DIN EN 61508-5 (VDE 0803-5)

DIN

Diese Norm ist zugleich eine **VDE-Bestimmung** im Sinne von VDE 0022. Sie ist nach Durchführung des vom VDE-Präsidium beschlossenen Genehmigungsverfahrens unter der oben angeführten Nummer in das VDE-Vorschriftenwerk aufgenommen und in der „etz Elektrotechnik + Automation" bekannt gegeben worden.

VDE

ICS 35.240.50

Einsprüche bis 2009-08-31

Vorgesehen als Ersatz für DIN EN 61508-5 (VDE 0803-5):2002-11

Entwurf

Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 5: Beispiele von Methoden für die Bestimmung von Sicherheits-Integritätslevein (IEC 65A/526/CDV:2008); Deutsche Fassung FprEN 61508-5:2008

Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 5: Examples of methods for the determination of safety integrity levels (IEC 65A/526/CDV:2008); German version FprEN 61508-5:2008

Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité – Partie 5 : Exemples de méthodes pour la détermination des niveaux d'intégrité de sécurité (CEI 65A/526/CDV:2008); Version allemande FprEN 61508-5:2008

Anwendungswarnvermerk

Dieser Norm-Entwurf mit Erscheinungsdatum 2009-06-08 wird der Öffentlichkeit zur Prüfung und Stellungnahme vorgelegt.

Weil die beabsichtigte Norm von der vorliegenden Fassung abweichen kann, ist die Anwendung dieses Entwurfes besonders zu vereinbaren.

Stellungnahmen werden erbeten

- vorzugsweise als Datei per E-Mail an **dke@vde.com** in Form einer Tabelle. Die Vorlage dieser Tabelle kann im Internet unter **www.dke.de/stellungnahme** abgerufen werden
- oder in Papierform an die DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE, Stresemannallee 15, 60596 Frankfurt am Main.

Die Empfänger dieses Norm-Entwurfs werden gebeten, mit ihren Kommentaren jegliche relevante Patentrechte, die sie kennen, mitzuteilen und unterstützende Dokumentationen zur Verfügung zu stellen.

Gesamtumfang 93 Seiten

DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE

Preisgr. 13 K
VDE-Vertr.-Nr. 1803010

Einzelverkauf und Abonnements durch VDE VERLAG GMBH, 10625 Berlin

Einzelverkauf auch durch Beuth Verlag GmbH, 10772 Berlin

Beginn der Gültigkeit

Diese Norm gilt ab ...

Nationales Vorwort

Die Deutsche Fassung des europäischen Dokuments FprEN 61508-5:2008 „Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 5: Beispiele von Methoden für die Bestimmung von Sicherheits-Integritätslevein" (Entwurf in der Umfrage) ist unverändert in diesen Norm-Entwurf übernommen worden.

Die Internationale Elektrotechnische Kommission (IEC) und das Europäische Komitee für Elektrotechnische Normung (CENELEC) haben vereinbart, dass ein auf IEC-Ebene erarbeiteter Entwurf für eine Internationale Norm zeitgleich (parallel) bei IEC und CENELEC zur Umfrage (CDV-Stadium) und Abstimmung als FDIS (en: Final Draft International Standard) bzw. Schluss-Entwurf für eine Europäische Norm gestellt wird, um eine Beschleunigung und Straffung der Normungsarbeit zu erreichen. Dem entsprechend ist das internationale Dokument IEC 65A/526/CDV:2008 „Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 5: Examples of methods for the determination of safety integrity levels" unverändert in den Entwurf FprEN 61508-5:2008 übernommen worden.

Da die Deutsche Fassung noch nicht endgültig mit der Englischen und Französischen Fassung abgeglichen ist, ist die englische Originalfassung des IEC-CDV entsprechend der diesbezüglich durch die IEC erteilten Erlaubnis beigefügt. Die Nutzungsbedingungen für den deutschen Text des Norm-Entwurfes gelten gleichermaßen auch für den englischen IEC-Text.

Das internationale Dokument wurde vom SC 65A „System aspects" der Internationalen Elektrotechnischen Kommission (IEC) erarbeitet.

Bei der Abstimmung zu dem Europäischen Schluss-Entwurf bei CENELEC und dem Internationalen Schluss-Entwurf bei IEC [Final Draft International Standard (FDIS)] sind jeweils nur „JA/NEIN"-Entscheidungen möglich, wobei „NEIN"-Entscheidungen fundiert begründet werden müssen. Dokumente, die bei CENELEC als Europäische Norm angenommen und ratifiziert werden, sind unverändert als Deutsche Normen zu übernehmen.

Für diesen Norm-Entwurf ist das nationale Arbeitsgremium GK 914 „Funktionale Sicherheit elektrischer, elektronischer und programmierbarer elektronischer Systeme (E, E, PES) zum Schutz von Personen und Umwelt" der DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE (www.dke.de) zuständig.

Änderungen

Gegenüber DIN EN 61508-5 (VDE 0803-5):2002-11 wurden folgende Änderungen vorgenommen:

a) vertiefte Diskussion der Risiken in Anhang A;

b) Hinzufügung eines neuen Anhanges B zur Auswahl der Methoden zur Bestimmung der Sicherheits-Integritätslevel;

c) Aufnahme der Beschreibung der Methode der Analyse der Schutzebenen (LOPA).

Nationaler Anhang NA
(informativ)

Zusammenhang mit Europäischen und Internationalen Normen

Für den Fall einer undatierten Verweisung im normativen Text (Verweisung auf eine Norm ohne Angabe des Ausgabedatums und ohne Hinweis auf eine Abschnittsnummer, eine Tabelle, ein Bild usw.) bezieht sich die Verweisung auf die jeweils neueste gültige Ausgabe der in Bezug genommenen Norm.

Für den Fall einer datierten Verweisung im normativen Text bezieht sich die Verweisung immer auf die in Bezug genommene Ausgabe der Norm.

Eine Information über den Zusammenhang der zitierten Normen mit den entsprechenden Deutschen Normen ist in Tabelle NA.1 wiedergegeben.

Tabelle NA.1

Europäische Norm	Internationale Norm	Deutsche Norm	Klassifikation im VDE-Vorschriftenwerk
FprEN61508-1:2008	65A/522/CDV:2008	E DIN EN 61805-1 (VDE 0803-1) in Vorbereitung	(VDE 0803-1)
FprEN61508-2:2008	65A/523/CDV:2008	E DIN EN 61805-2 (VDE 0803-2) in Vorbereitung	(VDE 0803-2)
FprEN61508-3:2008	65A/524/CDV:2008	E DIN EN 61805-3 (VDE 0803-3) in Vorbereitung	(VDE 0803-3)
FprEN61508-4:2008	65A/525/CDV:2008	E DIN EN 61805-4 (VDE 0803-4) in Vorbereitung	(VDE 0803-4)
FprEN61508-6:2008	65A/527/CDV:2008	E DIN EN 61805-6 (VDE 0803-6) in Vorbereitung	(VDE 0803-6)
FprEN61508-7:2008	65A/528/CDV:2008	E DIN EN 61805-7 (VDE 0803-7) in Vorbereitung	(VDE 0803-7)
–	ISO/IEC Guide 51:1990	–	–
–	IEC Guide 104:1997	–	–

Nationaler Anhang NB
(informativ)

Literaturhinweise

E DIN EN 61805-1 (VDE 0803-1), *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme –Teil 1: Allgemeine Anforderungen*

E DIN EN 61805-2 (VDE 0803-2), *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 2: Anforderungen an sicherheitsbezogene elektrische/elektronische/programmierbare elektronische Systeme*

E DIN EN 61805-3 (VDE 0803-3), *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 3: Anforderungen an Software*

E DIN EN 61805-4 (VDE 0803-4), *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 4: Begriffe und Abkürzungen*

E DIN EN 61805-6 (VDE 0803-6), *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 6: Anwendungsrichtlinie für IEC 61508-2 und IEC 61508-3*

E DIN EN 61805-7 (VDE 0803-7), *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme –Teil 7: Anwendungshinweise über Verfahren und Maßnahmen*

Deutsche Fassung

Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme –
Teil 5: Beispiele von Methoden für die Bestimmung von Sicherheits-Integritätslevein

Inhalt

Seite

Einleitung ... 4
2 Normative Verweisungen ... 8
3 Begriffe und Abkürzungen ... 8
Anhang A (informativ) Risiko und Sicherheitsintegrität – Allgemeine Konzepte ... 9
A.1 Allgemeines ... 9
A.2 Notwendige Risikominderung ... 9
A.2.1 Individuelles Risiko ... 10
A.2.2 Gesellschaftliche Risiken ... 10
A.2.3 Kontinuierliche Verbesserung ... 10
A.2.4 Risikoprofil ... 11
A.3 Die Rolle der sicherheitsbezogenen E/E/PE-Systeme ... 11
A.4 Sicherheitsintegrität ... 11
A.5 Betriebsarten und Bestimmung des SIL ... 12
A.5.1 Sicherheitsintegrität und Risikominderung für Anwendungen mit niedriger Anforderungsrate ... 12
A.5.2 Sicherheitsintegrität für Anwendungen in der Betriebsart mit hoher Anforderungsrate ... 14
A.5.3 Sicherheitsintegrität für Anwendungen in der Betriebsart mit kontinuierlicher Anforderung ... 15
A.5.4 Ausfälle infolge gemeinsamer und abhängiger Ursache ... 16
A.5.5 Sicherheits-Integritätslevel, bei Verwendung mehrerer Schichten eines Schutzes ... 17
A.6 Risiko und Sicherheitsintegrität ... 18
A.7 Sicherheits-Integritätslevel und Software-Sicherheits-Integritätslevel ... 18
A.8 Zuordnung von Sicherheitsanforderungen ... 19
A.9 Systeme zur Schadensbegrenzung ... 21
Anhang B (informativ) Auswahl von Methoden zur Bestimmung der Sicherheits-Integritätslevel ... 22
B.1 Allgemeines ... 22
B.2 Quantitative Methode der SIL-Bestimmung ... 22
B.3 Die Risikograph-Methode ... 23
B.4 Analyse der Schutzebenen (en.: Layer of Protection Analysis (LOPA)) ... 23
Anhang C (informativ) Konzepte für ALARP und tolerierbares Risiko ... 25
C.1 Allgemeines ... 25
C.2 ALARP-Modell ... 25
C.2.1 Einleitung ... 25

Seite
C.2.2 Grenzwert für das tolerierbare Risiko ... 26
Anhang D (informativ) Festlegung der Sicherheits-Integritätslevel: Eine quantitative Methode ... 28
D.1 Allgemeines ... 28
D.2 Allgemeine Methode ... 28
D.3 Beispielrechnung ... 29
Anhang E (informativ) Bestimmung der Sicherheits-Integritätslevel Risikograph-Methoden ... 31
E.1 Allgemeines ... 31
E.2 Aufbau des Risikographen ... 31
E.3 Kalibrierung ... 32
E.4 Mögliche andere Risikoparameter ... 33
E.5 Anwendung des Risikographen: allgemeines Schema ... 33
E.6 Beispiel eines Risikographen ... 34
Anhang F (informativ) Semi-quantitative Methode, Verwendung einer Analyse der Schutzebenen (LOPA) ... 38
F.1 Allgemeines ... 38
F.1.1 Beschreibung ... 38
F.1.2 Anhang Verweis ... 38
F.1.3 Beschreibung der Methode ... 38
F.2 Schadensereignis ... 38
F.3 Schweregrad ... 38
F.4 Auslösende Ursache ... 39
F.5 Eintrittswahrscheinlichkeit ... 39
F.6 Schutzebenen (PLs) ... 42
F.6.1 Allgemeines ... 42
F.6.2 Grundlegendes Steuerungssystem ... 42
F.6.3 Alarme ... 42
F.7 Zusätzliche Schadensbegrenzungsmaßnahmen ... 43
F.8 Vorläufige Wahrscheinlichkeit für das Ereignis ... 43
F.9 Sicherheits-Integritätslevel (SILs) ... 43
Anhang G (informativ) Festlegung der Sicherheits-Integritätslevel – Eine qualitative Vorgehensweise: Matrix des Ausmaßes des gefährlichen Vorfalls ... 45
Anhang G (informativ) Festlegung der Sicherheits-Integritätslevel – Eine qualitative Vorgehensweise: Matrix des Ausmaßes des gefährlichen Vorfalls ... 45
G.1 Allgemeines ... 45
G.2 Matrix des Ausmaßes des gefährlichen Vorfalls ... 45
Literaturhinweise ... 47

Bilder

Bild 1 – Gesamtrahmen der Betrachtung dieser Norm ... 7
Bild A.1 – Risikominderung: allgemeine Konzepte (Betriebsart mit niedriger Anforderungsrate) ... 13
Bild A.2 – Risiko- und Sicherheitsintegritätskonzepte ... 13

Seite

Bild A.3 – Risikodarstellung zu Anwendungen mit hoher Anforderungsrate 15
Bild A.4 – Risikodarstellung zu Anwendungen mit kontinuierlichen Anforderungsrate 16
Bild A.5 – Darstellung von Ausfällen infolge gemeinsamer Ursache (CCFs) von Elementen im EUC-Leit- oder Steuerungssystem und Elementen im sicherheitsbezogenen E/E/PE-System 17
Bild A.6 – Gemeinsame Ursache zwischen zwei sicherheitsbezogenen E/E/PE-Systemen 18
Bild A.7 – Zuordnung der Sicherheitsanforderungen zu den sicherheitsbezogenen E/E/PE-Systemen, sicherheitsbezogenen Systemen anderer Technologie und externen Einrichtungen zur Risikominderung 20
Bild C.1 – Tolerierbares Risiko und ALARP 26
Bild D.1 – Zuordnung der Sicherheitsintegrität: Beispiel für eine sicherheitsbezogene Schutzeinrichtung 30
Bild E.1 – Risikograph: Allgemeine Darstellung 34
Bild E.2 – Risikograph: Beispiel (zeigt nur allgemeine Prinzipien auf) 34
Bild G.1 – Matrix des Ausmaßes des gefährlichen Vorfalls: Beispiel (stellt nur die allgemeinen Prinzipien dar) 46

Tabellen

Tabelle C.1 – Beispiel für die Risikoklassifizierung von Unfällen 27
Tabelle C.2 – Interpretation der Risikoklassen 27
Tabelle E.1 – Beispieldaten, die sich auf das Beispiel des Risikographen (Bild E.2) beziehen 35
Tabelle E.2 – Beispielkalibrierung eines allgemeinen Risikographen 36

Einleitung

Systeme, die aus elektrischen und/oder elektronischen Elementen bestehen, werden seit vielen Jahren verwendet, um Sicherheitsfunktionen in vielen Anwendungsbereichen auszuführen. Auf Rechnern basierende Systeme (allgemein ausgedrückt programmierbare elektronische Systeme) werden in allen Anwendungsbereichen benutzt, um Nichtsicherheitsfunktionen und zunehmend auch um Sicherheitsfunktionen auszuführen. Falls Rechnersystemtechnologie wirksam und sicherheitsgerichtet eingesetzt wird, ist es wichtig, dass die für die Entscheidungsfindung Verantwortlichen ausreichende Hilfestellung bezüglich der Sicherheitsaspekte erhalten, nach denen diese Entscheidungen getroffen werden.

