Handout

DIN EN 61508 - SIL Level – Risikograph
Zuverlässigkeit
Methoden

Peter Kafka
RelConsult

Inhalt

- Zum Inhalt von DIN EN 61508
- Gefährdungsbeurteilung - Risikograph
- Zusammenhang

  Safety Failure Fraction (SFF) – Hardware Fault Tolerance (HFT) – SIL
- Zusammenhang

  SIL – Zuverlässigkeitsforderung – Zuverlässigkeitsziel
- Bewertungsverfahren
- Schlussfolgerung
- Anhang

Zum Inhalt von DIN EN 61508

Aufbau DIN EN 61508

Die Norm ist in sieben Teilen veröffentlicht.
Nur die ersten vier Teile enthalten normative Anforderungen.

- DIN EN 61508-1: Allgemeine Anforderungen
- DIN EN 61508-2: Anforderungen an sicherheitsbezogene elektrische / elektronische / programmierbare elektronische Systeme
- DIN EN 61508-3: Anforderungen an Software
- DIN EN 61508-4: Begriffe und Abkürzungen
- DIN EN 61508-5: Beispiele zur Ermittlung der Stufe der Sicherheits-integrität (SIL)
- DIN EN 61508-6: Richtlinien für die Anwendung von DIN EN 61508-2 und DIN EN 61508-3
- DIN EN 61508-7: Überblick über Techniken und Maßnahmen

Zum Inhalt von DIN EN 61508

Aufbau DIN EN 61508

Die Norm fordert kurz gefasst folgendes (Risikokonzept):

- Bestimmung der sicherheitstechnischen Kenngrößen:
  - Probability of Failure on Demand (PFD)
  - Hardware Fault Tolerance (HFT)
  - Safe Failure Fraction (SFF)
- Nachweis
  - Durchführung von Fehler vermeidenden Maßnahmen
    (61508-2, Annex B; 61508-3, Annex A / B)
  - Wirksamkeit Fehler beherrschender Maßnahmen (61508-2, Annex A)

Zum Inhalt von DIN EN 61508

Wichtige Vereinbarungen

Funktionale Sicherheit ist der Teil der Gesamtsicherheit, der von der korrekten Funktion eines sicherheitsbezogenen E/E/PE-Systems, sicherheitsbezogenen Systemen anderer Technologie und externer Einrichtungen zur Risikominderung abhängt.

Funktionale Sicherheit ist gegeben, wenn jede spezifizierte Sicherheitsfunktion ausgeführt wird und der für jede Sicherheitsfunktion geforderte Erfüllungsgrad erreicht wird.

Ein sicherheitsbezogenes System schließt alles (Hardware, Software, menschliche Faktoren) ein, das zur Ausführung von einer oder mehrerer Sicherheitsfunktionen erforderlich ist. Ausfälle der Sicherheitsfunktion würde eine signifikante Zunahme des Sicherheitsrisikos für Personen und/oder der Umwelt bedeuten.

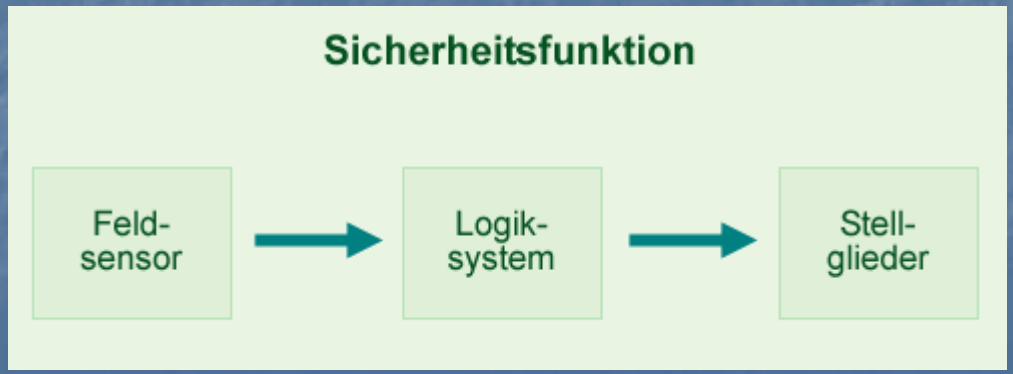
Ein sicherheitsbezogenes System kann eine eigenständige Anlage zur Ausführung einer bestimmten Sicherheitsfunktion sein (z. B. Brandmeldesystem) oder in eine andere Anlage integriert sein (z. B. Drehzahlüberwachung einer Maschine).

Zum Inhalt von DIN EN 61508

Anwendbarkeit

Die DIN EN 61508 ist auf sicherheitsbezogene Systeme anzuwenden, wenn eines oder mehrere dieser Systeme elektrische und/oder elektronische und/oder programmierbare elektronische (E/E/PE) Geräte enthalten.

Die Norm ist immer auf das gesamte sicherheitsbezogene E/E/PE-System anzuwenden, z. B. vom Sensor über Steuerelektronik und Kommunikationssysteme bis zum Aktuator, unter Berücksichtigung möglicher Fehler des Bedienpersonals.



