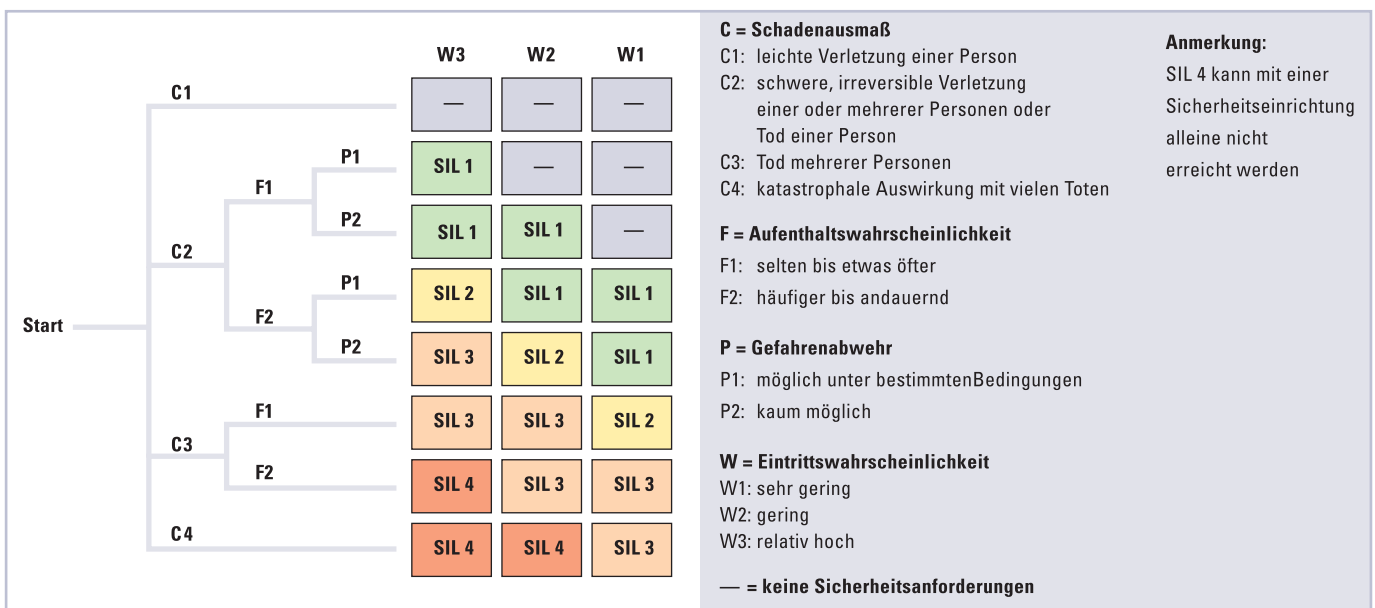


Bild 2: Risikograph für Personenschäden nach IEC 61508/61511

Nach erfolgreicher Prüfung der Anlage wird die Genehmigung durch die Behörde ausgestellt. Während des Betriebs der Anlage kann das LUA vom regionalen Umweltamt mit der Inspektion der Sicherheitseinrichtungen beauftragt werden.

Die Sicherheitsanalyse einer Anlage bzw. Teilanlage gliedert sich prinzipiell in vier Schritte. Zuerst wird die Grundfunktion der Sicherheitsanforderungen definiert, die »Safety Requirement Specification« oder kurz SRS. Was soll bzw. was muss mit der Sicherheitsfunktion erreicht werden? Im zweiten Schritt erfolgt die eigentliche Risikoanalyse, auch als »SIL Assessment« bezeichnet. Die Risikoanalyse wird z. B. mit Hilfe des Risikographs aus IEC 61511-3, Anhang D durchgeführt (Bild 2).

Der Anhang D der genannten Norm hat nur informativen Charakter, eine Anwendung des Risikographs ist also nicht obligatorisch. Alternative Verfahren sind genau so zulässig

und sogar teilweise von der Genehmigungsbehörde vorgegeben. Ein ebenfalls verwendetes Verfahren ist die Analyse nach der NAMUR Empfehlung NE93 »Nachweis der sicherheitstechnischen Zuverlässigkeit von PLT-Schutzeinrichtungen«.