Diese Internationale Norm beschreibt einen allgemeinen Lösungsweg für alle Tätigkeiten während des Sicherheitslebenszyklus für Systeme, die aus elektrischen und/oder elektronischen und/oder programmierbar elektronischen Elementen bestehen (E/E/PE) die eingesetzt werden, um Sicherheitsfunktionen auszuführen. Dieser allgemeine Lösungsweg wurde gewählt, um ein sinnvolles und konsistentes technisches Verfahren für alle elektrischen Sicherheitssysteme zu entwickeln. Ein Hauptziel ist es, die Entwicklung von anwendungsspezifischen Normen zu erleichtern.

In den meisten Situationen wird Sicherheit durch eine Anzahl von Systemen erreicht, die auf vielerlei Technologien (zum Beispiel Mechanik, Hydraulik, Pneumatik, Elektrik, Elektronik, programmierbare Elektronik) basieren. Jede Sicherheitsstrategie muss deshalb nicht nur alle Elemente innerhalb eines Einzelsystems (zum Beispiel Sensoren, Steuereinheiten und Aktoren) betrachten, sondern auch all die sicherheitsbezogenen Systeme, die einzelne Teile einer Gesamtheit sind. Da sich diese Internationale Norm mit sicherheitsbezogenen (E/E/PE) Systemen beschäftigt, kann sie einen Rahmen bereitstellen, innerhalb dessen sicherheitsbezogene Systeme, basierend auf anderen Technologien, betrachtet werden können.

Es ist berücksichtigt worden, dass eine große Vielfalt von Anwendungen, sicherheitsbezogener E/E/PE-Systeme in vielfältigen Anwendungsbereichen verwendet und diese einen weiten Bereich in Bezug auf Komplexität, Gefährdungs- und Risikopotentiale abdeckt. In jeder speziellen Anwendung hängen die erforderlichen Sicherheitsmaßnahmen von vielen anwendungsspezifischen Faktoren ab. Dadurch, dass diese Internationale Norm allgemein gehalten ist, wird die Formulierung solcher Maßnahmen in zukünftigen und in Revisionen bereits existierender, anwendungsspezifischer Internationaler Normen, ermöglicht.

Diese Internationale Norm

- betrachtet alle relevanten Phasen des Gesamt-Sicherheitslebenszyklus, des Sicherheitslebenszyklus des E/E/PE-Systems und des Software-Sicherheitslebenszyklus (zum Beispiel vom anfänglichen Konzept über Entwurf, Implementierung, Betrieb und Instandhaltung bis zur Außerbetriebnahme), wenn E/E/PE-Systeme benutzt werden, um Sicherheitsfunktionen auszuführen;
- wurde unter Berücksichtigung einer sich schnell entwickelnden Technologie entworfen. Der Betrachtungsrahmen ist ausreichend robust und ausführlich genug, um auch für zukünftige Entwicklungen verwendbar zu sein;
- ermöglicht die Erstellung anwendungsspezifischer Internationaler Normen, die sich mit sicherheitsbezogenen E/E/PE-Systemen befassen. Die Entwicklung anwendungsspezifischer Normen sollte innerhalb des Rahmens dieser Internationalen Norm zu einem hohen Grad an Übereinstimmung (zum Beispiel von zugrunde liegenden Prinzipien, Terminologie usw.) führen, sowohl innerhalb der Anwendungsbereiche als auch über die Anwendungsbereiche hinweg. Dies hat sowohl sicherheitstechnische als auch wirtschaftliche Vorteile;

ANMERKUNG 1 Hinweise [1] und [2] in den Literaturhinweisen sind anwendungsspezifische internationale Normen.

- liefert eine Methode für die Entwicklung der Spezifikation der Sicherheitsanforderungen, die notwendig ist, um die erforderliche funktionale Sicherheit für sicherheitsbezogene E/E/PE-Systeme zu erreichen;
- verwendet einen auf dem Risiko basierenden Lösungsansatz, durch den die Anforderungen zum Sicherheits-Integritätslevel bestimmt werden können;
- führt Sicherheits-Integritätslevels für die Spezifikation der Zielvorgabe der Sicherheitsintegrität der Sicherheitsfunktionen ein, die in dem sicherheitsbezogenen E/E/PE-System implementiert werden;

ANMERKUNG 2 Diese Norm legt weder die Anforderungen zur Sicherheitsintegrität für irgendeine Sicherheitsfunktion fest, noch bestimmt sie, wie der Sicherheits-Integritätslevel festgelegt wird. Stattdessen stellt sie einen risikobasierenden konzeptionellen Rahmen und Beispielverfahren bereit.

- legt Ausfallgrenzwerte für die von den sicherheitsbezogenen E/E/PE-Systemen auszuführenden Sicherheitsfunktionen fest, die mit den Sicherheits-Integritätsleveln verbunden sind;
- legt eine untere Grenze für die Ausfallgrenzwerte für eine Sicherheitsfunktion fest, die von einem einzelnen sicherheitsbezogenen E/E/PE-System ausgeführt wird. Für sicherheitsbezogene E/E/PE-Systeme, die
  - in der Betriebsart mit einer niedrigen Anforderungsrate betrieben werden, ist die untere Grenze bei einer mittleren Wahrscheinlichkeit eines gefahrbringenden Ausfalls bei Anforderung von 10^{-5} festgelegt,
  - in der Betriebsart mit einer hohen oder ununterbrochenen Anforderungsrate betrieben werden, ist die untere Grenze der Wahrscheinlichkeit eines gefahrbringenden Ausfalls auf 10^{-9} [h^{-1}] pro Stunde festgelegt;

ANMERKUNG 3 Ein einzelnes sicherheitsbezogenes E/E/PE-System bedeutet nicht auch notwendigerweise eine einkanalige Architektur.

ANMERKUNG 4 Es kann für einfache Systeme möglich sein, Entwürfe von sicherheitsbezogenen Systemen mit niedrigeren Zielwerten für die Sicherheitsintegrität zu erreichen, aber diese Grenzen werden als das betrachtet, was für relativ komplexe Systeme (zum Beispiel sicherheitsbezogene programmierbare elektronische Systeme) gegenwärtig erreicht werden kann.

- legt Anforderungen für die Vermeidung und Beherrschung von systematischen Fehlern fest, die auf Erfahrung und Urteilsvermögen beruhen, das durch praktische Erfahrung in der Industrie gewonnen wurde. Wenn auch die Wahrscheinlichkeit des Auftretens systematischer Ausfälle im Allgemeinen nicht quantifiziert werden kann, erlaubt die Norm jedoch für eine festgelegte Sicherheitsfunktion den Anspruch zu erheben, dass der mit der Sicherheitsfunktion verbundene Ausfallgrenzwert als erreicht betrachtet werden kann, wenn alle Anforderungen dieser Norm erfüllt worden sind;
- lässt einen weiten Bereich von Prinzipien, Verfahren und Maßnahmen zu, um funktionale Sicherheit für sicherheitsbezogene E/E/PE-Systeme zu erreichen, verwendet aber nicht das Fail-Safe-Konzept, das genutzt werden kann, wenn das Ausfallverhalten eindeutig definiert und das Niveau der Komplexität verhältnismäßig niedrig ist. Das Fail-Safe-Konzept wurde wegen des weiten Bereiches der Komplexität von sicherheitsbezogenen E/E/PE-Systemen, die im Rahmen der Norm behandelt werden, als ungeeignet betrachtet.

1 Anwendungsbereich

1.1 Dieser Teil der IEC 61508 liefert Informationen über

- die zugrunde liegenden Konzepte des Risikos und den Zusammenhang zwischen Risiko und Sicherheitsintegrität (siehe Anhang A);
- eine Anzahl von Methoden, die es ermöglichen den Sicherheits-Integritätslevel für die sicherheitsbezogenen E/E/PE-Systeme, zur Risikominderung festzulegen (siehe Anhänge B, C, D und E).

Die ausgewählte Methode hängt vom Anwendungsgebiet und den betrachteten besonderen Umständen ab. Die Anhänge B, C, D und E erläutern quantitative und qualitative Verfahren und wurden vereinfacht, um die zugrunde gelegten Prinzipien zu erläutern. Diese Anhänge wurden aufgenommen, um die allgemeinen Prinzipien einer Anzahl von Methoden aufzuzeigen, aber sie liefern keine endgültige Darstellung. Diejenigen, die die Anwendung der in den Anhängen aufgeführten Methoden beabsichtigen, sollten das angegebene Quellenmaterial zu Rate ziehen.

ANMERKUNG Für weitere Informationen bezüglich der in den Anhängen B und E dargestellten Vorgehensweisen siehe die Verweise [2] und [5] in den Literaturhinweisen. Siehe ebenfalls den Verweis [3] in den Literaturhinweisen zur Beschreibung einer zusätzlichen Vorgehensweise.

1.2 Die Teile 1, 2, 3 und 4 dieser Norm sind Sicherheits-Grundnormen, dieser Status ist aber im Zusammenhang mit einfachen sicherheitsbezogenen E/E/PE-Systemen nicht anwendbar (siehe 3.4.4 von Teil 4). Als Sicherheits-Grundnormen sind sie zur Verwendung durch technische Komitees bei der Erstellung von Normen nach *IEC Guide 104* und *ISO/IEC Guide 51* vorgesehen. Die IEC 61508 ist ebenfalls zur Verwendung als eigenständige Norm vorgesehen. Die horizontale Sicherheitsfunktion dieser internationalen Norm ist nicht anwendbar auf medizinische Einrichtungen nach der IEC 60601 Serie

1.3 Es steht in der Verantwortlichkeit eines Technischen Komitees, zur Vorbereitung und Erstellung eigener Festlegungen soweit wie möglich die Sicherheits-Grundnormen anzuwenden. In diesem Zusammenhang gilt, dass die Anforderungen, Prüfverfahren oder Prüfbedingungen dieser Sicherheits-Grundnorm nur dann anwendbar sind, wenn in den Festlegungen der Technischen Komitees darauf verwiesen wird oder diese eingebunden werden.

1.4 Bild 1 zeigt den gesamten Rahmen für die Teile 1 bis 7 der IEC 61508 und zeigt die Rolle, die IEC 61508-4 zum Erreichen der funktionalen Sicherheit der sicherheitsbezogenen E/E/PE-Systeme spielt.

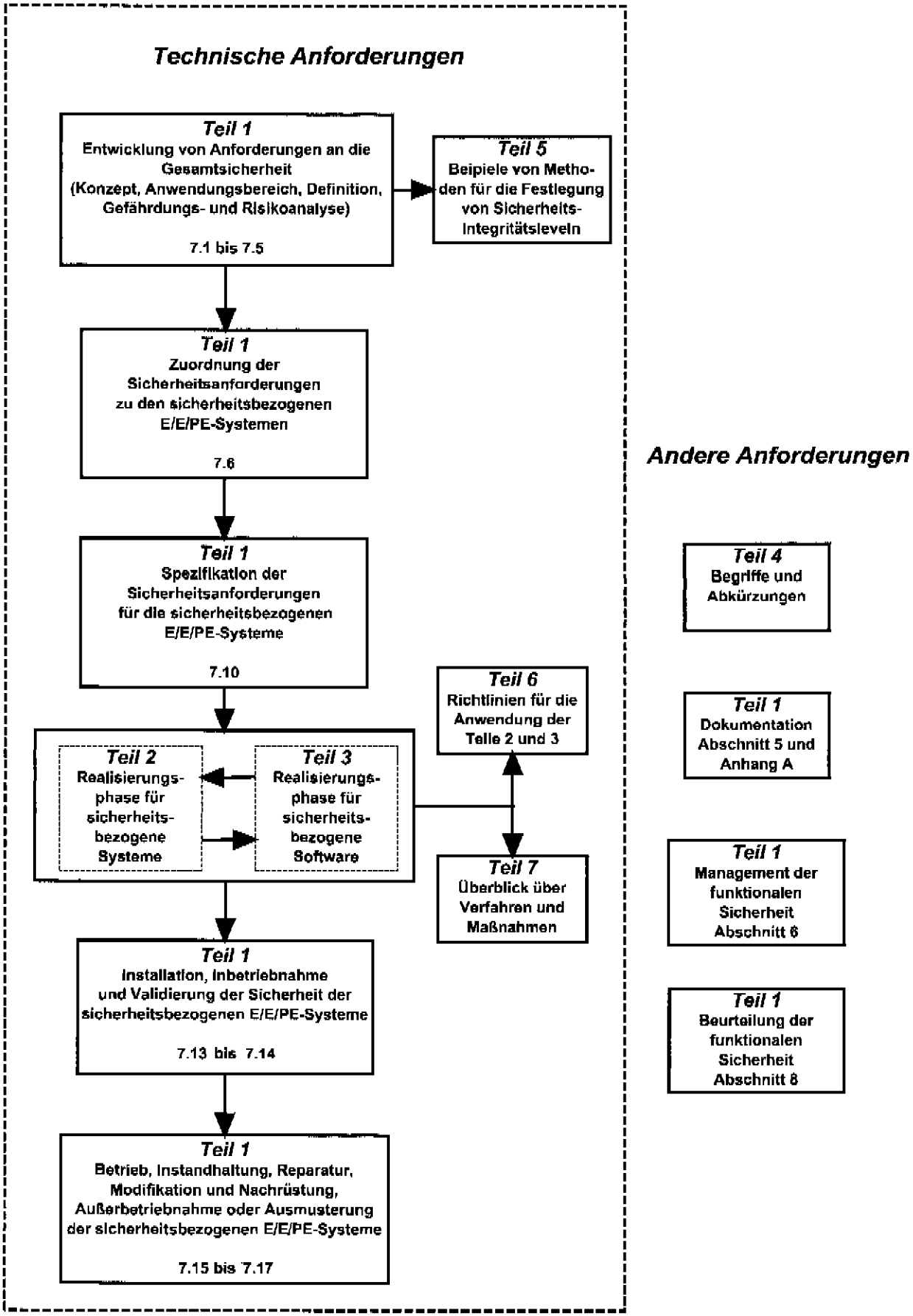


Bild 1 – Gesamtrahmen der Betrachtung dieser Norm

2 Normative Verweisungen

Die folgenden zitierten Dokumente sind für die Anwendung dieses Dokuments erforderlich. Bei datierten Verweisungen gilt nur die in Bezug genommene Ausgabe. Bei undatierten Verweisungen gilt die letzte Ausgabe des in Bezug genommenen Dokuments (einschließlich aller Änderungen).

IEC 61508-1:1998, *Functional safety of electrical/electronical/programmable electronic safety-related systems – Part 1: General requirements*

IEC 61508-2, *Functional safety of electrical/electronical/programmable electronic safety-related systems – Part 2: Requirements for electrical/electronical/programmable electronic safety-related systems*

IEC 61508-3:1998, *Functional safety of electrical/electronical/programmable electronic safety-related systems – Part 3: Software requirements*

IEC 61508-4:1998, *Functional safety of electrical/electronical/programmable electronic safety-related systems – Part 4: Definitions and abbreviations of terms*

IEC 61508-6, *Functional safety of electrical/electronical/programmable electronic safety-related systems – Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3*

IEC 61508-7, *Functional safety of electrical/electronical/programmable electronic safety-related systems – Part 7: Overview of techniques and measures*

ISO/IEC Guide 51:1990, *Guidelines for the inclusion of safety aspects in standards*

IEC Guide 104:1997, *Guide to the drafting of safety standards, and the role of Committees with safety pilot functions and safety group functions*

3 Begriffe und Abkürzungen

Für die Anwendung dieser Norm gelten die in IEC 61508-4 aufgeführten Begriffe und Abkürzungen.