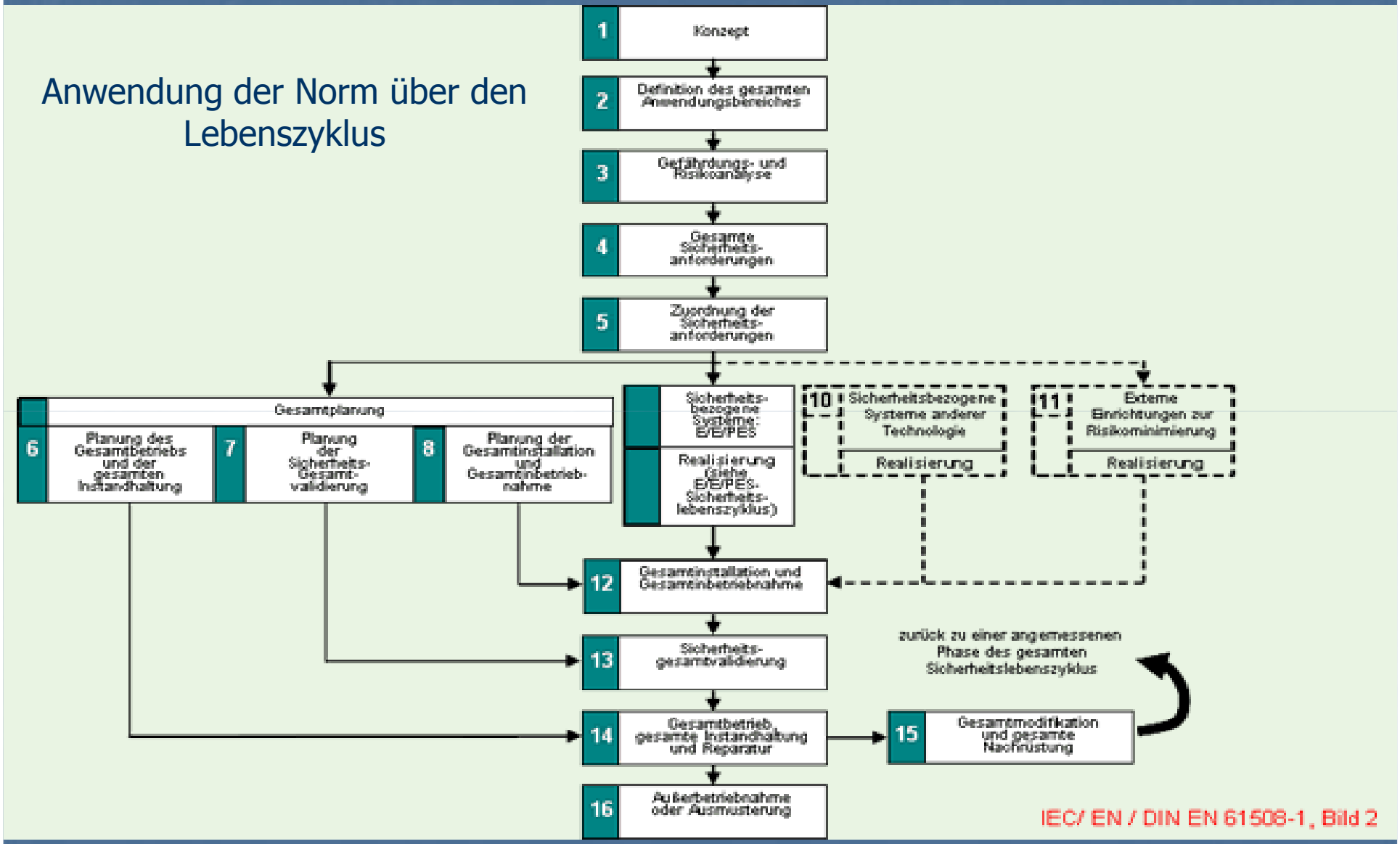
Zum Inhalt von DIN EN 61508

Anwendbarkeit

- Vermeidung „systematischer" Fehler durch Design-Anforderungen (61508-2, 3)
- Anforderungen an Betriebsbewährung (61508-2, Abschnitte 7.4.7.6 bis 7.4.7.10)
- Für Software wird auf „systematisches" Verhalten verwiesen und deshalb die Anwendung der quantitativen Analyse nicht gefordert (eigene Bemerkung: Argument nicht nachvollziehbar)

Zum Inhalt von DIN EN 61508

Anwendung der Norm über den Lebenszyklus



Zum Inhalt von DIN EN 61508

Anwendbarkeit (Beispiele)

- Notabschalt-Systeme
- Feuermelde- und Gaswarnsysteme
- Turbinenüberwachung
- Brennersteuerungen
- Automatische Überlastanzeige für Kräne
- Sicherheitsverriegelungen und Notabschaltsysteme für Maschinen
- Medizinische Geräte
- Dynamische Positionierung von Schiffsbewegungen
- Fly-by-wire Steuerung von Flugzeugleitwerken
- Bahnsignalsysteme
- Verwendung drehzahlvariabler Antriebsmotoren als Schutzmaßnahme
- Kraftfahrzeug-Antiblockiersysteme, Motormanagementsysteme
- Netzwerk-basierte Fernüberwachung

Zum Inhalt von DIN EN 61508

Rechtliche Stellung (siehe auch http://delegibus.org/2004,10.pdf)

EN 954
Die EN 954-1 ist unter der EU-Maschinenrichtlinie harmonisiert. Für komplexe (programmierbare) Elektronik mit Sicherheitsfunktionen müssen weitere Normen (z. B. DIN EN 61508) angewendet werden, um den anerkannten Stand der Technik zu erfüllen.

DIN EN 61508
Die Normenreihe EN 61508 zur funktionalen Sicherheit, mit der die IEC 61508 durch die Europäische Normenorganisation CENELEC übernommen worden ist, wurde 2001 durch CENELEC ratifiziert. Sie wird als DIN EN 61508 (VDE 0803) in das deutsche Normenwerk übernommen. Diese Normen beschreiben den Stand der Technik, ihre Einhaltung ist aber freiwillig und unverbindlich. Die DIN V VDE 0801 wurde 2004 zurückgezogen.

Harmonisierte Normen zur Maschinenrichtlinie siehe:
http://europa.eu.int/comm/enterprise/newapproach/standardization/harmstds/reflist/machines.html