Außerhalb Deutschlands wird häufig eine sogenannte LOPA »Layer Of Protection Analysis« durchgeführt. Da sich die Vorgehensweise nach IEC 61511 als recht zweckmäßig erwiesen hat und sich sowohl für die Analyse der Personengefährdung und Umweltgefährdung aber auch als Kostenanalyse für Produktionsausfallkosten eignet, wird dieses Verfahren in den folgenden Beispielen verwendet. Egal, welches Verfahren zum Einsatz kommt, wichtig ist stets die Dokumentation und Begründung der getroffenen Annahmen und Entscheidungen. Alle Festlegungen und Ergebnisse werden im Sicherheitsdokument nachvollziehbar aufgeführt. Sinnvollerweise sollte man bei der Sicher-

heitsanalyse auch den Kostenaspekt im Auge behalten: »Was kostet ein Fehler – was kostet die Vermeidung des Fehlers?«.

Eine ausführliche Anleitung zur Verwendung des Risikographs ist der o.g. IEC 61511-3 zu entnehmen, so dass hier nicht im Detail darauf eingegangen werden soll. Bereits bei der Durchführung der Risikoanalyse können Maßnahmen getroffen werden, um den erforderlichen SIL und die damit entstehenden Kosten zu reduzieren. Durch organisatorische Maßnahmen lässt sich z. B. die Aufenthaltsdauer von Personen im Risikobereich verkürzen und damit der Parameter F2 auf F1 ändern (siehe Bild 2). Beim Parameter »P«, der Gefahrenabwehr, ist durch konstruktive oder bauliche Maßnahmen, wie z. B. einer Berstscheibe oder einem Überdruckventil, eine Verringerung von P2 auf P1 machbar. Damit sind eventuell bereits in der Analysephase Verringerungen von SIL 3 auf SIL 1 erreichbar, was wiederum zu einfacheren →

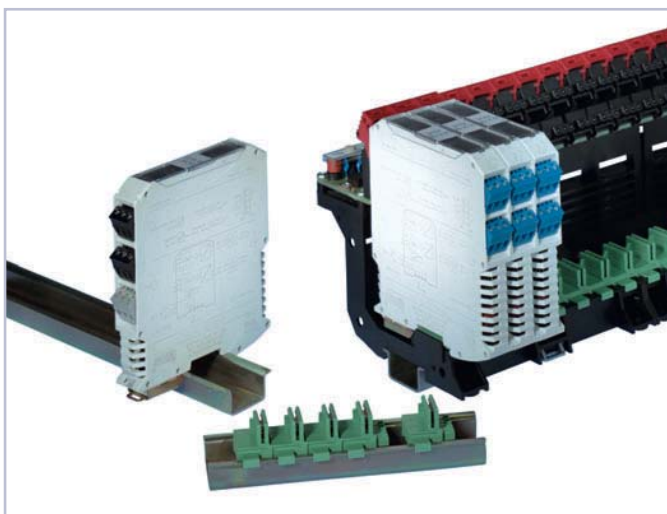


Bild 3: Ex i Trennstufen-system IS pac für SIL 2 und SIL 3 Anwendungen

und preiswerteren Lösungen führt.

Stehen die erforderlichen Anforderungen fest, folgt im dritten Schritt die Konfiguration der Sicherheitsketten, bestehend typischerweise aus SPS, Eingangs- und Ausgangskreis, inklusive der Auswahl der einzusetzenden Komponenten. Im letzten Schritt werden dann die Sicherheitsketten auf ihren SIL hin analysiert. Hierbei ist jeder Sicherheitskreis separat zu berechnen. Die Berechnung erfolgt auf Grundlage der Ausfallwahrscheinlichkeiten  $PFD_a$  der eingesetzten Komponenten, welche in den jeweiligen Prüfberichten dokumentiert sind. Bei einfachen, nicht redundanten Sicherheitskreisen werden diese

Werte addiert und das Ergebnis mit den zulässigen Werten aus Tabelle 4 verglichen.