Anhang A
(informativ)

Risiko und Sicherheitsintegrität – Allgemeine Konzepte

A.1 Allgemeines

Dieser Anhang liefert Informationen über die zugrunde liegenden Konzepte des Risikos und den Zusammenhang zwischen Risiko und Sicherheitsintegrität.

A.2 Notwendige Risikominderung

Die notwendige Risikominderung (siehe 3.5.14 der IEC 61508-4) ist die Minderung des Risikos, die erreicht werden muss, um das tolerierbare Risiko für eine bestimmte Situation zu erreichen (welches entweder qualitativ[1)] oder quantitativ[2)] angegeben werden darf). Das Konzept der notwendigen Risikominderung ist für die Entwicklung der Spezifikation der Sicherheitsanforderungen für die sicherheitsbezogenen E/E/PE-Systeme von grundlegender Bedeutung (insbesondere der Teil der Anforderungen zur Sicherheitsintegrität in der Spezifikation der Sicherheitsanforderungen). Der Zweck der Festlegung des tolerierbaren Risikos für einen bestimmten gefährlichen Vorfalls ist es darzulegen, was im Hinblick sowohl auf die Häufigkeit (oder Wahrscheinlichkeit) des gefährlichen Vorfalls als auch auf seine besonderen Auswirkungen für sinnvoll gehalten wird. Sicherheitsbezogene Systeme werden entworfen, um die Häufigkeit (oder Wahrscheinlichkeit) des gefährlichen Vorfalls und/oder die Auswirkungen des gefährlichen Vorfalls zu mindern.

Das tolerierbare Risiko hängt von vielen Faktoren ab (zum Beispiel der Schwere der Verletzung, der Anzahl der Personen, die einer Gefahr ausgesetzt sind, der Häufigkeit, mit der eine Person oder Personen einer Gefahr ausgesetzt sind und der Dauer der Einwirkung). Wichtige Faktoren werden die Empfindung und die Ansichten derjenigen sein, die dem gefährlichen Vorfall ausgesetzt sind. Zur Festlegung des tolerierbaren Risikos einer bestimmten Anwendung werden die folgenden Punkte betrachtet:

- gesetzliche Anforderungen, sowohl allgemeine als auch diejenigen, die sich direkt auf die spezifische Anwendung beziehen;
- Leitfäden der entsprechenden Behörden, die Sicherheitsregeln erstellen;
- Diskussionen und Übereinkünfte mit den verschiedenen Parteien, die an der Anwendung beteiligt sind;
- Industrienormen und -leitfäden;
- internationale Diskussionen und Übereinkünfte; die Rolle nationaler und Internationaler Normen gewinnt zunehmend an Wichtigkeit, um die Kriterien für das tolerierbare Risiko bei bestimmten Anwendungen festzulegen;
- die bestmögliche unabhängige industrielle, expertengestützte und wissenschaftliche Unterstützung durch Beratungsinstitutionen.

Bei der Bestimmung der notwendigen Anforderungen zur Sicherheitsintegrität der sicherheitsbezogenen E/E/PE-Systeme und andere Maßnahmen zur Risikominderung, sind im Hinblick auf die Erfüllung der tolerierten Häufigkeit eines gefährlichen Ereignisses, die Merkmale der Gefahr der einschlägigen Anwendung zu berücksichtigen. Die tolerierte Häufigkeit wird von den rechtlichen Anforderungen in dem Land der Anwendung und von den spezifizierten Kriterien durch Anwender-Organisationen, abhängen. Fragen, die berücksichtigt werden müssen zusammen mit, wie sie auf die sicherheitsbezogenen E/E/PE-Systeme anzuwenden sind, werden im Folgenden erörtert.

---

1) Um das tolerierbare Risiko zu erreichen, ist es erforderlich, die notwendige Risikominderung festzusetzen. Die Anhänge E und G der IEC 61508-5 skizzieren qualitative Methoden. Obwohl in den Beispielen zitiert ist die notwendige Risikominderung implizit durch die Angabe der SIL Anforderung nicht ausdrücklich durch einen numerischen Wert von risikomindernden Maßnahmen erforderlich.

2) Zum Beispiel, dass der gefährliche Vorfall, der zu einer bestimmten Auswirkung führt, nicht mit einer Häufigkeit von mehr als einmal in 10^8 Stunden auftreten darf.

A.2.1 Individuelles Risiko

Es werden in der Regel verschiedene Ziele für Beschäftigte und Personen im öffentlichen Bereich definiert. Die Zielvorgabe für das individuelle Risiko für die Beschäftigten bezieht sich auf die am höchsten gefährdete Person und kann ausgedrückt werden als das gesamte Risiko pro Jahr das sich bildet aus allen Tätigkeiten. Das Ziel ist auf eine hypothetische Person ausgelegt und muss daher den Anteil der Zeit berücksichtigen, den die einzelne Person bei der Arbeit verbringt. Dieses Ziel gilt für alle Risiken der gefährdeten Person und das Grenzrisiko für eine einzelne Sicherheitsfunktion muss andere Risiken mit berücksichtigen.

Vertrauen, dass das gesamte Risiko unter ein bestimmtes Ziel reduziert wurde, kann erreicht werden durch eine Reihe von Möglichkeiten. Eine Methode besteht darin alle Risiken in Betracht zu ziehen, und die Summe aller Risiken für die am stärksten exponierte Person zu bilden. Dies kann beispielsweise in Fällen in denen eine Person vielen Risiken ausgesetzt ist schwierig werden. Hier sind rechtzeitige Entscheidungen für die Systementwicklung notwendig. Ein alternativer Ansatz ist einen bestimmten Prozentsatz des gesamten individuellen Ziel-Risikos jeder einzelnen betrachteten Sicherheitsfunktion zuzuordnen. Der zugeordnete Anteil kann in der Regel bestimmt werden aus früheren Erfahrungen mit der Art der betrachteten Anlage.

Das Ziel für eine individuelle Sicherheitsfunktion sollte auch den Konservatismus der verwendeten Methode der Risikoanalyse berücksichtigen. Alle qualitativen Methoden wie Risikographen, beinhalten einige Bewertungen kritischer Parameter die zu einem Risiko beitragen. Faktoren, die zu Risiken beitragen sind die Auswirkung des gefährlichen Vorfalls und seine Häufigkeit. Bei der Festlegung dieser Faktoren kann es nötig sein eine Reihe von Risiko-Parametern zu berücksichtigen, wie eine Anfälligkeit für einen gefährlichen Vorfall, die Anzahl der Personen die möglicherweise durch den gefährlichen Vorfall betroffen sind (d. h. Nutzungsart) und die Wahrscheinlichkeit der Vermeidung des gefährlichen Vorfalls.

Qualitative Methoden beinhalten allgemein die Entscheidung, ob ein Parameter sich innerhalb einer bestimmten Bandbreite bewegt. Die Beschreibungen der Kriterien bei der Verwendung dieser Methoden benötigen ein hohes Maß an Vertrauen, dass das Ziel für die Risiken nicht überschritten wird. Dies kann einen Einstellbereich für Grenzen aller Parameter beinhalten, so dass Anwendungen deren Parameter die Grenzbedingung einhalten, die spezifizierten Risikokriterien für die Sicherheit, erfüllen. Dieses Konzept zur Festlegung der Grenzbereiche ist sehr konservativ, denn es werden nur sehr wenige Anwendungen existieren, bei denen alle Parameter im Worst Case Bereich liegen. Das Ziel der Häufigkeit solcher Methoden kann daher höher sein als das Ziel quantitativer Methoden, es gibt ein hohes Maß an Vertrauen, dass das Gesamtrisiko aller Gefährdungen tolerierbar ist.

Wenn Personen im öffentlichen Bereich einem Risiko des Ausfalls eines sicherheitsbezogenen E/E/PE-Systems ausgesetzt sind, dann kommt in der Regel ein niedrigeres Ziel zur Anwendung.

A.2.2 Gesellschaftliche Risiken

Diese entstehen, wenn mehrere Todesfälle durch ein einzelnes Ereignis zu erwarten sind. Solche Ereignisse werden gesellschaftlich genannt, weil sie geeignet sind, eine sozialpolitische Reaktion auszulösen. Es kann bedeutende öffentliche und organisatorische Abneigung gegen die hohe Auswirkung dieser Ereignisse geben und muss in einigen Fällen berücksichtigt werden. Das Kriterium für ein gesellschaftliches Risiko wird oft ausgedrückt, als eine maximale kumulierte Häufigkeit für tödliche Verletzungen zu einer bestimmten Anzahl von Personen. Dieses Kriterium wird in der Regel in der Form einer F/N-Kurve dargestellt, wobei F die kumulative Häufigkeit einer Gefährdung und N die Anzahl der Todesfälle, die aus den Gefährdungen entstehen. Die Beziehung ist in der Regel eine gerade Linie, wenn diese auf einer logarithmischen Skala gezeichnet wird. Die Steigung der Linie wird davon abhängen, in welchem Umfang Organisationen Risiken mit höheren Auswirkungen scheuen. Die Anforderung wird sein, dass die kumulierte Häufigkeit für eine bestimmte Zahl von Todesfällen niedriger ist als die kumulierte Häufigkeit in der F/N-Kurve. (siehe Verweis [4])

A.2.3 Kontinuierliche Verbesserung

Die Grundsätze zur Verringerung des Risikos, auf einen Wert so niedrig wie vernünftiger Weise möglich, werden im Anhang C vorgestellt.

A.2.4 Risikoprofil

Bei der Entscheidung, Risikokriterien für eine bestimmte Gefährdung anzuwenden, kann es notwendig werden ein Risikoprofil über die gesamte Laufzeit der Anlage in Betracht zu ziehen. Das Restrisiko wird variieren von niedrig, nach einer Wiederholungsprüfung oder nach Durchführung einer Reparatur, bis zu einem Maximum kurz vor einer Wiederholungsprüfung. Dies sollte unter Umständen von Organisationen in Betracht gezogen werden, die die anzuwenden Risikokriterien spezifizieren. Wenn Intervalle für Wiederholungsprüfungen von Bedeutung sind, dann kann es angemessen sein, die maximale Wahrscheinlichkeit einer Gefährdung die vor einer Wiederholungsprüfung akzeptiert werden kann, zu spezifizieren. Oder die PFD (t) oder PFH (t) ist niedriger als die obere SIL-Grenze mehr als ein bestimmter Prozentsatz der Zeit (z.B. 90%).

A.3 Die Rolle der sicherheitsbezogenen E/E/PE-Systeme

Sicherheitsbezogene E/E/PE-Systeme tragen dazu bei die für das Erreichen des tolerierbaren Risikos notwendige Risikominderung zu liefern.

Ein sicherheitsbezogenes System

- beinhaltet sowohl die geforderten Sicherheitsfunktionen, die notwendig sind, einen sicheren Zustand für die EUC-Einrichtung zu erreichen oder einen sicheren Zustand für die EUC-Einrichtung aufrechtzuerhalten, und
- ist dazu vorgesehen, selbständig oder mit anderen sicherheitsbezogenen E/E/PE-Systemen, oder externen Maßnahmen zur Risikominderung die notwendige Sicherheitsintegrität für die geforderten Sicherheitsfunktionen zu erreichen (3.4.1 der IEC 61508-4).

ANMERKUNG 1 Der erste Teil der Definition gibt an, dass das sicherheitsbezogene System die Sicherheitsfunktionen ausführen muss, die in der Spezifikation der Anforderungen an die Sicherheitsfunktionen festgelegt werden. Zum Beispiel könnte die Spezifikation der Anforderungen zu den Sicherheitsfunktionen festlegen, dass bei Erreichen der Temperatur „x" das Ventil "y" öffnen muss, um eine Wasserzufuhr in einen Behälter zu ermöglichen.

ANMERKUNG 2 Der zweite Teil der Definition gibt an, dass das sicherheitsbezogene System die Sicherheitsfunktionen mit einem der Anwendung angemessenen Grad an Gewissheit ausführen muss, um das tolerierbare Risiko zu erreichen.

Eine Person kann ein integraler Bestandteil eines sicherheitsbezogenen E/E/PE-Systems sein. Eine Person könnte zum Beispiel von einer Anzeigetafel Informationen über den Zustand der EUC entgegennehmen und eine auf diesen Informationen beruhende sicherheitsgerichtete Handlung ausführen.

Sicherheitsbezogene E/E/PE-Systeme können in einer Betriebsart mit niedriger Anforderungsrate oder in einer Betriebsart mit hoher oder kontinuierlicher Anforderungsrate betrieben werden (siehe 3.5.12 der IEC 61508-4).

A.4 Sicherheitsintegrität

Sicherheitsintegrität ist definiert als die „Wahrscheinlichkeit eines sicherheitsbezogenen Systems, die geforderten Sicherheitsfunktionen unter allen festgelegten Bedingungen innerhalb eines festgelegten Zeitraumes zufrieden stellend auszuführen" (3.5.2 der IEC 61508-4). Die Sicherheitsintegrität bezieht sich auf die Leistungsfähigkeit der sicherheitsbezogenen Systeme, die Sicherheitsfunktionen auszuführen (die auszuführenden Sicherheitsfunktionen sind in der Spezifikation der Anforderungen an die Sicherheitsfunktionen festgelegt).

Die Sicherheitsintegrität setzt sich aus den folgenden beiden Elementen zusammen:

- Der Sicherheitsintegrität der Hardware; derjenige Teil der Sicherheitsintegrität, der sich auf zufällige Hardwareausfälle mit gefahrbringender Ausfallart bezieht (siehe 3.5.5 der IEC 61508-4). Das Erreichen der festgelegten Stufe der Sicherheitsintegrität der Hardware kann mit einer vernünftigen Genauigkeit abgeschätzt werden. Die Anforderungen können daher unter Verwendung der üblichen Regeln für die Kombination von Wahrscheinlichkeiten zwischen den Teilsystemen aufgeteilt werden. Zum Erreichen einer angemessenen Sicherheitsintegrität der Hardware kann die Anwendung redundanter Architekturen notwendig sein.

– Die Systematische Sicherheitsintegrität: derjenige Teil der Sicherheitsintegrität, der sich auf systematische Ausfälle mit gefahrbringender Ausfallart bezieht (siehe 3.5.4 der IEC 61508-4). Obwohl die mittlere Ausfallrate für systematische Ausfälle abgeschätzt werden kann, führen die durch Entwurfsfehler und Ausfälle infolge gemeinsamer Ursache resultierenden Ausfalldaten dazu, dass die Verteilung der Ausfälle schwer vorherzusagen ist. Dies führt zu einer zunehmenden Ungewissheit in den Berechnungen der Ausfallwahrscheinlichkeiten für eine bestimmte Situation (zum Beispiel die Wahrscheinlichkeit eines Ausfalls einer sicherheitsbezogenen Schutzeinrichtung). Daher muss eine Beurteilung der Auswahl der besten Vorgehensweisen diese Ungewissheit verringern. Es ist zu beachten, dass Maßnahmen zur Reduzierung der Wahrscheinlichkeit zufälliger Hardwareausfälle keinen Einfluss auf die Wahrscheinlichkeit eines systematischen Ausfalls haben. Methoden, wie zum Beispiel die Verwendung redundanter Kanäle mit identischer Hardware, die sehr wirksam in der Beherrschung zufälliger Hardwareausfälle sind, haben nur einen geringen Nutzen bei der Reduzierung systematischer Ausfälle wie Softwarefehler.