Zum Inhalt von DIN EN 61508

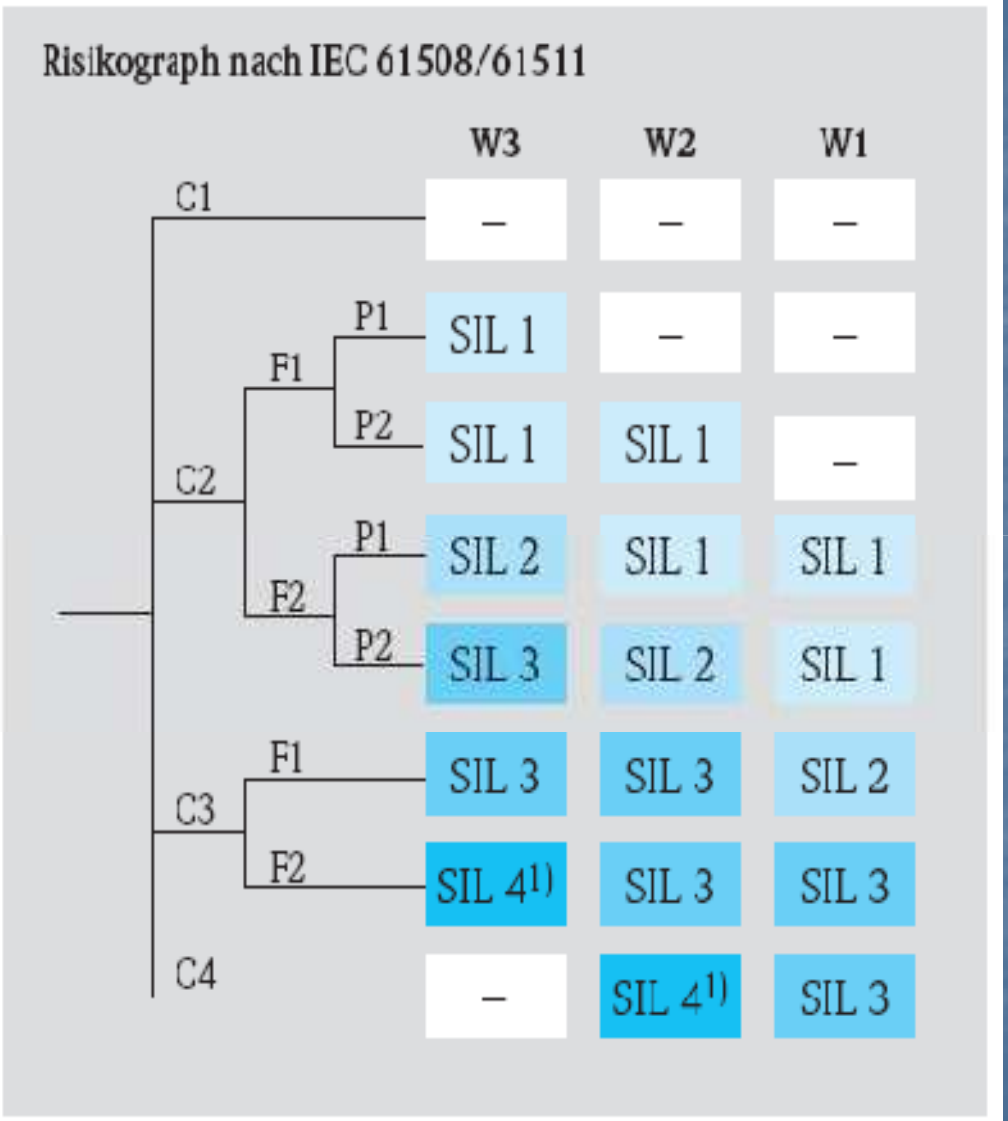
Rechtliche Stellung

Die EN 61508 ist nicht unter einer EU-Richtlinie harmonisiert. Eine automatische Vermutungswirkung zur Erfüllung der Schutzziele einer Richtlinie geht somit von ihr nicht aus. Dennoch kann der Hersteller eines Produktes der Sicherheitstechnik die EN 61508 auch zur Erfüllung grundlegender Anforderungen aus Europäischen Richtlinien nach der neuen Konzeption verwenden, z. B. in den folgenden Fällen:

- Es existiert keine harmonisierte Norm für den betreffenden Anwendungsbereich. In diesem Fall darf der Hersteller die EN 61508 verwenden. Sie hat aber keine Vermutungswirkung.

- Aus einer harmonisierten Europäischen Norm (z. B. EN 954, EN 60204-1) wird auf die DIN EN 61508 verwiesen. Hierdurch wird sichergestellt, dass die betreffenden Anforderungen der Norm eingehalten werden ("mitgeltende Norm"). Wendet der Hersteller die EN 61508 im Sinne dieser Verweisung sachkundig und verantwortungsbewusst an, so nutzt er die Vermutungswirkung der verweisenden Norm.

Gefährdungsbeurteilung - Risikograph



Schadenausmaß
C1 leichte Verletzung einer Person oder kleinere schädliche Umwelteinflüsse
C2 schwere, irreversible Verletzung einer oder mehrerer Personen oder Tod einer Person oder vorübergehende größere schädliche Umwelteinflüsse
C3 Tod mehrerer Personen oder lang andauernde größere schädliche Umwelteinflüsse, z. B. nach Störfall-verordnung.
C4 katastrophale Auswirkung, sehr viele Tote.

Aufenthaltsdauer
F1 selten bis öfter
F2 häufig bis dauernd

Gefahrenabwehr
P1 möglich unter bestimmten Bedingungen
P2 kaum möglich

Eintrittswahrscheinlichkeit
W1 sehr gering
W2 gering
W3 relativ hoch

Zusammenhang SFF-HFT-SIL

Typ A: „Einfache“ Geräte (alle Fehler bekannt und beschreibbar)			
SFF Safe Failure Fraction	HFT Hardware Fault Tolerance		
	0	1	2
< 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

Typ B: „Komplexe“ Geräte (nicht alle Fehler bekannt und beschreibbar)			
SFF Safe Failure Fraction	HFT Hardware Fault Tolerance		
	0	1	2
< 60 %	not allowed	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

Erklärungen:

Einfache Geräte: z. B. Relais, Transistoren

Komplexe Geräte: z. B. Prozessoren

SF: Prozentualer Anteil von Ausfällen ohne Potential für einen Funktionsausfall

HFT: HFT = N, dann würden N+1 Fehler zum Ausfall führen

SIL: Safety Integrity Level einer Sicherheitsfunktion

Zusammenhang SIL - Zuverlässigkeit

SIL	Niedrige Anforderungsrate [Ausfall/Anf.] ≤1 mal pro Jahr	Hohe Anforderungsrate [Ausfall/h] ≥ 1 mal pro Jahr oder dauernd
1	10E-2 bis 10E-1	10E-6 bis 10E-5
2	10E-3 bis 10E-2	10E-7 bis 10E-6
3	10E-4 bis 10E-3	10E-8 bis 10E-7
4	10E-5 bis 10E-4	10E-9 bis 10E-8