Leider wird in der Praxis häufig der errechnete Wert von dem gewünschten abweichen. Welche Möglichkeiten gibt es jetzt, den SIL der Sicherheitssysteme zu erhöhen? Da die Prüfzeiten  $T_{proof}$  bei »low demand« Sicherheitssystemen nahezu linear in das Ergebnis eingehen, kann durch eine Verkürzung der Prüfzeiten eine Erhöhung des SIL erreicht werden. Allerdings steigen durch die häufigeren Prüfungen wiederum die Kosten. Ein weiteres probates Mittel ist der Aufbau von Redundanzen. Je nach verwendeter Redundanz sind wesentliche Verbesserungen

zu erzielen. Man spricht hier z. B. von 1oo2 (1 out of 2) oder 2oo3 (2 out of 3) Redundanzen, also eins aus zwei bzw. zwei aus drei Redundanz. Am effektivsten sind die diversitären Redundanzen, die mit unterschiedlichen Messgeräten und Messverfahren arbeiten. Wird beispielsweise eine Temperaturmessung mittels eines Temperaturmessumformers durchgeführt, so verringert zwar ein zweiter, redundanter Messumformer des gleichen Typs die Ausfallwahrscheinlichkeit. Allerdings entsteht hier die Möglichkeit eines sogenannten Common Cause Fehlers (»Beta-Faktor«), eines für beide Messumformer, die unter einer gemeinsamen Belastung stehen, gleichzeitig auftretenden Fehlers. Dies wäre beispielsweise ein systematischer Fehler in der Messumformersoftware, der z. B. bei einem bestimmten Messergebnis im selben Moment beide Geräte befällt. Bei diversitären Redundanzen werden Messumformer unterschiedlicher Hersteller und eventuell sogar mit unterschiedlichen Messverfahren eingesetzt, um eben diesen Common Cause Fehler auszuschalten und eine wesentliche Verringerung der Ausfallwahrscheinlichkeit herbeizuführen. Eine weitere Verbesserung der Sicherheitskette lässt sich durch Diagnosemethoden erreichen. Die Früherkennung von Ausfällen oder Fehlfunktionen durch die »Diagnostic Coverage« verbessert ebenfalls die Sicherheitsanwendung, da die gefährlichen, unerkannten Ausfälle in gefährliche, erkannte Ausfälle überführt werden.

Im Sicherheitshandbuch dokumentiert der Betreiber seine Sicherheitsketten über die Betriebsdauer der Systeme mit allen aufgetretenen Fehlern. Was zuerst mal als lästiger Papierkram interpretiert werden könnte, hilft aber auch bei der Auslegung neuer Sicherheitskreise. Ist ein Sicherheitssystem seit einigen Jahren im Einsatz und sind in der Zeit keine bzw. wenige sicherheitskritische Fehler

Name der Software	Hersteller	Bemerkung
SILence	HIMA	
SILver	EXIDA	Internet-Anwendung
TRAC	ABB	mit Risikograph
TRAMS	ABB	zur Dokumentation

Tabelle 8: Auswahl verfügbarer Software-Tools mit Gerätedatenbanken

aufgetreten, so ist über die Argumentation der Betriebsbewährtheit ebenfalls eine Erhöhung des SIL für diese Anwendung zu erzielen. Es sei noch angemerkt, dass eine nachträgliche Änderung des Ergebnisses der durchgeführten Risikoanalyse zur Verringerung des notwendigen SIL nicht empfehlenswert ist. Schließlich wurde die Analyse nach »bestem Wissen und Gewissen« durchgeführt und, wenn es nicht wirkliche Änderungen in der Anlage gab, gibt es keine logische Begründung für eine nachträgliche Änderung.