A.5 Betriebsarten und Bestimmung des SIL

Die Betriebsart bezieht sich auf die Art und Weise, wie eine Sicherheitsfunktion verwendet werden soll, mit Bezug auf die Häufigkeit der Anforderungen an sie, diese kann entweder mit:

– **Betriebsart mit niedriger Anforderungsrate**: Wenn die Häufigkeit der Anforderungen während des Betriebs, an die Sicherheitsfunktion nicht häufiger als einmal pro Jahr erfolgt; oder

– **Betriebsart mit hoher Anforderungsrate:** Wenn die Häufigkeit der Anforderungen während des Betriebs, an die Sicherheitsfunktion häufiger als einmal pro Jahr erfolgt; oder

– **Kontinuierliche Anforderungsrate:** Wenn die Anforderung an die Sicherheitsfunktion kontinuierlich erfolgen.

Die Tabellen 2 und 3 der IEC 61508-1 zeigen die Ausfallgrenzwerte für jede der Betriebsarten im Zusammenhang mit den vier Sicherheits-Integritätsleveln. Die Betriebsarten werden in den folgenden Abschnitten weiter beschrieben:

A.5.1 Sicherheitsintegrität und Risikominderung für Anwendungen mit niedriger Anforderungsrate

Die erforderliche Sicherheitsintegrität der sicherheitsbezogenen E/E/PE-Systeme und Maßnahmen zur Risikominderung muss auf einer solchen Stufe sein, dass sichergestellt ist, dass:

– die durchschnittliche Wahrscheinlichkeit von Ausfällen bei Anforderung der sicherheitsbezogenen Systeme ausreichend niedrig ist, um zu verhindern, dass die Häufigkeit des gefahrbringenden Vorfalls die zum Erreichen des tolerierbaren Risikos geforderte Häufigkeit überschreitet; und/oder

– die sicherheitsbezogenen Systeme die Auswirkungen eines Ausfalls in dem erforderlichen Ausmaß verändern, um das tolerierbare Risiko zu erreichen.

Bild A.1 zeigt die allgemeinen Konzepte der Risikominderung. Im allgemeinen Modell ist angenommen, dass

– eine EUC und ein Steuerungssystem vorhanden ist;

– zugehörige menschliche Faktoren vorhanden sind;

– die sicherheitsbezogenen Schutzmaßnahmen folgendes umfassen

  – sicherheitsbezogene E/E/PE-Systeme;

  – andere risikomindernde Maßnahmen.

ANMERKUNG Bild A.1 ist ein verallgemeinertes Risikomodell zur Darstellung der allgemeinen Prinzipien. Um das Risikomodell für eine bestimmte Anwendung zu entwickeln, ist es notwendig, die spezifische Art und Weise, mit der die notwendige Risikominderung durch die sicherheitsbezogenen E/E/PE-Systeme und/oder andere risikomindernden Maßnahmen erreicht wird, zu berücksichtigen. Das daraus hervorgehende Risikomodell kann daher von dem in Bild A.1 gezeigten abweichen.

Die in Bild A.1 und A.2 gezeigten unterschiedlichen Risiken sind:

– EUC-Risiko: das Risiko, das für die festgelegten gefährlichen Vorfälle der EUC, des EUC-Leit- oder Steuerungssystems und zugehöriger menschlicher Faktoren besteht; vorgesehene sicherheitsbezogene

Schutzmerkmale werden bei der Bestimmung dieses Risikos nicht berücksichtigt (siehe 3.2.4 der IEC 61508-4);

- tolerierbares Risiko: das Risiko, das in einem gegebenen Zusammenhang basierend auf den üblichen gesellschaftlichen Wertvorstellungen tragbar ist (siehe 3.1.6 der IEC 61508-4);
- Restrisiko: im Zusammenhang mit dieser Norm ist das Restrisiko das Risiko, das für die festgelegten gefährlichen Vorfälle der EUC, des EUC-Leit- oder Steuerungssystems und zugehöriger menschlicher Faktoren verbleibt, jedoch unter Berücksichtigung der sicherheitsbezogenen E/E/PE-Systeme und anderer risikomindernden Maßnahmen (siehe auch 3.1.7 der IEC 61508-4).

Das EUC-Risiko ist eine Funktion des zur EUC selbst zugehörigen Risikos, jedoch unter Berücksichtigung der durch das EUC-Leit- oder Steuerungssystem erreichten Risikominderung. Um ungerechtfertigte Anforderungen an die Sicherheitsintegrität des EUC-Leit- oder Steuerungssystems zu verhindern, legt diese Norm Beschränkungen für die Anforderungen, die gestellt werden können, fest (siehe 7.5.2.5 der IEC 61508-1).

Die notwendige Risikominderung wird durch eine Kombination aller sicherheitsbezogenen Schutzmerkmale erreicht. Die Risikominderung, die vom Ausgangspunkt des EUC-Risikos aus notwendig ist, um das tolerierbare Risiko zu erreichen, ist in Bild A.1 gezeigt (wichtig für eine Sicherheitsfunktion die in der Betriebsart mit niedriger Anforderungsrate arbeitet).

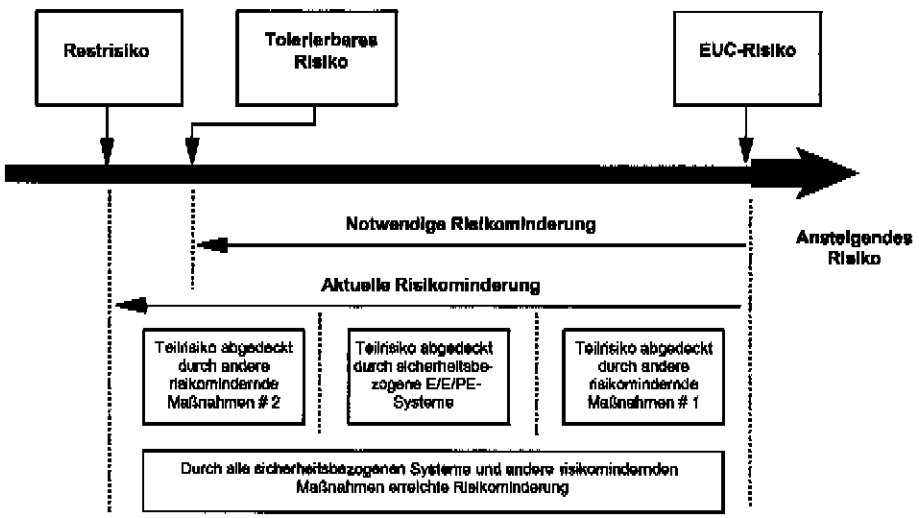


Bild A.1 – Risikominderung: allgemeine Konzepte (Betriebsart mit niedriger Anforderungsrate)

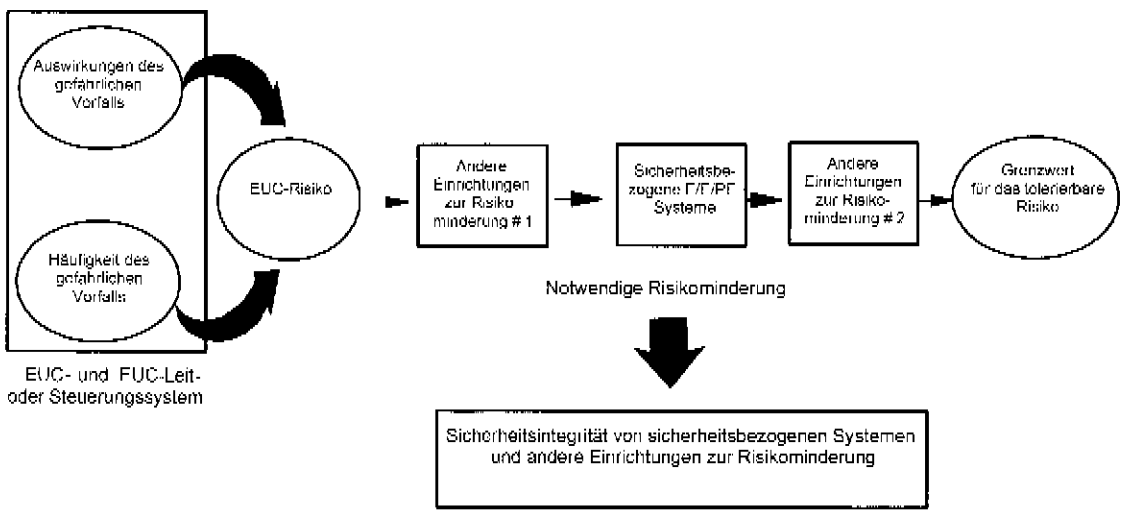


Bild A.2 – Risiko- und Sicherheitsintegritätskonzepte

A.5.2 Sicherheitsintegrität für Anwendungen in der Betriebsart mit hoher Anforderungsrate

Die erforderliche Sicherheitsintegrität der sicherheitsbezogenen E/E/PE-Systeme und andere Maßnahmen zur Risikominderung müssen auf einer Ebene sein um sicherzustellen, dass

- die durchschnittliche Wahrscheinlichkeit eines Ausfalls bei Anfrage des sicherheitsbezogenen Systems so gering ist, dass die Überschreitung der Frequenz eines gefährlichen Vorfalls zur Einhaltung des zulässigen Risikos, vermieden wird, und/oder
- die durchschnittliche Wahrscheinlichkeit des Ausfalls pro Stunde des sicherheitsbezogenen Systems so gering ist, dass die Überschreitung der Frequenz eines gefährlichen Vorfalls zur Einhaltung des zulässigen Risikos, vermieden wird.

Bild A.3 zeigt die allgemeinen Konzepte für Anwendungen in der Betriebsart mit hoher Anforderungsrate. Das Modell geht davon aus, dass

- eine EUC und ein Steuerungssystem vorhanden ist;
- zugehörige menschliche Faktoren vorhanden sind;
- die sicherheitsbezogenen Schutzmaßnahmen folgendes umfassen;
  - sicherheitsbezogene E/E/PE-Systeme in einer Betriebsart mit hoher Anforderungsrate,
  - andere risikomindernde Maßnahmen,

Verschiedene Anforderungen an die sicherheitsbezogenen E/E/PE-Systeme können wie folgt auftreten:

- Allgemeine Anforderungen durch das EUC;
- Anforderungen durch Ausfälle des EUC-Leit- oder Steuerungssystems;
- Anforderungen durch menschliches Versagen.

Wenn die Gesamtanforderungsrate aus allen Anforderungen an das System mehr als 1 pro Jahr überschreitet, dann ist dieser kritische Faktor die Rate gefahrbringender Ausfälle des sicherheitsbezogen E/E/PE-Systems. Die Restfrequenz der Gefährdung kann die gefährliche Ausfallrate des sicherheitsbezogenen E/E/PE-Systems nie überschreiten. Sie kann niedriger sein, wenn andere Maßnahmen zur Risikominderung die Wahrscheinlichkeit von Schäden reduzieren.

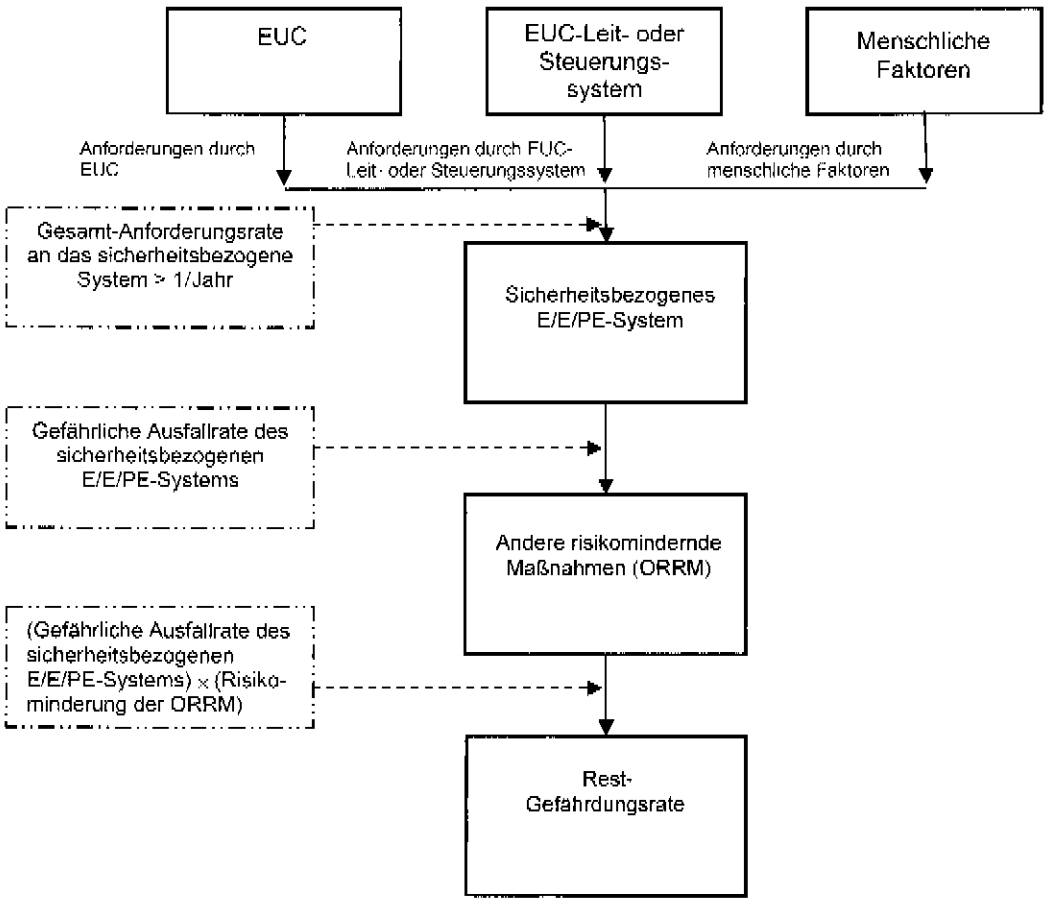


Bild A.3 – Risikodarstellung zu Anwendungen mit hoher Anforderungsrate

A.5.3 Sicherheitsintegrität für Anwendungen in der Betriebsart mit kontinuierlicher Anforderung

Die erforderliche Sicherheitsintegrität der sicherheitsbezogenen E/E/PE-Systeme und jeder anderen Maßnahme zur Risikominderung muss auf einer Ebene sein um sicherzustellen, dass die durchschnittliche Wahrscheinlichkeit des Ausfalls pro Stunde des sicherheitsbezogenen Systems so gering ist, dass die Überschreitung der Frequenz eines gefährlichen Vorfalls zur Einhaltung des zulässigen Risikos, vermieden wird.