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

Zur Ermittlung dieser Zuverlässigkeitswerte gibt der „Stand der Technik" geeignete quantitative Methoden vor
(z. B. FTA, PSA, Markov)
Die Norm:
Simulation, Cause-Consequence Analyse, FTA, Markov, Blockdiagramm

Bewertungsverfahren

Die Norm unterscheidet zwei Bewertungsverfahren:

- Hardware-Fehlertoleranz (HFT) und die Sicherheits-Ausfallfraktion (SFF)
  (Methode: z. B. Blockdiagramm)
- Berechnung der Ausfallwahrscheinlichkeit bzw. Nichtverfügbarkeit
  (Methode: z. B. FMEA, FTA, Markov)

Ermittlung des erforderlichen SIL:

z. B. mit Hilfe des Risikograph (Methode: z. B. HAZOP, FMEA)

Einbeziehung menschlicher Faktoren:

- menschliche Aktivitäten oder Fehler, die eine Anforderung des sicherheits-bezogenen E/E/PE-Schutzsystems auslösen (initial action)
- menschliches Versagen bei der Reaktion auf Alarme (recovery action)
- menschliches Versagen bei Test und Wartung, das die Wirksamkeit herabsetzt und die Wahrscheinlichkeit eines Ausfalls bei Anforderung erhöht (corrective action)

Bewertungsverfahren

Zur Bestimmung der „Probability of Failure of each Safety Function due to Random Hardware Failures“ (61508- 2, 7.4.3.2.1):

- Quantitative Methode: dann Wert ≤ target value
- Qualitative Methode: dann Wert ≤ lower target value

Damit ist bei der qualitativen Methode eine Art „Unsicherheitsfaktor“ eingebaut.

Die Bedingungen zur „Calculation of Probability“ sind relativ ausführlich und vollständig im Abschnitt 61508- 2, 7.4.3.2.2 aufgelistet.

Die benannten Methoden (Simulation, C-C-Analysis, FTA, Markov, BDM) entsprechen nach eigenen Kenntnissen nicht dem Stand der Technik.

Auch besteht der Widerspruch zum Einbeziehen des menschlichen Faktors.

Schlussfolgerung

- Die Norm hat weit reichenden internationalen Eingang in vielen Branchen gefunden;
- Sie ist umfangreich und sicherlich nicht frei von Widersprüchen oder erforderlichen Interpretationen;
- Klar erkennbar ist das „Risikokonzept" und das Bestreben eine möglichst „sichere"
- Technik zu bauen und zu betreiben;
- Der Weg zu quantitativen Analysen und Vorgehensweisen ist vorgezeichnet aber nicht zwingend vorgeschrieben;
- Es ist vorauszusehen, dass die quantitative Analyse „Stand der Technik" wird (siehe z. B. SIL Konformitätserklärungen verschiedener Hersteller);
- Es ist erwartbar, dass die „generische" Norm noch von weiteren Branchen für eigene Belange angepasst wird (siehe z. B. Automobilindustrie mit Vereinbarung von SIL-A);
- Auf Grund der fehlenden Erfahrung in vielen Branchen mit quantitativer Zuverlässigkeitsanalyse und der zugehörigen Risikoabschätzung ist eine schrittweise berufliche Fortbildung bzw. Einarbeitung der zuständigen Mitarbeiter angebracht.

Anhang - Praktischer Hinweis

Wie geht man beim Lesen der Norm am besten vor?

Anhang A der EN 61508-5 liefert eine Einführung zu den Themen Risiko und Sicherheits-integrität.

In EN 61508-1 sind die Anforderungen an den gesamten Sicherheitslebenszyklus (enthalten in Abschnitt 7) in einem Lebenszyklus-Diagramm (Abbildung 2) zusammengefasst. Ein Überblick zu jeder Phase ist in Tabelle 1.

Zusätzlich enthält Abschnitt 7.18 die Anforderungen an Verifikation, Management und Bewertung der Funktionalen Sicherheit.

EN 61508-6, Anhang A, gibt einen achtseitigen Überblick über die Anforderungen von EN 61508-2 und EN 61508-3.

In EN 61508-2 sind die Anforderungen an den E/E/PES Sicherheitslebenszyklus (enthalten in Abschnitt 7) in einem Lebenszyklus-Diagramm (Abbildung 2) zusammengefasst. Ein Überblick zu jeder Phase ist in Tabelle 1.

In gleicher Weise sind in EN 61508-3 die Anforderungen an den Softwarelebenszyklus (enthalten in Abschnitt 7) in Abbildung 3 zusammengefasst, ein Überblick in Tabelle 1.

Anhang - Anwendungsspezifische Normen

Die Norm dient auch als Basisnorm zur Erstellung branchen- oder anwendungs-spezifischer Normen. So Z. B.:

IEC 61511-1: Funktionale Sicherheit - Sicherheitstechnische Systeme für die Prozessindustrie - Teil 1: Allgemeines, Begriffe, Anforderungen an Systeme, Software und Hardware

IEC 61511-2: Funktionale Sicherheit - Sicherheitstechnische Systeme für die Prozessindustrie - Teil 2: Anleitungen zur Anwendung der IEC 61511-1

IEC 61511-3: Funktionale Sicherheit - Sicherheitstechnische Systeme für die Prozessindustrie - Teil 3: Anleitung für die Bestimmung der erforderlichen Sicherheits-Integritätslevel

IEC 61513: Kernkraftwerke - Leittechnik für Systeme mit sicherheitstechnischer Bedeutung - Allgemeine Systemanforderungen

In Entwicklung befinden sich IEC 62061 für den Maschinenbereich und IEC 61800-5-2 für Antriebssysteme.