Wie man an den oben aufgeführten Punkten recht gut erkennt, kann die Analyse und Optimierung von Sicherheitskreisen eine recht zeitaufwändige Angelegenheit sein. Zum Glück sind mittlerweile einige Software-Tools am Markt erhältlich, die bei der Auslegung von Sicherheitsketten Unterstützung bieten. Gute Tools zeichnen sich u. a. darin aus, dass sie dem Betreiber Gerätedatenbanken zur Verfügung stellen, in denen möglichst viele Geräte mit ihren Sicherheitskennwerten gelistet sind (Tabelle 8).

Einige der Tools enthalten auch eine Risikoanalyse mit dem Risikograph, mitlaufende Kostenermittlung und eine Logbuchfunktion, in der getroffene Entscheidungen versioniert abgelegt werden. So gut und hilfreich die jeweiligen Software-Tools auch sind, sie entbinden allesamt den Betreiber nicht von seiner Verantwortung.

### Explosionsschutz und SIL

In Anlagen mit explosionsgefährdeten Bereichen treten häufig auch Anwendungen der funktionalen Sicherheit auf. Generell sind auch hier alle Zündschutzarten einsetzbar. Allerdings kommt bei der funktionalen Sicherheit erschwerend hinzu, dass die Prüfintervalle meistens im jährlichen Rhythmus

liegen, während bei reinen Explosionsschutz-Applikationen das Prüf- und Wartungsintervall typischerweise drei Jahre beträgt.

Daher kommt der einfachen und möglichst preiswerten Prüfbarkeit bei Kombinationsanwendungen aus Explosionsschutz und Funktionale Sicherheit eine besondere Bedeutung zu. Während bei den meisten Zündschutzarten, wie z. B. Druckfeste Kapselung »d« oder Erhöhte Sicherheit »e«, die Prüfungen nur im abgeschalteten Zustand und besonderen Genehmigungen möglich sind, kann bei der Zündschutzart Eigensicherheit »i« ein Arbeiten wie unter »Normalbedingungen« erfolgen. Messungen und Prüfungen sind im Betrieb im explosionsgefährdeten Bereich möglich, was beim Test der Sicherheitskreise einen großen Vorteil darstellt. Daher bietet es sich an, bei Anwendungen der funktionalen Sicherheit in explosionsgefährdeten Bereichen die Kreise in der Zündschutzart Eigensicherheit »i« zu errichten. Das Schutzprinzip der Eigensicherheit basiert auf der Strom-, Spannungs- und Leistungsbegrenzung der Signale, die in den explosionsgefährdeten Bereich gehen. Hierbei werden auch ein bzw. zwei mögliche Fehler betrachtet, woraus die Kategorien »ib« und »ia« resultieren, die wiederum die Verwendbarkeit für Zone 1 oder Zone 0 Stromkreise definieren. Dies resultiert aber nicht automatisch in eine Lösung, die für die funktionale Sicherheit geeignet ist, da hierbei keine ausreichende Aussage über Verfügbarkeit und Qualität der Signalübertragung getroffen wird. Eine entsprechende Analyse und SIL-Bewertung muss also auch hier durchgeführt werden.

Mit eigensicheren Komponenten und Systemen sind verschiedene Lösungen möglich. Der »klassische Ansatz« erfolgt über Punkt zu Punkt Verbindungen mit konventionellen Trennstufen oder Sicherheitsbarrieren. Sicherheitsbarrieren als einfache, passive

Netzwerke sind hierbei die einfachste Lösung, da sie keinen aktiven Beitrag zur Sicherheitskette liefern und prinzipiell wie ein passives Teil berücksichtigt werden können. Allerdings weisen Stromkreise mit Sicherheitsbarrieren potentielle funktionelle Risiken auf, die u. a. durch den Längswiderstand und den Erdbezug des Potentialausgleichs begründet sind. Daher werden seit einigen Jahren vorzugsweise galvanische Trennstufen eingesetzt (Bild 3). Diese müssen, da sie ja meistens mit externer Versorgung und komplexerer innerer Elektronik ausgestattet sind, eine entsprechende SIL-Analyse aufweisen. Die für die Projektierung notwendigen Parameter wie  $PFD_a$  oder Prüfintervalle  $T_{proof}$  sind in den Test-Reports bzw. Sicherheitshandbüchern dokumentiert.