Mit einem sicherheitsbezogenen E/E/PE-System in der Betriebsart mit kontinuierlicher Anforderung können andere risikomindernde Maßnahmen die Restfrequenz der Gefährdung, entsprechend der bereitgestellten Risikominderung, mindern. Das Modell ist in Bild A.4 gezeigt.

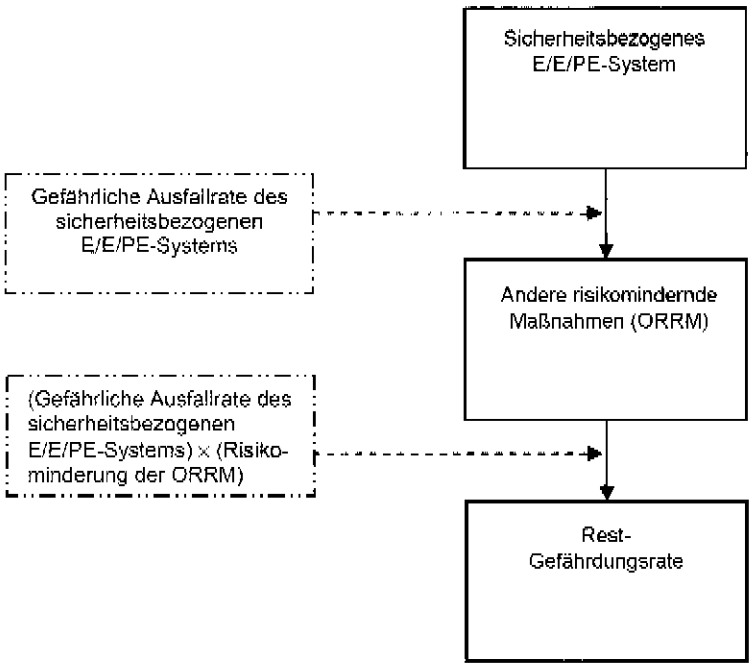


Bild A.4 – Risikodarstellung zu Anwendungen mit kontinuierlichen Anforderungsrate

A.5.4 Ausfälle infolge gemeinsamer und abhängiger Ursache

Während der Bestimmung der Sicherheits-Integritätslevel ist es wichtig Ausfälle infolge gemeinsamer und abhängiger Ursachen zu berücksichtigen. Die oben gezeigten Modelle in den Bildern A.1, A.2, A.3 und A.4 basieren auf der Grundlage, dass jedes Sicherheitssystem für die gleiche Gefährdung völlig unabhängig ist. Es gibt viele Anwendungen, bei denen dies nicht der Fall ist. Beispiele hierfür sind die folgenden:

1. wenn ein gefahrbringender Ausfall eines Elements in dem EUC-Leit- oder Steuerungssystem dazu führt, dass eine Anforderung an ein sicherheitsbezogenes System erfolgt und das sicherheitsbezogene System verwendet ein Element das aus dem gleichen Grund ausfällt. Ein Beispiel hierfür wäre, wenn ein Steuerungs- und Schutzsystem, getrennte Sensoren verwendet, aber eine gemeinsame Ursache zum Ausfall dieser beiden führen könnte (siehe Abbildung A.5);
2. wenn mehr als ein sicherheitsbezogenes System verwendet wird und innerhalb derer sind Teile der Ausrüstung gleichen Typs, so ist jedes sicherheitsbezogene System Ziel für Ausfälle infolge gleicher Ursache. Ein Beispiel wäre, wenn die gleiche Art von Sensor in zwei getrennten Schutzsystemen verwendet wird, die beide Risikominderungen für die gleiche Gefährdung bereitstellen (siehe Abbildung A.6);
3. wenn mehr als ein Schutzsystem verwendet wird, die Schutzsysteme diversitär sind, aber die Wiederholungsprüfungen erfolgen für alle Systeme gleichzeitig. In solchen Fällen wird die tatsächliche PFDavg, erreicht durch die Kombination mehrerer Systeme erheblich höher sein als die erwartete PFDavg der Multiplikation der PFDavg der einzelnen Systeme;
4. wenn das gleiche Element als Teil eines Leit- oder Steuerungssystems und eines sicherheitsbezogenen Systems verwendet wird. Wo mehr als ein Schutzsystem verwendet wird und in denen das gleiche einzelne Element als Teil von mehr als einem System verwendet wird.

In solchen Fällen ist die Wirkung der gemeinsamen Ursache/Abhängigkeit in Betracht zu ziehen. Es sollte berücksichtigt werden, ob die endgültige Anordnung in der Lage ist, die erforderliche systematische Eignung und die erforderliche Wahrscheinlichkeit gefährlicher zufälliger Hardware-Ausfallraten im Zusammenhang mit der erforderlichen gesamt Risikominderung zu erreichen. Die Wirkung von Ausfällen infolge gemeinsamer Ursache ist nur schwer zu bestimmen, und benötigt oftmals die Konstruktion von Spezialmodellen (z. B. Fehlerbaum- oder Markov-Modelle).

Die Wirkung infolge gemeinsamer Ursache ist wahrscheinlich größer in Anwendungen mit hohen Sicherheits-Integritätsleveln. In einigen Anwendungen kann Diversität erforderlich sein, so dass Auswirkungen infolge gemeinsamer Ursache minimiert werden. Es sollte jedoch darauf hingewiesen werden, dass es mit der Diversität zu Problemen beim Entwurf, der Instandhaltung und Änderung kommen kann. Die Einführung von Diversität kann zu Fehlern führen, aufgrund von Unkenntnis und mangelnder Erfahrung mit den diversen Geräten.

A.5.5 Sicherheits-Integritätslevel, bei Verwendung mehrerer Schichten eines Schutzes

Wenn mehrere Schichten eines Schutzes verwendet werden, um eine annehmbare Risiko-Frequenz zu erreichen, kann es zu Wechselwirkungen zwischen den Systemen selbst und auch zwischen den Systemen und den Ursachen einer Anforderung, kommen.

Wie bereits oben in A.5.4 erörtert, gibt es immer wieder Bedenken wegen der Gleichzeitigkeit von Prüfungen und Ausfällen infolge gemeinsamer Ursache, da diese wesentliche Faktoren sein können, wenn die Anforderungen an die Gesamt-Risikominderung hoch sind und wenn die Frequenz der Anforderungen gering ist. Die Bewertung der Wechselwirkungen zwischen den Schichten der Sicherheit und zwischen Schichten der Sicherheit und Ursachen der Anforderung kann sehr komplex sein und können die Entwicklung eines ganzheitlichen Modells nötig machen (z. B. wie in ISO / IEC 31010 ed. 1: Risk management -Risk assessment techniques, beschrieben) und auf der Grundlage, zum Beispiel eines Top-down-Ansatzes mit dem Top-Ereignis als der zulässigen Frequenz der Gefährdung. Das Modell kann alle Schichten der Sicherheit für die Berechnung der tatsächlichen Risikominderung und alle Ursachen von Anforderungen für die Berechnung der tatsächlichen Häufigkeit von Unfällen, beinhalten. Dies ermöglicht die Ermittlung von minimalen Schnittmengen (d.h. Ausfall-Szenarien), zeigt die Schwachpunkte (d.h. die kleinste minimale Schnittmenge: Einzel-, Doppel-Ausfälle, usw.) in der Anordnung der Systeme und eine Systemverbesserung durch eine Analyse der Empfindlichkeiten.

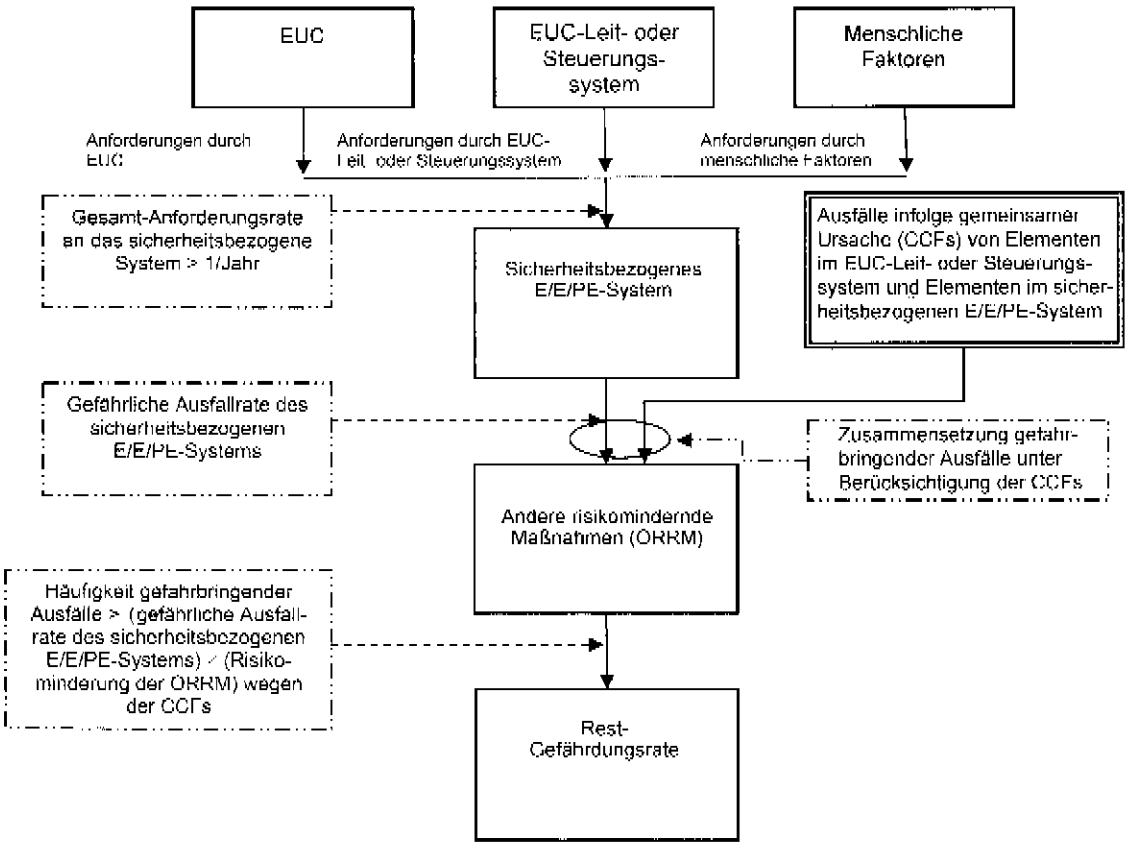


Bild A.5 – Darstellung von Ausfällen infolge gemeinsamer Ursache (CCFs) von Elementen im EUC-Leit- oder Steuerungssystem und Elementen im sicherheitsbezogenen E/E/PE-System

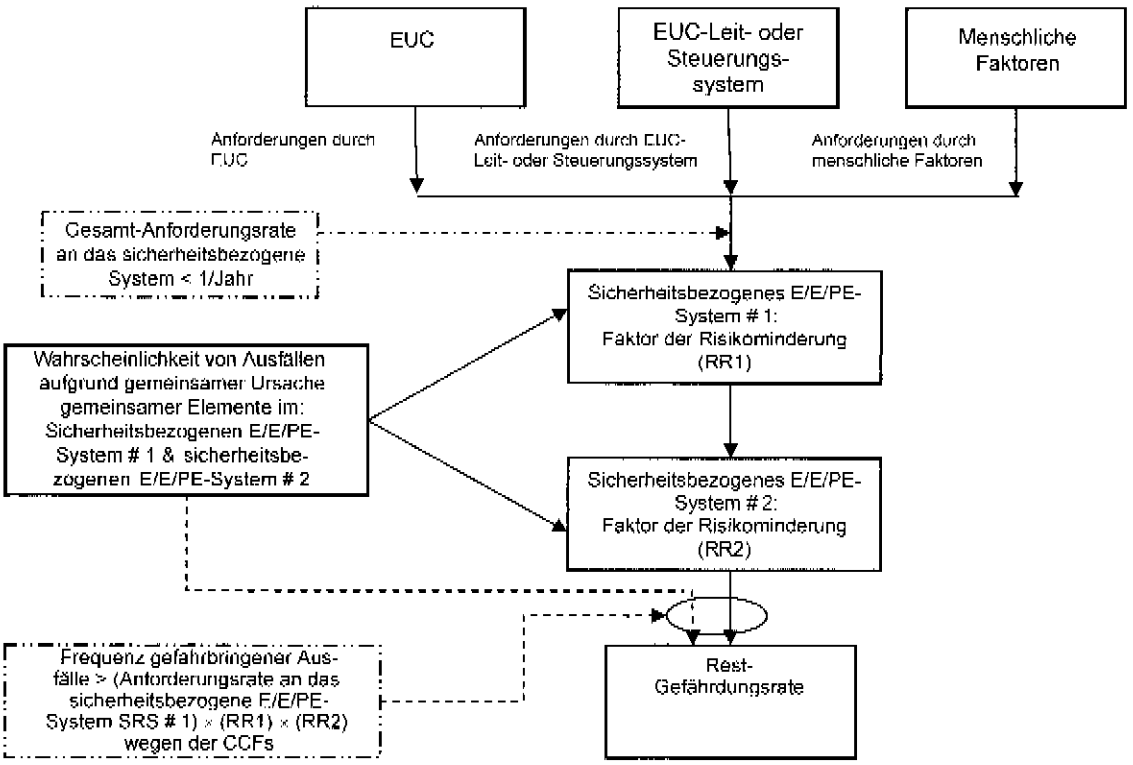


Bild A.6 – Gemeinsame Ursache zwischen zwei sicherheitsbezogenen E/E/PE-Systemen

A.6 Risiko und Sicherheitsintegrität

Es ist wichtig, dass die Unterscheidung zwischen Risiko und Sicherheitsintegrität vollständig erkannt wird. Das Risiko ist ein Maß für die Wahrscheinlichkeit und die Auswirkung eines bestimmten auftretenden gefährlichen Vorfalls. Es kann für unterschiedliche Situationen ausgewertet werden (EUC-Risiko, notwendige Risikominderung, um das tolerierbare Risiko zu erreichen, tatsächliches Risiko (siehe Bild A.1)). Das tolerierbare Risiko wird bestimmt unter Berücksichtigung des in A.2 beschriebenen Sachverhalts. Die Sicherheitsintegrität bezieht sich nur auf die sicherheitsbezogenen E/E/PE-Systeme und andere risikomindernde Maßnahmen und ist ein Maß für die Wahrscheinlichkeit dieser Systeme/Einrichtungen, die notwendige Risikominderung in Bezug auf die festgelegten Sicherheitsfunktionen zufrieden stellend zu erreichen. Sobald das tolerierbare Risiko festgelegt und die notwendige Risikominderung bestimmt worden ist, können die Anforderungen zur Sicherheitsintegrität für die sicherheitsbezogenen Systeme zugeordnet werden (siehe 7.4, 7.5 und 7.6 der IEC 61508-1).

ANMERKUNG Die Zuordnung ist notwendigerweise iterativ, um den Entwurf so zu optimieren, dass die verschiedenen Anforderungen erfüllt werden.