Anhang - Weitere Referenzen

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/electronical/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*
11. NAMUR Empfehlung NE 93 ›Nachweis der sicherheitstechnischen Zuverlässigkeit von PLT-Schutzeinrichtungen‹ Bayer Technology Service, *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
14. Homepage des IEC (FAQ-Listen, Broschüren etc.) unter http://www.iec.ch/zone/fsafety
15. Homepage der Firma EXIDA – www.exida.com - mit Infoschriften, Fachartikeln und Fachbüchern
16. ›Elektronische Sicherheitssysteme‹ von Josef Börcsök ISBN 3-7785-2939-0; Hüthig-Verlag

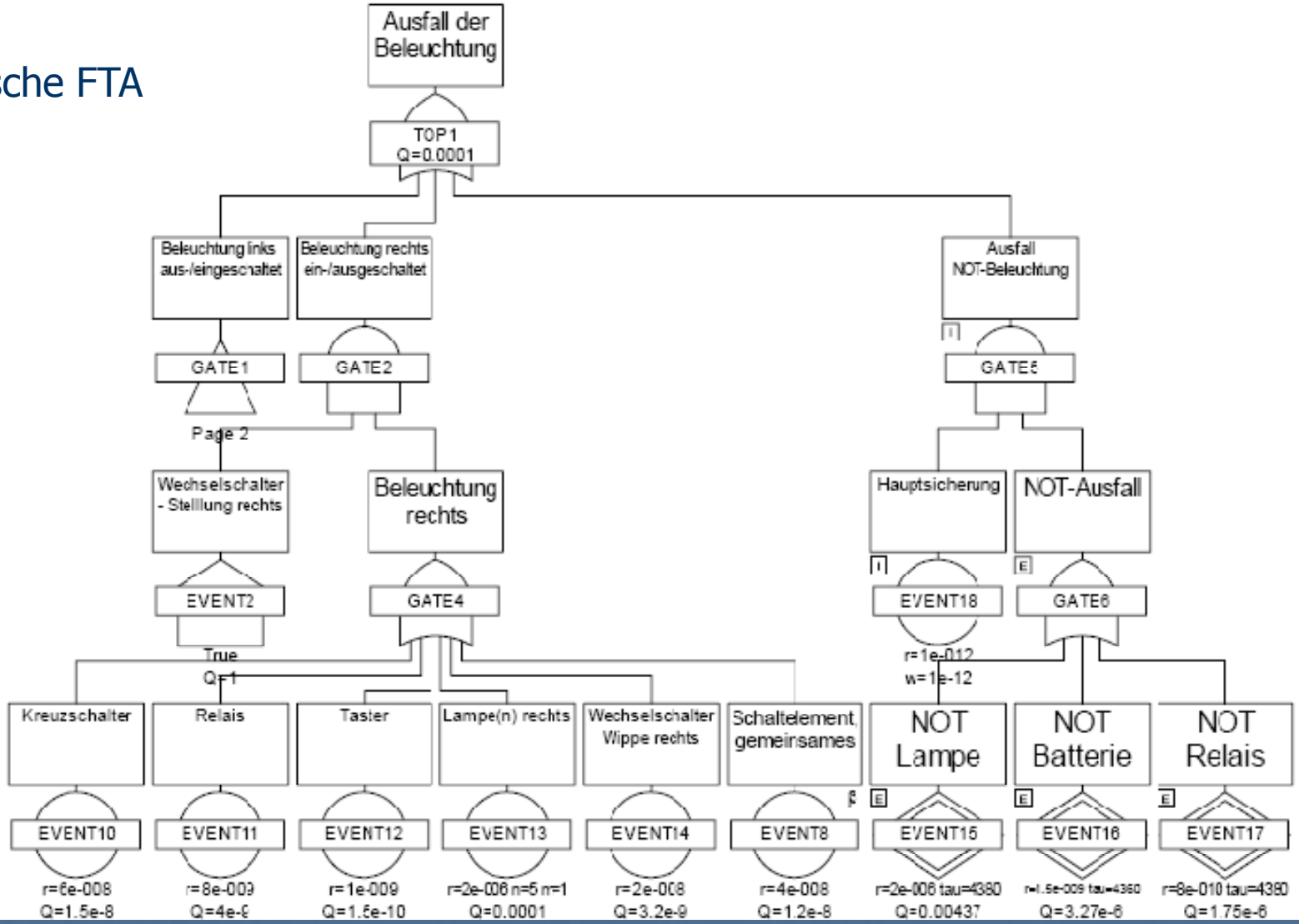
DIN EN ISO 12100 löst DIN EN 292 ab
Mit Ausgabedatum 04/2004 sind die beiden Normen:

DIN EN ISO 12100-1: Sicherheit von Maschinen - Grundbegriffe, allgemeine Gestaltungsleitsätze - Teil 1: Grundsätzliche Terminologie, Methodologie (ISO 12100-1:2003) sowie

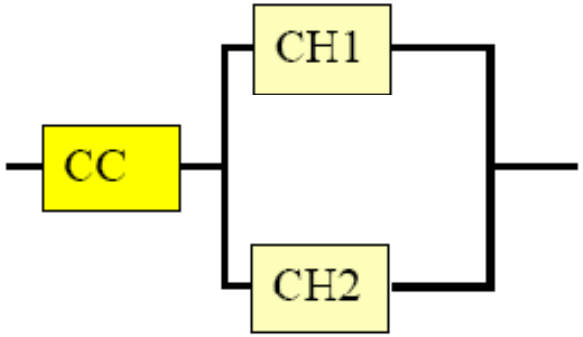
DIN EN ISO 12100-2: Sicherheit von Maschinen - Grundbegriffe, allgemeine Gestaltungsleitsätze - Teil 2: Technische Leitsätze (ISO 12100-2:2003)

Anhang – Fehlerbaum Methode (FTA)