Durch den Einsatz der Trennstufen kann sich bei der Auslegung der Sicherheitskette ein Problem ergeben. Da sowohl im Sensor als auch im Aktorkreis jetzt ein weiteres Element dazwischengeschaltet wird, wird natürlich die  $PFD_a$  der Sicherheitskette um diese Werte vermindert. Ein Stromkreis, der eben noch den Anforderungen an z. B. SIL 2 genügt, wird dadurch eventuell nur noch für SIL 1 verwendbar sein. Es wird daher empfohlen, dass eine Trennstufe, die für Sicherheitskreise verwendet werden kann, maximal 10 % des gesamten für den erforderlichen Sicherheitslevel verfügbaren  $PFD_a$  für sich beanspruchen sollte. Während also z. B. ein Wert von  $5 \cdot 10^{-3}$  für ein SIL 2 ausreicht, sollte die entsprechende Trennstufe maximal  $5 \cdot 10^{-4}$  davon für sich verbrauchen. In Bild 4 ist dargestellt, wie die typische Verteilung der Ausfallwahrscheinlichkeiten in einer Sicherheitskette mit Trennstufen aussehen sollte.

Wenn dieses nicht möglich ist bzw. keine entsprechende Trennstufe erhältlich ist, bleibt die Alternative der Redundanz, wie bereits vorher beschrieben. Eine weitere →

Alternative besteht im Aufbau einer zusätzlichen Diagnose. Hier bietet sich als interessante Lösung das HART-Kommunikationssignal an, das eine Vielzahl von Parametern liefert, die u.a. auch für Früherkennung von Fehlern verwendbar sind. Zur Auswertung der HART-Informationen stehen z. B. spezielle HART-Management Systeme zur Verfügung, die die HART-Signale über einen HART-Multiplexer gesammelt einlesen und auswerten. Auch der HART-Multiplexer muss natürlich eine SIL-Bewertung aufweisen, da er ja in den Sicherheitskreis eingreift und die relevanten analogen Prozesssignale verfälschen könnte (Bild 5). Die SIL-Bewertung der HART-Multiplexer beinhaltet daher nicht die Nutzung der HART-Informationen zur Steuerung und Kontrolle der Sicherheitskette, sondern vielmehr den Nachweis, dass der HART-Multiplexer keine sicherheitsrelevanten Einflüsse auf das Analogsignal hat.

In den letzten Jahren wird bei vielen neuen Anlagen vermehrt die moderne Bus-technologie eingesetzt. Auch für den Aufbau von Sicherheitssystemen stehen Lösungskonzepte und Produkte zur Verfügung. Speziell auf Sicherheitsanwendungen hin aufgebaute Busprotokolle sind z. B. PROFISafe oder INTERBUS-Safety. Die durchgängige Verwendbarkeit und damit die Akzeptanz scheidet allerdings häufig an der geringen Auswahl der hierfür zur Verfügung stehenden Feldgeräte. Hier bietet die Remote I/O Technik mehr Auswahlmöglichkeiten. Herkömmliche analoge Feldgeräte mit SIL-Klassifizierung lassen sich problemlos am Remote I/O betreiben. Wichtigste Voraussetzung allerdings ist, dass natürlich das Remote I/O System ebenfalls nach den SIL-Kriterien bewertet ist. Das derzeit einzige System am Markt, das Remote I/O System I.S.1 der Firma R. STAHL, erfüllt die Anforderungen an SIL 1 (Bild 6).