A.7 Sicherheits-Integritätslevel und Software-Sicherheits-Integritätslevel

Um den weiten Bereich der notwendigen Risikominderungen, den sicherheitsbezogene Systeme erreichen müssen, abzudecken, ist es nützlich, über eine Anzahl von Sicherheits-Integritätsleveln zur Erfüllung der Anforderungen der Sicherheitsintegrität der Sicherheitsfunktionen, die den sicherheitsbezogenen Systemen zugewiesen sind, zu verfügen. Software-Sicherheits-Integritätslevel werden als Grundlage für die Spezifikation der Anforderungen zur Sicherheitsintegrität von Sicherheitsfunktionen, die teilweise durch die sicherheitsbezogene Software realisiert werden, verwendet. Die Spezifikation der Anforderungen zur Sicherheitsintegrität sollte den Sicherheits-Integritätslevel für die sicherheitsbezogenen E/E/PE-Systeme bestimmen.

In dieser Norm sind vier Sicherheits-Integritätslevel festgelegt, wobei der Sicherheits-Integritätslevel 4 die höchste und der Sicherheits-Integritätslevel 1 die niedrigste Stufe ist.

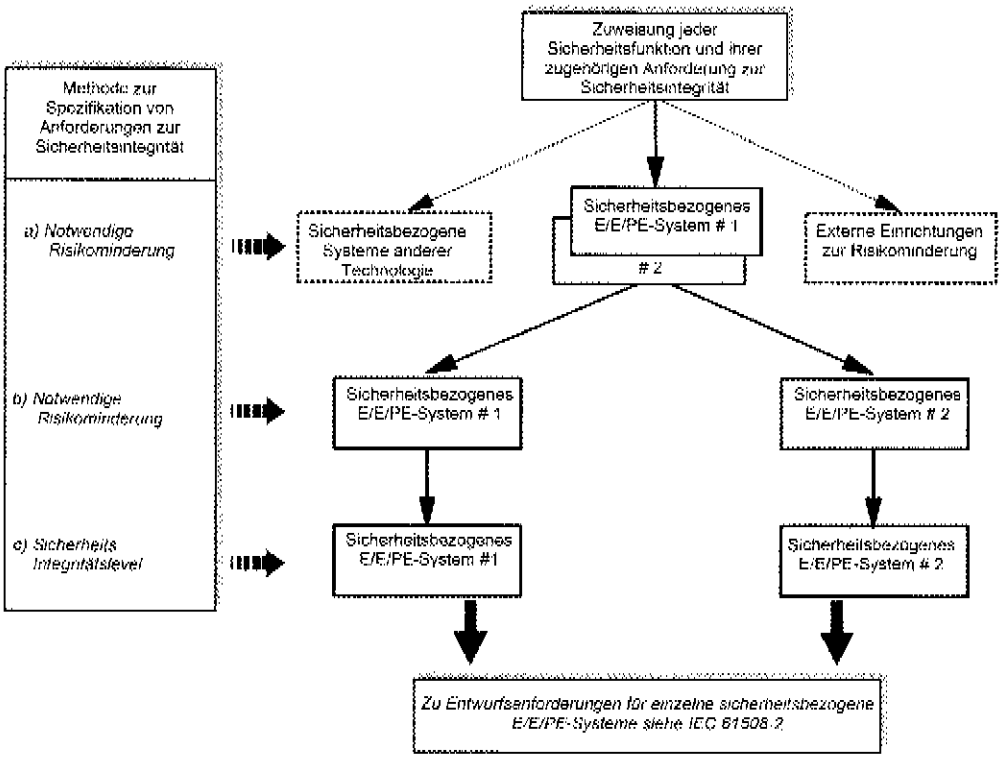
Die Versagens- und Ausfallgrenzwerte für die vier Sicherheits-Integritätslevel sind in den Tabellen 2 und 3 der IEC 61508-1 angegeben. Zwei Parameter sind angegeben, einer für sicherheitsbezogene Systeme, die in einer Betriebsart mit niedriger Anforderungsrate betrieben werden, und einer für sicherheitsbezogene Systeme, die in einer Betriebsart mit hoher oder kontinuierlicher Anforderungsrate betrieben werden.

ANMERKUNG Für sicherheitsbezogene Systeme, die in einer Betriebsart mit niedriger Anforderungsrate betrieben werden, ist das interessierende Maß für die Sicherheitsintegrität die Wahrscheinlichkeit, die entworfene Funktion auf Anforderung nicht auszuführen. Für sicherheitsbezogene Systeme, die mit einer Betriebsart mit hoher oder kontinuierlicher Anforderungsrate betrieben werden, ist das interessierende Maß für die Sicherheitsintegrität die mittlere Wahrscheinlichkeit eines gefahrbringenden Ausfalls pro Stunde (siehe 3.5.12 und 3.5.13 der IEC 61508-4).

A.8 Zuordnung von Sicherheitsanforderungen

Die Zuordnung von Sicherheitsanforderungen (sowohl der Sicherheitsfunktionen als auch der Anforderungen zur Sicherheitsintegrität) zu den sicherheitsbezogenen E/E/PE-Systemen, sicherheitsbezogenen Systemen anderer Technologie und externen Einrichtungen zur Risikominderung wird in Bild A.7 dargestellt (dies ist identisch zu Bild 6 der IEC 61508-1). Die Anforderungen an die Phase der Zuordnung der Sicherheitsanforderungen sind in 7.6 der IEC 61508-1 enthalten.

Die Methoden für die Zuordnung der Anforderungen zur Sicherheitsintegrität zu den sicherheitsbezogenen E/E/PE-Systemen, sicherheitsbezogenen Systemen anderer Technologie und externen Einrichtungen zur Risikominderung hängen zuallererst davon ab, ob die notwendige Risikominderung in einer numerischen oder qualitativen Art und Weise festgelegt ist. Diese Methoden werden als quantitative bzw. qualitative Methoden bezeichnet (siehe Anhänge B, C, D und E).



ANMERKUNG 1 Anforderungen an die Sicherheitsintegrität sind jeder Sicherheitsfunktion vor der Zuweisung zugeordnet (siehe 7.5.2.6 von IEC 61508-1).

ANMERKUNG 2 Eine Sicherheitsfunktion kann mehr als einem sicherheitsbezogenen System zugeordnet werden.

Bild A.7 – Zuordnung der Sicherheitsanforderungen zu den sicherheitsbezogenen E/E/PE-Systemen, sicherheitsbezogenen Systemen anderer Technologie und externen Einrichtungen zur Risikominderung

A.9 Systeme zur Schadensbegrenzung

Systeme zur Schadensbegrenzung werden aktiv, im Falle des vollständigen oder teilweisen Ausfalls anderer sicherheitsbezogener Systeme wie z. B. E/E/PE-Sicherheits-Systeme. Das Ziel ist eher die Verringerung der Auswirkungen im Zusammenhang mit einem gefährlichen Vorfall als dessen Häufigkeit. Zu Beispielen für Systeme zur Schadensbegrenzung gehören Feuer- und Gas-Systeme (Erkennung von Feuer / Gas- und nachgeordnete Maßnahmen, um das Feuer zu löschen (z. B. durch Wasserflutung) und Airbag-Systeme in einem Auto).

Bei der Bestimmung der Anforderungen der Sicherheitsintegrität sollte berücksichtigt werden, dass, wenn die Entscheidungen über die Schwere der Auswirkungen getroffen werden, nur die erhöhten Auswirkungen zu berücksichtigen sind. Das bedeutet, Bestimmung der Zunahme der Schwere der Auswirkungen, wenn die Funktion nicht in Betrieb ist, gegenüber wenn diese wie vorgesehen arbeitet. Dies kann erfolgen, indem zunächst die Konsequenzen betrachtet werden, wenn das System nicht wie vorgesehen funktioniert und dann betrachtet, welchen Unterschied es ausmacht wenn die Systeme zur Schadensbegrenzung ordnungsgemäß arbeiten. Bei der Berücksichtigung der Auswirkungen, wenn das System nicht wie vorgesehen funktioniert, wird sich in der Regel eine Reihe von Ergebnissen mit unterschiedlichen Wahrscheinlichkeiten ergeben.

ANMERKUNG Die Anleitung zur Bestimmung des Sicherheits-Integritätslevels für Feuer-, Gas- und Notabschaltungs-Systeme ist im Anhang B der ISO 10418, Petroleum and natural gas industries. – Analysis, design and testing of basicsurface process safety systems on offshore production installations – Requirements and Guidelines, enthalten.

Anhang B
(informativ)

Auswahl von Methoden zur Bestimmung der Sicherheits-Integritätslevel

B.1 Allgemeines

Dieser Anhang enthält eine Reihe von Verfahren die zur Bestimmung des Sicherheits-Integritätslevels verwendet werden können. Keines der Verfahren eignet sich für alle Anwendungen und die Benutzer wählen das am besten geeignete aus. Bei der Auswahl der am besten geeigneten Verfahren sollten die folgenden Faktoren berücksichtigt werden.

1. Die Risiko-Akzeptanzkriterien die zu erfüllen sind. Einige der Verfahren werden nicht geeignet sein, wenn erforderlich nachzuweisen, dass das Risiko so weit wie vernünftigerweise möglich reduziert wurde.
2. Die Betriebsart der Sicherheitsfunktion. Einige Verfahren sind nur für die Betriebsart mit niedriger Anforderungsrate, geeignet.
3. Das Wissen und die Erfahrung der Personen, die die SIL-Bestimmung durchführen und wie der traditionelle Ansatz in dem Bereich gewesen war.
4. Das notwendige Vertrauen, das das sich ergebende Restrisiko die spezifizierten Kriterien der Anwender-Organisation erfüllt. Einige der Methoden können verbunden werden zu quantifizierten Zielen, einige Ansätze sind aber nur qualitativ.
5. Es kann mehr als eine Methode verwendet werden. Eine Methode kann für eine Vorauswahl verwendet werden, gefolgt von einem anderen strengeren Ansatz, wenn die Vorauswahl die Notwendigkeit eines hohen Sicherheits-Integritätslevels zeigt.
6. Die Schwere der Auswirkungen. Strengere Methoden können ausgewählt werden wenn die Auswirkungen mehrere Todesopfer beinhalten.
7. Ob gemeinsame Ursachen zwischen den sicherheitsbezogenen E/E/PE-Systemen oder zwischen dem sicherheitsbezogenen E/E/PE-System und den Ursachen der Anforderungen, bestehen.

Unabhängig von der angewandten Methode sollten alle gemachten Annahmen für das zukünftige Management der Sicherheit aufgezeichnet werden. Alle Entscheidungen sollten aufgezeichnet werden, damit die SIL-Beurteilung verifiziert und einer unabhängigen Beurteilung der funktionalen Sicherheit unterzogen werden kann.

B.2 Quantitative Methode der SIL-Bestimmung

Die quantitative Methode ist in Anhang D beschrieben. Sie kann zusammen mit der ALARP-Methode in Anhang C verwendet werden.

Die quantitative Methode kann sowohl für einfache als auch komplexe Anwendungen verwendet werden. Bei komplexen Anwendungen können Fehlerbäume konstruiert werden um das Gefährdungsmodell darzustellen. Das maximale Ereignis wird in der Regel ein oder mehrere Todesopfer sein und eine Logik entworfen, um die Ursachen der Anforderungen und Ausfälle der sicherheitsbezogenen E/E/PE-Systeme darzustellen, die zu dem maximalen Ereignis führen. Es stehen Software-Werkzeuge zur Verfügung gemeinsame Ursachen zu modellieren, wenn die gleiche Art von Ausrüstung, für die Steuerungs- und Schutz-Funktionen, verwendet wird. In einigen komplexen Anwendungen kann ein einzelnes Ausfallereignis an mehr als einer Stelle im Fehlerbaum auftreten. Dies erfordert die Durchführung einer bool`schen Reduzierung. Die Werkzeuge unterstützen auch die Anfälligkeitsanalyse um die beherrschenden Faktoren des Einflusses auf die Häufigkeit des maximalen Ereignisses zu zeigen. Der SIL kann begründet werden durch die Bestimmung der erforderlichen Risikominderung um das tolerierbare Risiko-Kriterium zu erreichen.

Die Methode ist geeignet für Sicherheitsfunktionen, in der Betriebsart mit kontinuierlicher/hoher- und der Betriebsart mit niedriger Anforderungsrate. Diese Methode ergibt in der Regel geringe SILs, da das Risikomodell speziell für jede Anwendung und numerische Werte entworfen worden ist, um jeweils einen Risikofaktor darzustellen, statt der numerischen Bereiche die in kalibrierten Risikographen verwendet werden. Quantitative Methoden erfordern jedoch die Konstruktion eines speziellen Modells für jeden gefährlichen Vorfall.

Die Modellierung erfordert Geschick, Werkzeuge und Kenntnisse über die Anwendung und kann erhebliche Zeit zur Entwicklung und zur Überprüfung erfordern.

Die Methode erleichtert den Nachweis, dass das Risiko so weit wie vernünftigerweise möglich reduziert wurde. Dies kann geschehen, durch Berücksichtigung von Möglichkeiten für eine weitere Risikominderung, der Integration von zusätzlichen Einrichtungen in das Fehlerbaum-Modell und dann die Bestimmung der Verringerung des Risikos und der Vergleich mit den Kosten für diese Möglichkeit.

B.3 Die Risikograph-Methode

Die qualitative Methode des Risikographen ist in Anhang E beschrieben. Die Methode ermöglicht es, den Sicherheits-Integritätslevel auf der Kenntnis der Risikofaktoren die mit dem EUC-Leit- oder Steuerungssystem verbunden sind, zu bestimmen. Es wird eine Reihe von Parametern eingeführt, die zusammen die Art der Gefährdungssituation beschreiben, wenn sicherheitsrelevante Systeme versagen oder nicht zur Verfügung stehen. Ein Parameter wird aus einem Satz von vieren gewählt, und die ausgewählten Parameter werden dann so kombiniert, um den der Sicherheitsfunktion zugeordneten Sicherheits-Integritätslevel, zu bestimmen. Die Methode wurde ausführlich im Maschinensektor, siehe ISO 14121-2 und Anhang A der ISO 13849-1, verwendet.

Die Methode kann qualitativ sein, in diesem Fall ist die Auswahl der Parameter subjektiv und erfordert ein erhebliches Urteilsvermögen. Das Restrisiko kann nicht durch die Kenntnis der Werte der Parameter berechnet werden. Es ist nicht geeignet, wenn eine Organisation fordert, dass Restrisiko auf einen bestimmten, quantitativen, Wert zu reduzieren.

Die Beschreibung der Parameter kann numerische Werte beinhalten, die sich durch die Kalibrierung des Risikographen, gegen numerische tolerierte Risikokriterien, herleiten. Das Restrisiko lässt sich, aus den verwendeten numerischen Werten der Parameter, berechnen. Es ist geeignet, wenn eine Organisation Vertrauen fordert, dass das Restrisiko auf einen bestimmten quantitativen Wert reduziert ist. Die Erfahrung hat gezeigt, dass die Verwendung der Methode eines kalibrierten Risikographen zu hohen Sicherheits-Integritätslevel führen kann. Dies liegt daran, dass die Kalibrierung in der Regel mit verwendeten Worst Case Werten der einzelnen Parameter durchgeführt wird. Jeder Parameter hat den Bereich einer Dekade, so dass für Anwendungen, bei denen alle Parameter für den Bereich Durchschnittswerte sind, wird der SIL eine Dekade höher sein als das notwendige tolerierbare Risiko. Das Verfahren wird umfangreich in der Prozess- und dem Offshore-Sektor eingesetzt.