Typische FTA



Anhang – Common Cause Failure



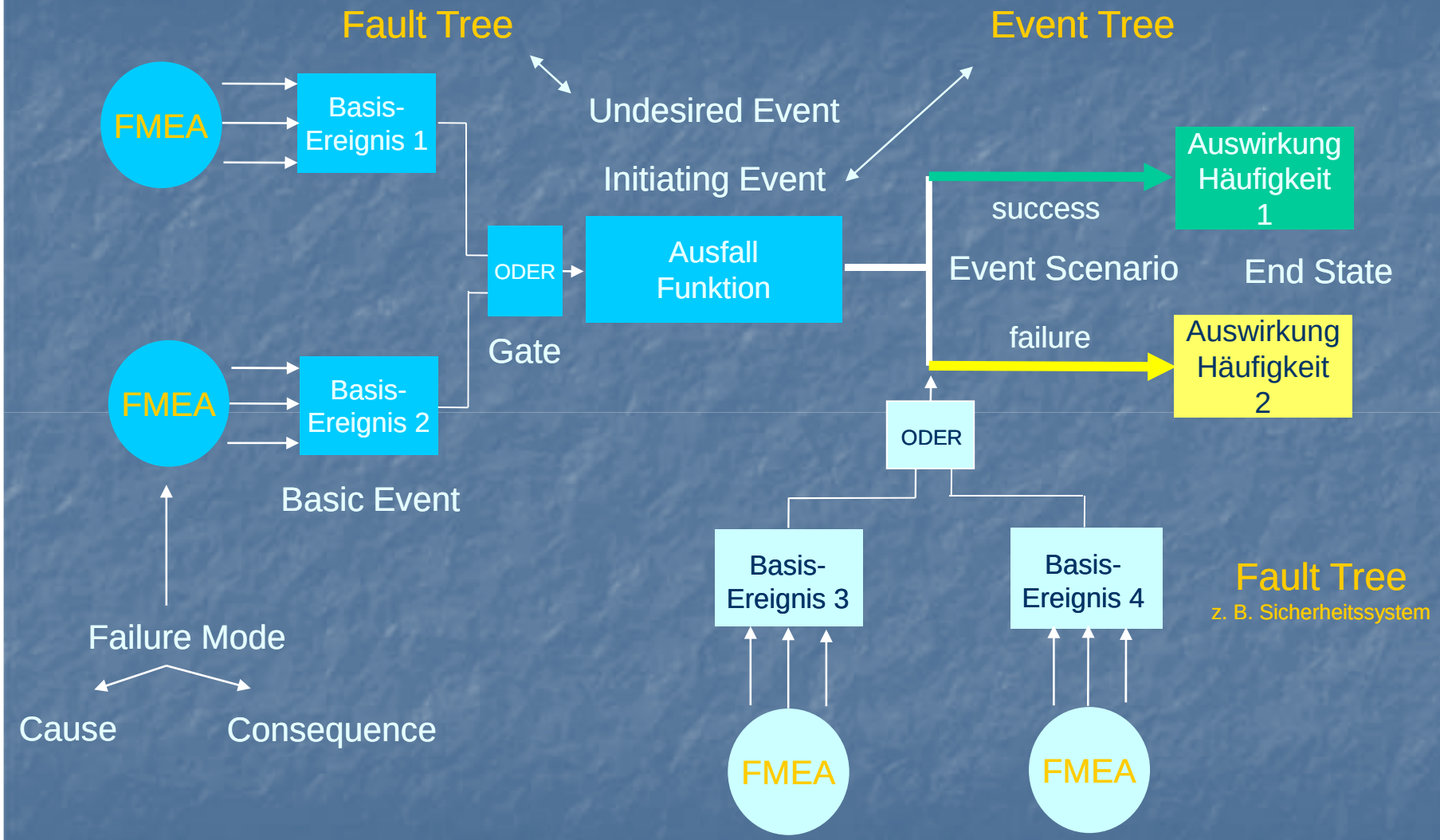
- CH1: PFD(t): 10^{-5}
  CH2: PFD(t): 10^{-5}
  CC: β= 1%

$$PFD = PFD_{CH1} \cdot PFD_{CH2} + CC$$

$$PFD = 10^{-10} + 10^{-7}$$

Common Cause Failure (CC) dominiert
Ausfall redundanter Schaltungen !

Anhang – PSA Methode



Anhang – PSA Methode

Typischer Ablauf einer PSA Analyse

- Klärung des zu betrachtenden Untersuchungsgegenstand und seiner Zustände
- Erstellung Systemstruktur
- Erstellung Funktionsstruktur
- Durchführung von FMEA‘s (ggf. beim Unterlieferanten)
- Aufbau der Analysestruktur mit Festlegung auslösender und unerwünschter Ereignisse und Durchführung von FTA und ETA unter Berücksichtigung der FMEA‘s
- Review der qualitativen FTA und ETA durch unabhängige Dritte
- Erstellung der Daten-Basis zur quantitativen Auswertung von FTA und ETA
- Probabilistische Berechnung von FTA und ETA
- Eingehende Diskussion der Ergebnisse
- Identifikation von geeigneten Ertüchtigungsmaßnahmen
- Iterationsschleife unter Berücksichtigung verbesserter Komponenten, Funktionen und/oder Systemstrukturen
- Festlegung von Aktionen zur Systemertüchtigung

Anhang – SW Analysemethoden

Table B. 1 — Semi-formal methods (referenced by Table A.1, A.2 and A.4
Tabelle B.7 – Semi-formale Methoden (Verweisung aus Tabelle A.1, A.2 und A.4)

	Technique/Measure*		See IEC 61508-7	SIL1	SIL2	SIL3	SIL4
1	Logic/function block diagrams	Logik- und Funktions-Blockdiagramme	see note below	R / +	R / +	HR / ++	HR / ++
2	Sequence diagrams	Ablaufdiagramme	see note below	R / +	R / +	HR / ++	HR / ++
3	Data flow diagrams	Datenflussdiagramme	C.2.2	R / +	R / +	R / +	R / +
4	Finite state machines/state transition diagrams	Zustandsübergangs-diagramme	B.2.3.2	R / +	R / +	HR / ++	HR / ++
5	Time Petri nets	Petri Netze	B.2.3.3	R / +	R / +	HR / ++	HR / ++
6	Decision/truth tables	Entscheidungs- und Wahrheitstabellen	C.6.1	R / +	R / +	HR / ++	HR / ++

NOTE - Logic/function block diagrams and sequence diagrams are described in IEC 61131-3: 1993 Programmable controllers - Part 3: Programming Languages.

R: Recommended; HR: Highly Recommended

* Appropriate techniques/measures shall be selected according to the safety integrity level.