Damit sich der Anwender nicht mit der relativ komplexen Struktur dieser Sicherheitskette auseinandersetzen muss, ist es sinnvoll, das Gesamtsystem wie eine Komponente zu betrachten. Bei I.S.1 sind der Feldbus-Trennübertrager für den eigensicheren Profi-

bus DP, der eigensichere Profibus DP selbst, die CPU-Baugruppe des Systems und die analogen und digitalen Ein-/Ausgangsbaugruppen in der SIL-Bewertung gemeinsam berücksichtigt, d. h. der Anwender rechnet lediglich mit nur einem Wert für die Ausfall-

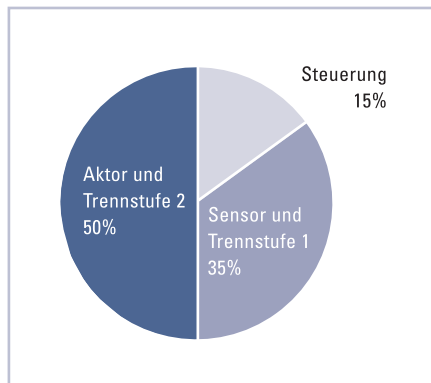


Bild 4: Typische Verteilung der PFDa in einer Sicherheitskette mit Trennstufen



Bild 5: HART-Multiplexer mit HART-Anschlußboard für Anwendungen bis SIL 3

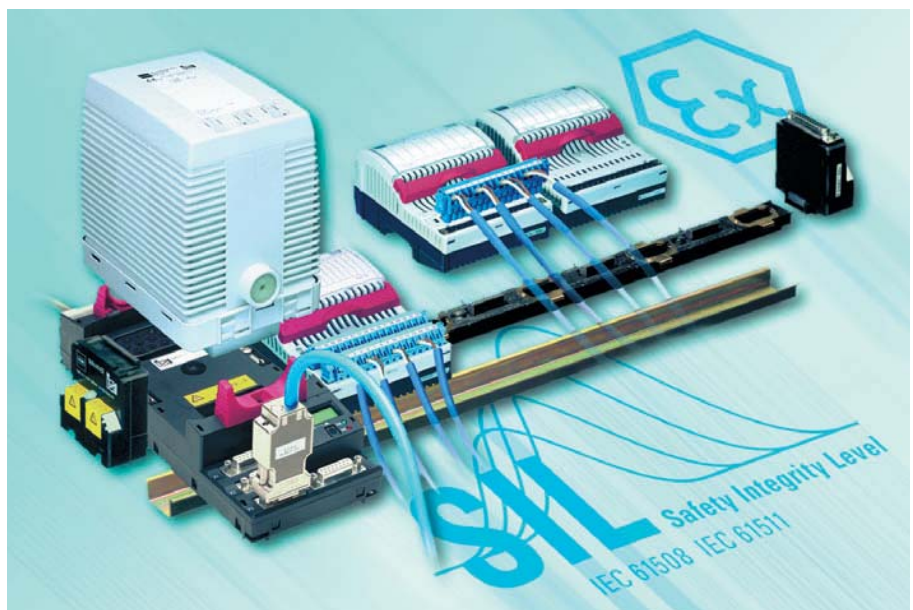


Bild 6: Remote I/O System I.S.1 für Sicherheitsanforderungen bis SIL 1

wahrscheinlichkeit seiner Sicherheitskette und addiert die entsprechenden Werte der Feldgeräte und des Automatisierungssystems dazu. Leider sind bislang nur wenige Automatisierungssysteme mit einem SIL Assessment verfügbar. In der Praxis wird daher bei der Berechnung für Systeme ohne SIL ein Erfahrungswert für die Ausfallwahrscheinlichkeit von 0,001 herangezogen.