Die Risikograph-Methode berücksichtigt nicht, Ausfälle infolge gemeinsamer Ursache zwischen den Ursachen von Anforderungen und der Ursache des Ausfalls des sicherheitsbezogenen E/E/PE-Systems oder gemeinsame Ursachen mit anderen Schichten eines Schutzes.

B.4 Analyse der Schutzebenen (en.: Layer of Protection Analysis (LOPA))

Die grundlegende Methode ist in einer Reihe von Büchern beschrieben und das Verfahren kann in einer Reihe von verschiedenen Formen erfolgen. Eine Technik, die für die SIL-Bestimmung verwendet werden kann, ist im Anhang F beschrieben.

Das Verfahren ist quantitativ und der Anwender hat die zulässigen Häufigkeiten für jede Auswirkung und Schweregrad festzulegen. Es erfolgt eine numerische Gutschrift für die Schutzebenen, die die Häufigkeit der individuellen Ursachen für Anforderungen reduzieren. Nicht alle Schutzebenen sind für alle Ursachen von Anforderungen zuständig, so dass das Verfahren für komplexere Anwendungen verwendet werden kann. Die den Schutzebenen zugeordneten numerischen Werte können auf die nächste signifikante Zahl oder den nächsten signifikanten Dekadebereich aufgerundet werden. Wenn numerische Werte von Schutzebenen auf die nächste signifikante Zahl gerundet sind, dann ergibt die Methode im Durchschnitt geringere Anforderungen an die Risikominderung und niedrigere SIL-Werte als kalibrierte Risikographen.

Da numerische Ziele, bestimmten Auswirkungen, Schweregraden zugeordnet sind, kann der Anwender darauf vertrauen, dass das Restrisiko die Firmenkriterien erfüllt.

Wie beschrieben, ist die Methode nicht geeignet für Funktionen, die in der Betriebsart mit kontinuierlicher Anforderung betrieben werden und berücksichtigt nicht den Ausfall infolge gemeinsamer Ursache zwischen

Ursachen der Anforderungen und dem sicherheitsbezogenen E/E/PE-System. Die Methode kann jedoch angepasst werden und eignet sich dann für solche Fälle.

Anhang C
(informativ)

Konzepte für ALARP und tolerierbares Risiko

C.1 Allgemeines

Dieser Anhang berücksichtigt einen bestimmten Ansatz zur Erreichung eines tolerierbaren Risikos. Er ist nicht vorgesehen als eine endgültige Beschreibung der Methode, sondern zur Erläuterung der allgemeinen Prinzipien. Das Konzept beinhaltet einen Prozess der kontinuierlichen Verbesserung, wobei alle Optionen, die das Risiko reduzieren berücksichtigt sind, in Bezug auf Kosten und Nutzen. Diejenigen, die beabsichtigen, die in diesem Anhang aufgeführten Methoden anzuwenden, sollten das angegebene Quellenmaterial zu Rate ziehen. [6]

C.2 ALARP-Modell

C.2.1 Einleitung

C.2 gibt einen Überblick über die Hauptprüfungen, die bei der Regulierung industrieller Risiken verwendet werden, und gibt an, dass es sich darum handelt festzustellen, ob

a) das Risiko so groß ist, dass es insgesamt abgelehnt werden muss; oder

b) das Risiko so klein ist oder so weit verringert worden ist, dass es unbedeutend ist; oder

c) das Risiko zwischen den beiden oben in a) und b) genannten Zuständen liegt, und dass es auf die niedrigste Stufe, die praktikabel ist, verringert worden ist, unter Berücksichtigung des aus der Akzeptanz folgenden Nutzens und der Kosten jeder weiteren Minderung.

Im Hinblick auf c) erfordert das ALARP-Prinzip, dass jedes Risiko so weit wie vernünftigerweise möglich gemindert wird, oder bis zu einer Stufe, die so niedrig wie vernünftigerweise möglich ist (ALARP= as low as reasonably practicable = so niedrig wie vernünftigerweise möglich). Wenn ein Risiko zwischen die beiden Extreme fällt (d. h. zwischen den nicht annehmbaren Bereich und den weithin annehmbaren Bereich) und das ALARP-Prinzip angewendet worden ist, ist das resultierende Risiko das für die betreffende Anwendung tolerierbare Risiko. Diese Vorgehensweise mit drei Bereichen ist in Bild C.1 gezeigt.

Oberhalb einer bestimmten Stufe wird das Risiko als nicht tolerierbar betrachtet und kann unter keinem üblichen Umstand gerechtfertigt werden.

Unterhalb dieser Ebene gibt es einen tolerierbaren Bereich, in dem eine Tätigkeit erlaubt ist, vorausgesetzt, dass die zugehörigen Risiken so weit wie vernünftigerweise möglich gemindert worden sind. "Tolerierbar" unterscheidet sich hier von "annehmbar": Es zeigt die Bereitwilligkeit an, mit einem Risiko eines bestimmten Nutzens wegen zu leben, mit der gleichzeitigen Erwartung, es zu beobachten und zu vermindern, sobald dies möglich ist. Hier ist eine Nutzen-Beurteilung erforderlich, entweder explizit oder implizit, um die Kosten und die Notwendigkeit für weitere Sicherheitsmaßnahmen abzuwägen. Je höher das Risiko, desto mehr Aufwand kann erwartet werden, um dieses zu verringern. An der Grenze der Tolerierbarkeit würde Aufwand in großem Missverhältnis zum Nutzen gerechtfertigt werden. Hier wird das Risiko beträchtlich und Recht und Billigkeit verlangen selbst für eine unbedeutende Minderung einen beträchtlichen Aufwand.

Wo Risiken weniger bedeutsam sind, wird verhältnismäßig weniger Aufwand benötigt, um sie zu mindern, und am unteren Ende des tolerierbaren Bereiches ist eine Abwägung zwischen Kosten und Nutzen ausreichend.

Unterhalb des tolerierbaren Bereiches werden die Stufen des Risikos als so unbedeutsam betrachtet, dass der Regelsetzer keine weiteren Verbesserungen fordern muss. Dies ist der weithin annehmbare Bereich, in dem Risiken im Vergleich zum täglichen Risiko, das wir alle erfahren, klein sind. Während in dem weithin annehmbaren Bereich keine weitere Arbeit notwendig ist, um ALARP darzulegen, ist andererseits Wachsamkeit notwendig, um sicherzustellen, dass das Risiko auf dieser Stufe verbleibt.

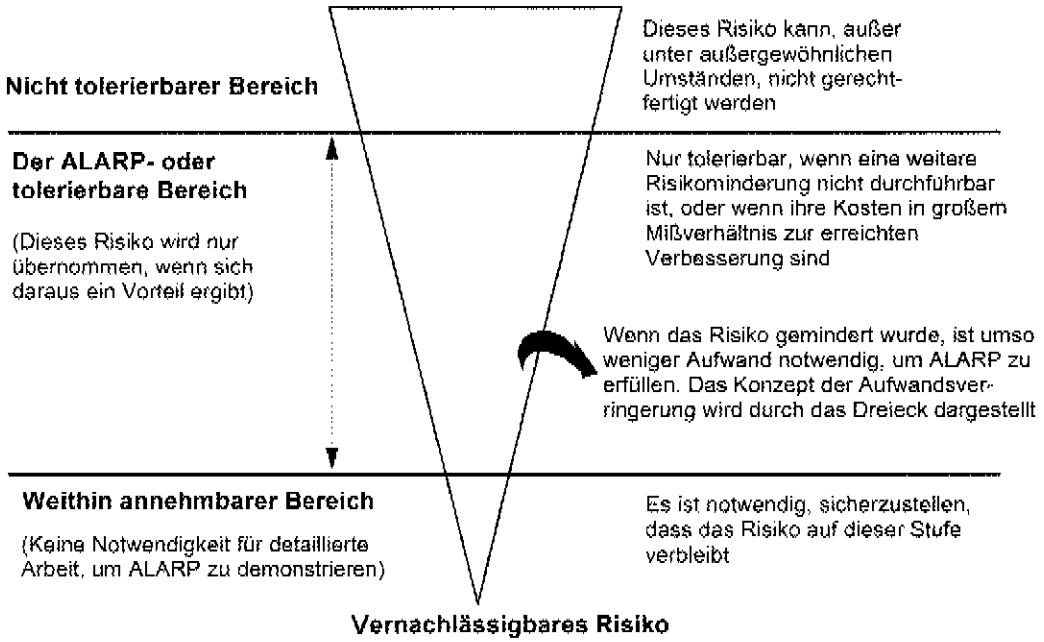


Bild C.1 – Tolerierbares Risiko und ALARP

Das ALARP-Konzept kann benutzt werden, wenn qualitative oder quantitative Risikogrenzwerte verwendet werden. C.2.2 zeigt eine Methode für quantitative Risikogrenzwerte (Anhang D und F zeigen quantitative Methoden und die Anhänge E und G zeigen qualitative Methoden für die Festlegung der notwendigen Risikominderung für eine bestimmte Gefährdung. Die aufgezeigten Methoden könnten in der Entscheidungsfindung das ALARP-Konzept mit einbeziehen.).

ANMERKUNG Für weitere Informationen zu ALARP siehe Verweis [6] der Literaturhinweise.

C.2.2 Grenzwert für das tolerierbare Risiko

Eine Möglichkeit, wie ein Grenzwert für das tolerierbare Risiko erreicht werden kann, ist es, eine Anzahl von Auswirkungen zu bestimmen und ihnen tolerierbare Häufigkeiten zuzuweisen. Diese Anpassung der Auswirkungen zu den tolerierbaren Häufigkeiten erfolgt durch Diskussion und Übereinkommen zwischen den beteiligten Parteien (z. B. den Behörden, die Sicherheitsregeln erstellen, und denjenigen, die das Risiko verursachen, und denjenigen, die dem Risiko ausgesetzt sind).

Unter Berücksichtigung von ALARP-Konzepten kann die Anpassung der Auswirkungen mit einer tolerierbaren Häufigkeit durch Risikoklassen erfolgen. Tabelle C.1 ist ein Beispiel, das vier Risikoklassen (I, II, III, IV) für eine Anzahl von Auswirkungen und Häufigkeiten enthält. Unter Verwendung des ALARP-Konzeptes interpretiert Tabelle C.2 jede Risikoklasse. Das bedeutet, dass die Beschreibung jeder Risikoklasse auf Bild C.1 basiert. Die Risiken in diesen Risikoklassen sind die Risiken, die vorhanden sind, wenn die Maßnahmen zur Risikominderung durchgeführt worden sind. Im Hinblick auf Bild C.1 sind die Risikoklassen wie folgt festgelegt:

- Risikoklasse I ist im nicht annehmbaren Bereich;
- Risikoklassen II und III sind im ALARP-Bereich; die Risikoklasse II ist gerade noch im ALARP-Bereich;
- Risikoklasse IV ist im weithin annehmbaren Bereich.

Für jede bestimmte Situation oder jeden bestimmten Bereich vergleichbarer Industrien würde eine Tabelle, ähnlich zu Tabelle C.1, unter Berücksichtigung eines weiten Bereiches gesellschaftlicher, politischer und wirtschaftlicher Faktoren entwickelt werden. Jede Auswirkung würde an die Häufigkeit angepasst und die Tabelle mit Risikoklassen ausgefüllt werden. Zum Beispiel könnte „häufig" in Tabelle C.1 ein Ereignis bezeichnen, das wahrscheinlich dauernd eintritt, was als Häufigkeit von mehr als 10 Ereignissen pro Jahr bezeichnet werden könnte. Eine kritische Auswirkung könnte der Tod einer Person und/oder mehrfache schwer wiegende Verletzungen oder eine schwer wiegende Berufskrankheiten sein.

Tabelle C.1 – Beispiel für die Risikoklassifizierung von Unfällen

Häufigkeit	Auswirkung			
	katastrophal	kritisch	begrenzt	Geringfügig
häufig	I	I	I	II
wahrscheinlich	I	I	II	III
gelegentlich	I	II	III	III
gering	II	III	III	IV
unwahrscheinlich	III	III	IV	IV
nicht glaubhaft	IV	IV	IV	IV

ANMERKUNG 1 Die tatsächlichen Risikoklassen I, II, III, IV sind vom Einsatzgebiet abhängig und ebenfalls davon, was die aktuellen Häufigkeiten „häufig", „wahrscheinlich" usw. bedeuten. Daher sollte diese Tabelle eher als Beispiel gesehen werden, wie eine solche Tabelle ausgefüllt werden könnte, und weniger als Festlegung für die zukünftige Verwendung.

ANMERKUNG 2 Die Bestimmung des Sicherheits-Integritätslevels aus den Häufigkeiten dieser Tabelle wird in Anhang D darstellt.

Tabelle C.2 – Interpretation der Risikoklassen

Risikoklasse	Interpretation
Klasse I	Nicht tolerierbares Risiko
Klasse II	unerwünschtes Risiko, das nur tolerierbar ist, wenn eine Risikominderung nicht durchführbar ist oder die Kosten der Minderung unverhältnismäßig hoch im Vergleich zur erzielten Verbesserung sind
Klasse III	tolerierbares Risiko wenn die Kosten einer Risikominderung die erreichbare Verbesserung übersteigen
Klasse IV	vernachlässigbares Risiko

Anhang D
(informativ)

Festlegung der Sicherheits-Integritätslevel: Eine quantitative Methode

D.1 Allgemeines

Dieser Anhang skizziert, wie die Sicherheits-Integritätslevel bei Verwendung einer quantitativen Methode festgelegt werden können, und zeigt auf, wie die in Tabellen, zum Beispiel Tabelle D.1, enthaltenen Informationen verwendet werden können. Eine quantitative Methode ist von besonderem Wert, wenn:

- das tolerierbare Risiko in einer numerischen Art und Weise bestimmt worden ist (z. B. dass eine bestimmte Auswirkung nicht mit einer Häufigkeit größer als einmal in 10^4 Jahren auftreten sollte);
- numerische Grenzwerte für die Sicherheits-Integritätslevel der sicherheitsbezogenen Systeme bestimmt worden sind. Derartige Grenzwerte sind in dieser Norm festgelegt worden (siehe Tabellen 2 und 3 der IEC 61508-1).

Dieser Anhang ist nicht als endgültige Beschreibung der Methode, sondern zur Erläuterung der allgemeinen Prinzipien vorgesehen. Er ist insbesondere anwendbar, wenn das Risikomodell dem in den Bildern A.1 und A.2 gezeigten entspricht.