Anhang – SW Programmiersprachen

	Programming language	SIL1	SIL2	SIL3	SIL4
1	Ada	HR	HR	R	R
2	Ada with subset	HR	HR	HR	HR
3	MODULA-2	HR	HR	R	R
4	MODULA -2 with subset	HR	HR	HR	HR
5	PASCAL	HR	HR	R	R
6	PASCAL with subset	HR	HR	HR	HR
7	FORTRAN 77	R	R	R	R
8	FORTRAN 77 with subset	HR	HR	HR	HR
9	C	R	---	NR	NR
10	C with subset and coding standard, and use of static analysis tools	HR	HR	HR	HR

Entnommen aus IEC 61508, Teil 7

R: Recommended
HR: Highly Recommended

Anhang – SW Programmierstandard

Table B.1 — Design and coding standards
(referenced by table A.4)

Technique/Measure			SIL 1	SIL 2	SIL 3	SIL4
1	Use of coding standard		HR	HR	HR	HR
2	No dynamic objects		R	HR	HR	HR
3a	No dynamic variables		---	R	HR	HR
3b	Online checking of the installation of dynamic variables		---	R	HR	HR
4	Limited use of interrupts		R	R	HR	HR
5	Limited use of pointers		---	R	HR	HR
6	Limited use of recursion		---	R	HR	HR
7	No unconditional jumps in programs in higher level languages		R	HR	HR	HR

R: Recommended
HR: Highly Recommended

Anhang - Bussysteme

Anzunehmende Fehler in der Datenkommunikation (61508-2, Abschnitt 7.4.8):

- Übertragungsfehler
- Wiederholung
- Verlust
- Einfügung
- Falsche Abfolge
- Nachrichtenverfälschung
- Zeitliche Verzögerung
- Maskierung

Anhang – ZV Datenquellen

Data Source:	Equipment Covered:
MIL-HDBK-217F - Reliability Prediction of Electronic Equipment	Electronic components
EPRD - Electronic Parts Reliability Data (RAC)	Electronic components
NPRD-95 Non-electronic Parts Reliability Data (RAC)	Mechanical and electro-mechanical components
NONOP-1 Non-operating Reliability Data (RAC)	Mechanical and electro-mechanical components
FMD-97 Failure Mode/Mechanism Distributions (RAC)	Electronic, electrical, mechanical and electromechanical components
SR-332 Reliability Prediction for Electronic Equipment (Telcordia Technologies)	Electronic components
EiReDA - European Industry Reliability Data	Mainly components in EDF nuclear power plants
OREDA - Offshore Reliability Data (DNV)	Topside and sub-sea equipment for offshore oil and gas production
Michel - Handbook of Reliability Prediction for Mechanical Equipment	Mechanical equipment - military applications
T-Book (Reliability Data of Components in Nordic Nuclear Power Plants	Components in nuclear power plants (S)
Reliability Data for Control and Safety Systems - PDS Data Handbook	Sensors, detectors, valves & control logic
Safety Equipment Reliability Handbook (exida)	Safety equipment (sensors, logic units, actuators)
WellMaster (ExproSoft)	Components in oil wells
SubseaMaster (ExproSoft)	Components in sub-sea oil/gas production systems

Anhang – ZV Datenquellen

Data Source:	Equipment Covered:
PERD - Process Equipment Reliability Data (AIChE)	Process equipment
GIDEP (Government-Industry Data Exchange Program)	
CCPS Guidelines for Process Equipment Reliability Data, (AIChE)	Process equipment
PERD - Process Equipment Reliability Data (AIChE)	Process equipment
FARADIP	Electronic, electrical, mechanical, pneumatic equipment
IEEE Std. 500-1984: IEEE Guide to the Collection and Presentation of Electrical, Electronic, Sensing Component, and Mechanical Equipment Reliability Data for Nuclear Power Generating Stations	See title
FASIT (Feil og avbrudd i kraftsysteme)	Power supply systems (in Norwegian)
Guide FIDE 2004, Edition A, Methodologie de fiabilite pour les systemes electroniques	Electronic components
PDS, Data Handbook, 2004 Edition; SINTEF	Reliability data for safety instrumented systems
ZEDB, Zentrale Zuverlässigkeits- und Ereignisdatenbank (VGB)	Zuverlässigkeitskenngrößen für Kernkraftwerks-komponenten (D)
RDF 2000, CNET	Electronic components
IEEE Gold Book - IEEE STD 493-1997	Daten für kommerzielle Spannungs-Verteilungs-systeme

"Aha Effekt": so viele Daten gibt es !

Anhang – Vermutungswirkung

Die von den privaten Normungsgremien herausgegebenen technischen Normen haben, abgesehen vom Ausnahmefall der Inkorporierung oder statischen Verweisung, keine unmittelbare Bindungswirkung. Dagegen kommt einer Reihe von technischen Normen, auf die im Rahmen technischer Standards, zum Beispiel die allgemein anerkannten Regeln der Technik, durch Gesetz oder Rechtsverordnung gesondert verwiesen wird, eine mittelbare Bindungswirkung zu. Bei derartigen normkonkretisierenden Verweisungen spricht eine Vermutung dafür, dass die verwiesenen technischen Normen die allgemein anerkannten Regeln der Technik wiedergeben. Diese Vermutungswirkung hat auch prozessuale Bedeutung. Allerdings ist die Ansicht, bei der Beachtung derartiger technischer Normen streite ein Anscheinsbeweis dafür, dass ordnungsgemäß geleistet sei, als zu weitgehend abzulehnen. Nach den Grundsätzen des Anscheinsbeweises ist es vielmehr nur möglich, diesen zum Beweis der Kausalität oder des Verschuldens im Fall eines Schadens heranzuziehen. Insoweit ist aber insbesondere im Bereich des innovativen Abweichens von technischen Normen Zurückhaltung angebracht, um die technische Innovation nicht zu behindern.