### Zusammenfassung und Ausblick

Obwohl oder gerade weil das Thema der funktionalen Sicherheit eine recht große Komplexität erreicht hat, muss sich der Anwender mit diesem Thema auseinandersetzen. Es darf nicht sein, dass auf Grund komplizierter oder unübersichtlicher Vorschriften und Verfahren die Sicherheit der Anlagen und vor allem die des Personals auf der Strecke bleibt. Glücklicherweise berichtet die Fachpresse in der letzten Zeit häufiger über diese Thematik, so dass der Anwender hier bereits einen guten Überblick erhält. Es ist nicht weiter verwunderlich, dass sich insbesondere die Hersteller explosionsgeschützter Betriebsmittel der »Funktionalen Sicherheit« angenommen haben und sowohl Produkte als auch Schulungen hierzu anbieten. Die langjährigen Erfahrungen mit der doch recht ähnlichen Thematik des Explosionsschutzes zusammen mit den dafür notwendigen qualitativ hochwertigen Fertigungsmethoden und Entwicklungsabläufen bieten hierfür eine solide Grundlage. Noch entwickeln sich die Normen des Explosionsschutzes und der Funktionalen Sicherheit unabhängig voneinander. Doch bereits in der Überarbeitung der Niederspannungsrichtlinie (RL 73/23/EEC) wird die »Funktionale Sicherheit« enthalten sein. Eine neue europäische Norm für »Sicherheits-

einrichtungen im Explosionsschutz« (CENELEC TC31-WG9) ist in Vorbereitung, die einen Verweis auf die IEC 61508 enthält.

Es ist folglich davon auszugehen, dass uns die Funktionale Sicherheit auch in Zukunft begleiten wird und nicht, wie bei so manchem anderen Thema, als Modeerscheinung irgendwann wieder verschwindet.

### Literaturhinweise

1. Richtlinie 96/82/EU »Beherrschung der Gefahren bei schweren Unfällen mit gefährlichen Stoffen« Amtsblatt der Europäischen Gemeinschaften 1996
2. Störfallverordnung im Bundesimmissionsschutzgesetz 12. BImSchV »Verordnung zur Umsetzung EG-rechtlicher Vorschriften betreffend die Beherrschung der Gefahren bei schweren Unfällen mit gefährlichen Stoffen« vom 26.04.2000, BGBl Teil I 2000
3. DIN V 19250 »Grundlegende Sicherheitsbetrachtung für MSR-Schutzeinrichtungen« (zurückgezogen am 31.07.2004)
4. DIN V 19251 »Leittechnik – MSR-Schutzeinrichtungen – Anforderungen und Maßnahmen zur gesicherten Funktion« (zurückgezogen am 31.07.2004)
5. IEC 61508 1998 Functional safety of electrical/electrical/programmable electronic safety related systems Part 1 - Part 6
6. DIN EN 61508/VDE 0803 – Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme
7. IEC 61511 12/2003 Functional safety-Safety instrumented systems for the process industry sector
8. Entwurf DIN IEC 61511 VDE 0810; Stand Februar 2004  
»Funktionale Sicherheit – Sicherheitstechnische Systeme für die Prozessindustrie«
9. VDI/VDE Richtlinie 2180 »Sicherung von Anlagen der Verfahrenstechnik mit Mitteln der Prozessleittechnik (PLT)«
10. NAMUR Empfehlung NE 31 »Anlagensicherung mit Mitteln der Prozessleittechnik«  
Bayer Technology Service, [office@namur.de](mailto:office@namur.de)
11. NAMUR Empfehlung NE 93  
»Nachweis der sicherheitstechnischen Zuverlässigkeit von PLT-Schutzeinrichtungen«  
Bayer Technology Service, [office@namur.de](mailto:office@namur.de)
12. Entwurf DIN IEC 62061 »Sicherheit von Maschinen – Funktionale Sicherheit von elektrischen, elektronischen und programmierbaren Steuerungen von Maschinen.«
13. Siemens Safety Integrated »Applikationshandbuch Sicherheitstechnik« unter [www.siemens.de/safety](http://www.siemens.de/safety)
14. Homepage des IEC (FAQ-Listen, Broschüren etc.) unter <http://www.iec.ch/zone/fsafety>
15. Homepage der Firma EXIDA – [www.exida.com](http://www.exida.com) - mit Infoschriften, Fachartikeln und Fachbüchern
16. »Elektronische Sicherheitssysteme« von Josef Börcsök  
ISBN 3-7785-2939-0; Hüthig-Verlag