Aus: http://delegibus.org/2004,10.pdf

Anhang – IEC 61508 – IEC 61511

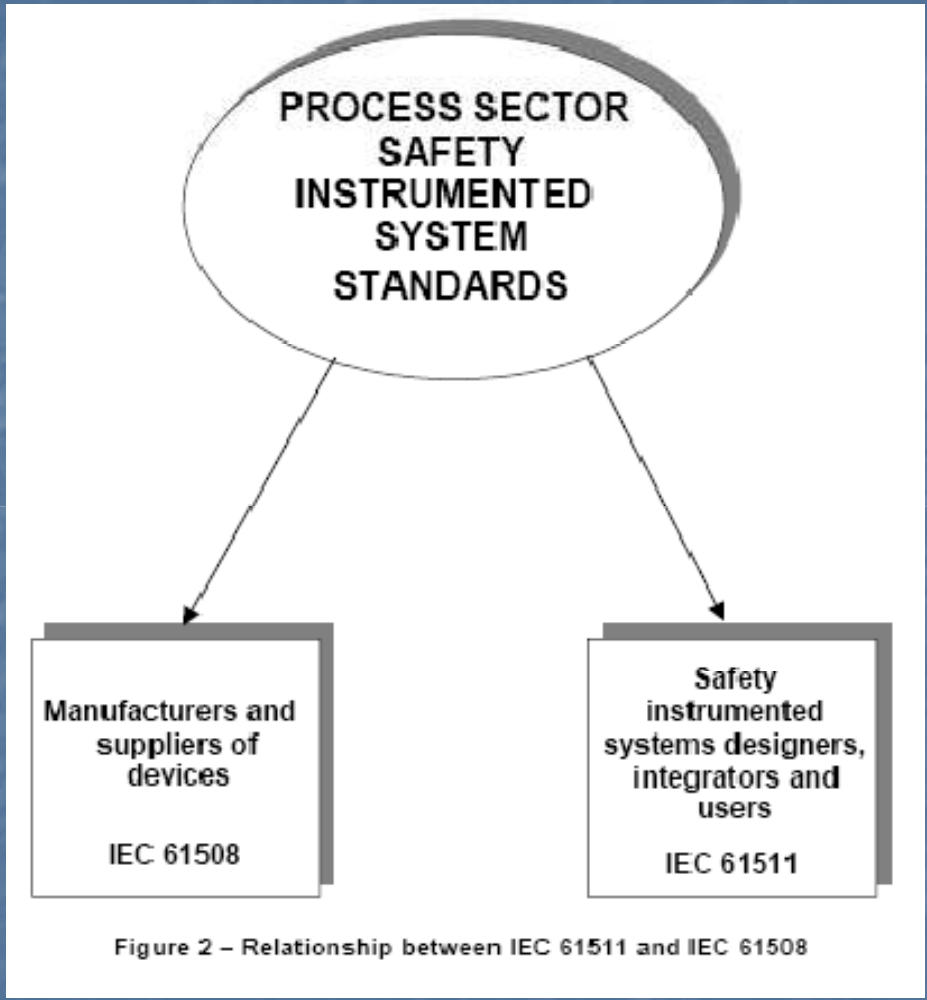


Figure 2 – Relationship between IEC 61511 and IEC 61508

Der Lieferant der Sicherheits-instrumentierung sollte der 61508 und der Anlagenbauer der 61511 folgen

Anhang – IEC 61511-1 Prozess Industrie

8 Process hazard and risk analysis

8.1 Objectives

The objectives of the requirements of this clause are:

- to determine the hazards and hazardous events of the process and associated equipment;
- to determine the sequence of events leading to the hazardous event;
- to determine the process risks associated with the hazardous event;
- to determine any requirements for risk reduction;
- to determine the safety functions required to achieve the necessary risk reduction;
- to determine if any of the safety functions are safety instrumented functions (see Clause 9).

Title
61511-1, Ed. 1: Functional safety - Safety instrumented systems for the process industry sector - Part 1: Framework, definitions, system, hardware and software requirements

Anhang – IEC 61511-1 Prozess Industrie

8.2 Requirements

8.2.1 A hazard and risk analysis shall be carried out on the process and its associated equipment (for example, BPCS). It shall result in

- a description of each identified hazardous event and the factors that contribute to it (including human errors);
- a description of the consequences and likelihood of the event;
- consideration of conditions such as normal operation, start-up, shutdown, maintenance, process upset, emergency shutdown;
- the determination of requirements for additional risk reduction necessary to achieve the required safety;
- a description of, or references to information on, the measures taken to reduce or remove hazards and risk;

- a detailed description of the assumptions made during the analysis of the risks including probable demand rates and equipment failure rates, and of any credit taken for operational constraints or human intervention;
- allocation of the safety functions to layers of protection (see Clause 9) taking account of potential reduction in effective protection due to common cause failure between the safety layers and between the safety layers and the BPCS (see note 1);
- identification of those safety function(s) applied as safety instrumented function(s) (see Clause 9).

Anhang – IEC 61511-1 Prozess Industrie

9.3.2 A safety instrumented function of safety integrity level 4 shall be permitted only if the criteria in either a), or both b) and c) below are met.

a) There has been an explicit demonstration, by a combination of appropriate analytical methods and testing, of the target safety integrity failure measure having been met.

b) There has been extensive operating experience of the components used as part of the safety instrumented function.

NOTE Such experience should have been gained in a similar environment and, as a minimum, components should have been used in a system of comparable complexity level.

c) There is sufficient hardware failure data, obtained from components used as part of the safety instrumented function, to allow sufficient confidence in the hardware safety integrity target failure measure that is to be claimed.

NOTE The data should be relevant to the proposed environment, application and complexity level.

Anhang – IEC 61511-1 Prozess Industrie

9.5 Requirements for preventing common cause, common mode and dependent failures

9.5.1 The design of the protection layers shall be assessed to ensure that the likelihood of common cause, common mode and dependent failures between protection layers and between protection layers and the BPCS are sufficiently low in comparison to the overall safety integrity requirements of the protection layers. The assessment may be qualitative or quantitative.

9.5.2 The assessment shall consider the following:

- independency between protection layers;
- diversity between protection layers;
- physical separation between different protection layers;
- common cause failures between protection layers and between protection layers and BPCS (for example, can plugging of relief valves cause the same problems as plugging of sensors in a SIS?).

BPCS: Basic Process Control System

SIS: Safety Instrumented System