D.2 Allgemeine Methode

Das für die Darstellung der allgemeinen Prinzipien verwendete Modell wird in Bild A.1 gezeigt. Die wesentlichen Schritte der Methode sind für jede durch das sicherheitsbezogene E/E/PE-System realisierte Sicherheitsfunktion erforderlich und sind die folgenden:

- Bestimmung des tolerierbaren Risikos aus einer Tabelle ähnlich der Tabelle C.1;
- Bestimmung des EUC-Risikos;
- Bestimmung der notwendigen Risikominderung, um das tolerierbare Risiko zu erreichen;
- Zuordnung der notwendigen Risikominderung zu den sicherheitsbezogenen E/E/PE-Systemen, sicherheitsbezogenen Systemen anderer Technologien und externen Einrichtungen zur Risikominderung (siehe 7.6 der IEC 61508-1).

Tabelle C.1 enthält Risikohäufigkeiten und ermöglicht die Festlegung eines numerischen Grenzwertes (F_I) für das tolerierbare Risiko.

Die Häufigkeit, die mit dem Risiko, das für die EUC, einschließlich des EUC-Leit- oder Steuerungssystems und menschlicher Faktoren ohne jede Schutzmaßnahme existiert (das EUC-Risiko), zusammenhängt, kann unter Anwendung quantitativer Risikobeurteilungsmethoden abgeschätzt werden. Diese Häufigkeit (F_{np}), mit der ein gefährlicher Vorfall ohne vorhandene Schutzmaßnahmen auftreten könnte, ist einer von zwei Bestandteilen des EUC-Risikos; der andere Bestandteil ist die Auswirkung des gefährlichen Vorfalls. F_{np} kann bestimmt werden durch:

- Analyse der Ausfallraten in vergleichbaren Situationen;
- Daten aus relevanten Datenbanken;
- Berechnung unter Anwendung angemessener Vorhersagemethoden.

Diese Norm macht Einschränkungen bezüglich der minimalen Ausfallraten, die für das EUC-Leit- oder Steuerungssystem geltend gemacht werden können (siehe 7.5.2.5 der IEC 61508-1). Falls geltend gemacht wird, dass das EUC-Leit- oder Steuerungssystem eine geringere Ausfallrate als diese minimalen Ausfallraten hat, muss das EUC-Leit- oder Steuerungssystem als sicherheitsbezogenes System betrachtet werden und allen Anforderungen an sicherheitsbezogene Systeme in dieser Norm unterworfen werden.

D.3 Beispielrechnung

Bild D.1 liefert ein Beispiel, wie der Grenzwert der Sicherheitsintegrität für eine einzelne sicherheitsbezogene Schutzeinrichtung berechnet wird. In diesem Fall ist:

$$PFD_{avg} \leq F_t / F_{np}$$

Dabei ist

- PFD_{avg} die mittlere Wahrscheinlichkeit eines Ausfalls bei Anforderung der sicherheitsbezogenen Schutzeinrichtung, welches der Versagensgrenzwert der Sicherheitsintegrität für sicherheitsbezogene Schutzeinrichtungen bei Betriebsart mit niedriger Anforderungsrate ist (siehe Tabelle 2 der IEC 61508-1 und 3.5.12 der IEC 61508-4)
- F_t die Häufigkeit der tolerierbaren Gefährdung
- F_{np} die Anforderungsrate der sicherheitsbezogenen Schutzeinrichtung

Ebenfalls in Bild D.1:

- C ist die Auswirkung des gefährlichen Vorfalls;
- F_p ist die Häufigkeit des Risikos bei Vorhandensein der Schutzmerkmale;

Es ist ersichtlich, dass die Bestimmung von F_{np} für die EUC wegen seiner Beziehung zu PFD_{avg} und damit zum Sicherheits-Integritätslevel wichtig ist.

Die erforderlichen Schritte zur Erzielung des Sicherheits-Integritätslevels (wenn die Auswirkung C konstant bleibt) werden unten (wie in Bild D.1) für die Situation angegeben, in der die gesamte notwendige Risikominderung durch eine einzelne sicherheitsbezogene Schutzeinrichtung erreicht wird, welche die Gefährdungsrate mindestens von F_{np} auf F_t verringern muss:

- Bestimmung der Häufigkeit des EUC-Risikos ohne das Vorhandensein irgendwelcher Schutzmaßnahmen (F_{np});
- Bestimmung der Auswirkung C ohne das Vorhandensein irgendwelcher Schutzmaßnahmen;
- Bestimmung, ob für die Häufigkeit (F_{np}) und die Auswirkung (C) eine tolerierbare Stufe des Risikos erreicht worden ist, unter Verwendung der Tabelle C.1. Wenn durch die Verwendung der Tabelle C.1 diese Bestimmung zu der Risikoklasse I führt, ist eine weitere Risikominderung erforderlich. Die Risikoklassen IV oder III entsprechen tolerierbaren Risiken. Die Risikoklasse II erfordert weitere Untersuchungen;

ANMERKUNG Tabelle C.1 wird zur Überprüfung verwendet, ob weitere Maßnahmen zur Risikominderung notwendig sind, da es möglich ist, ein tolerierbares Risiko ohne zusätzliche Schutzmaßnahmen zu erreichen.

- Festlegung der Wahrscheinlichkeit eines Ausfalls bei Anforderung für die sicherheitsbezogene Schutzeinrichtung PFD_{avg}, um die minimal erforderliche Risikominderung (ΔR) zu erreichen. Für eine konstante Auswirkung ergibt dies für die beschriebene spezielle Situation:

  $PFD_{avg} = (F_t / F_{np}) = \Delta R$;

- Für $PFD_{avg_{avg}} = (F_t / F_{np})$ kann der Sicherheits-Integritätslevel der Tabelle 2 der IEC 61508-1 entnommen werden (z. B. für $PFD_{avg} = 10^{-2} - 10^{-3}$ ist der Sicherheits-Integritätslevel = 2).

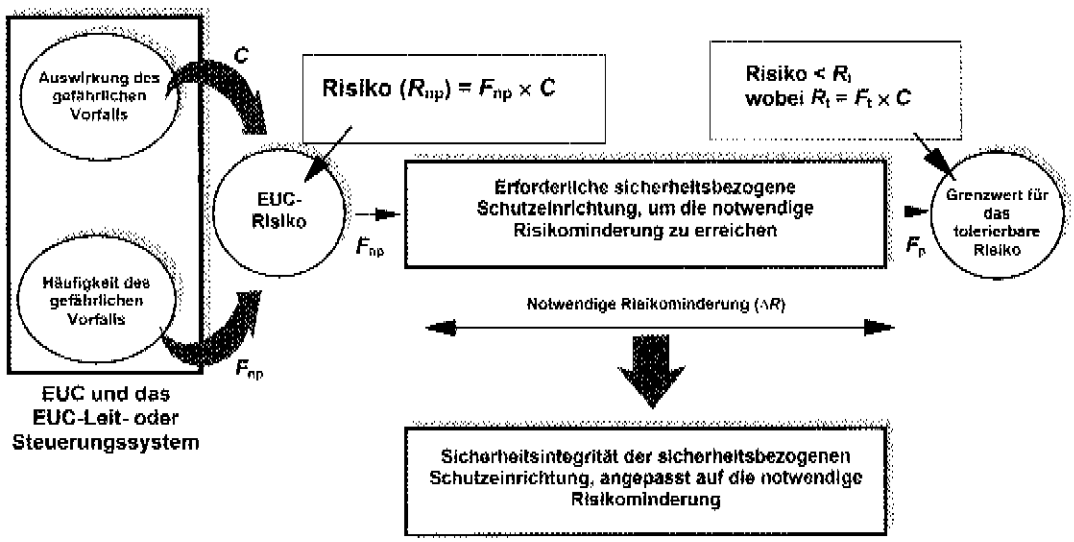


Bild D.1 – Zuordnung der Sicherheitsintegrität: Beispiel für eine sicherheitsbezogene Schutzeinrichtung

Anhang E
(informativ)

Bestimmung der Sicherheits-Integritätslevel Risikograph-Methoden

E.1 Allgemeines

Dieser Anhang beschreibt die Risikograph-Methode, die es ermöglicht, den Sicherheits-Integritätslevel eines sicherheitsbezogenen Systems aus der Kenntnis der Risikofaktoren, die mit der EUC und dem EUC-Leit- oder Steuerungssystem zusammenhängen, zu bestimmen. Die Vorgehensweise ist insbesondere anwendbar, wenn das Risikomodell dem in den Bildern A.1 und A.2 gezeigten entspricht. Die Methode kann auf einer qualitativen oder quantitativen Basis verwendet werden.

Wo diese Methode angewendet worden ist, wird zur Vereinfachung der Umstände eine Anzahl von Parametern eingeführt, die gemeinsam den Charakter der Gefährdungssituation beschreiben, wenn sicherheitsbezogene Systeme versagen oder nicht vorhanden sind. Ein Parameter wird aus je einem von vier Parametersätzen ausgewählt, und die ausgewählten Parameter werden dann kombiniert, um den Sicherheits-Integritätslevel, der den Sicherheitsfunktionen zugeordnet wird, festzulegen. Diese Parameter:

- erlauben es, eine sinnvolle Abstufung des Risikos durchzuführen, und
- enthalten die Schlüsselfaktoren der Risikobeurteilung.

Dieser Anhang ist nicht als eine endgültige Beschreibung der Methode, sondern zur Erläuterung der allgemeinen Prinzipien vorgesehen.

E.2 Aufbau des Risikographen

Das nachfolgende vereinfachte Verfahren basiert auf folgender Gleichung:

$$R = (f) \text{ eines bestimmten } (C)$$

Dabei ist

R das Risiko ohne sicherheitsbezogenes System

f die Häufigkeit des gefährlichen Vorfalls ohne sicherheitsbezogenes System

C die Auswirkung des gefährlichen Vorfalls ist (die Auswirkungen könnten auf den Schaden, der mit Gesundheit und Sicherheit oder mit Umweltschäden einhergeht, bezogen werden)

Die Häufigkeit des gefährlichen Vorfalls f setzt sich in diesem Fall aus drei beeinflussenden Faktoren zusammen:

- der Häufigkeit und Zeit des Aufenthalts im Gefahrenbereich;
- der Möglichkeit, den gefährlichen Vorfall zu vermeiden;
- der Wahrscheinlichkeit des Auftretens des gefährlichen Vorfalls, ohne das Vorhandensein irgendeines sicherheitsbezogenen Systems (jedoch mit externen Einrichtungen zur Risikominderung) – dieses wird als die "Wahrscheinlichkeit eines unerwünschten Ereignisses" bezeichnet.

Dies führt zu den folgenden vier Risikoparametern:

- Auswirkung des gefährlichen Vorfalls (C);
- Häufigkeit und Zeit des Aufenthalts im Gefahrenbereich (F);
- Möglichkeit, den gefährlichen Vorfall zu vermeiden (P);
- Wahrscheinlichkeit des unerwünschten Ereignisses (W).

Die Risiko-Parameter können festgelegt werden, auf einer qualitativen Grundlage, wie in Tabelle E.1 oder auf einer quantitativen Grundlage, wie in Tabelle E.2. Bei der Entscheidung, für die numerischen Werte im Zusammenhang mit jedem Parameter der Tabelle E.2 wird eine Kalibrierung erforderlich.

E.3 Kalibrierung

Die Ziele der Kalibrierung sind wie folgt:

Die Beschreibung aller Parameter in einer solchen Weise, die es dem SIL-Bewertungs-Team ermöglicht, auf der Grundlage der Merkmale der Anwendung, eine objektive Entscheidung zu treffen;

Die Sicherstellung, dass die SIL-Auswahl für eine Anwendung im Einklang mit den firmeninternen Risikokriterien steht und Berücksichtigung, der Risiken aus anderen Quellen;

Die Ermöglichung den Prozess der Parameterauswahl zu verifizieren.

Die Kalibrierung des Risikographen ist das Verfahren der Zuordnung von numerischen Werten zu den Parametern des Risikographen. Dies bildet die Grundlage für die Beurteilung des vorhandenen Prozessrisikos, und erlaubt die Bestimmung der erforderlichen Integrität der berücksichtigten sicherheitstechnischen Funktion. Jedem der Parameter wird eine Reihe von Werten zugeordnet, so dass sich bei der Anwendung in Kombination eine abgestufte Bewertung des Risikos, ohne die jeweilige Sicherheitsfunktion, ergibt. So wird ein Maß für den Grad des Vertrauens das in die SIF zu setzen ist, bestimmt. Der Risikograph stellt im einzelnen Beziehungen zwischen Kombinationen von Risiko-Parametern und den Sicherheits-Integritätsleveln her. Die Beziehung zwischen der Kombination der Risikoparameter und Sicherheits-Integritätsleveln wird durch die Berücksichtigung des tolerierbaren Risikos in Zuordnung zur bestimmten Gefährdung, erreicht.

Bei der Berücksichtigung der Kalibrierung des Risikographen ist es wichtig, die Anforderungen in Bezug auf das Risiko, die aus den Erwartungen von sowohl der Eigentümer und den Anforderungen einer Regulierungsbehörde entstehen, in Betracht zu ziehen. Die Risiken für das Leben können in einer Reihe von Möglichkeiten, wie in A.2 und Anhang C beschrieben, betrachtet werden.

Falls es notwendig ist, die Häufigkeit eines einzelnen Todesfalls auf ein bestimmtes Maximum zu reduzieren, dann kann nicht davon ausgegangen werden, dass die gesamte Risikominderung einem einzigen SIS übertragen werden kann. Die exponierten Personen sind einem breiten Spektrum von Risiken ausgesetzt, die sich aus anderen Quellen (z. B. Sturz-, Brand- und Explosionsgefahren), bilden. Bei der Kalibrierung ist die Zahl der Gefährdungen denen Personen ausgesetzt sind und die gesamte Zeit der Gefährdungsdauer zu berücksichtigen.

Bei der Betrachtung des erforderlichen Ausmaßes der Risikominderung, kann eine Organisation Kriterien, in Bezug auf die zusätzlichen Kosten für die Verhinderung eines Todesfalls, haben. Dies kann durch Division der jährlichen Kosten für die zusätzliche Hardware- und Ingenieurleistung für die zusätzliche Risikominderung im Zusammenhang mit einem höheren Maß an Integrität berechnet werden. Eine weitere Ebene der Integrität ist gerechtfertigt, wenn die zusätzlichen Kosten für die Vermeidung eines Todesfalls geringer sind als ein bestimmter Betrag.

Die oben genannten Fragen sind zu berücksichtigen bevor die Parameterwerte festgelegt werden können. Die meisten der Parameter sind einem Wertebereich zugeordnet (z. B. wenn die erwartete Anforderungsrate für einen bestimmten Prozess zwischen einem Dekaden-Bereich pro Jahr liegt, dann kann W3 verwendet werden). Ähnlich für Anforderungen im unteren Dekaden-Bereich, für die W2 gelten würde und für Anforderungen im nächst unteren Dekadenbereich für den W1 gilt. Die Zuweisung der einzelnen Parameter zu einem bestimmten Bereich unterstützt das Team bei der Auswahl des Parameterwerts für eine bestimmte Anwendung. Um den Risikographen zu kalibrieren werden den Parametern Werte oder Wertebereiche zugewiesen. Das der Parameterkombinationen zugeordnete Risiko wird dann gegenüber den definierten Risikokriterien beurteilt. Die Parameterbeschreibungen werden dann angepasst, so dass für alle Kombinationen aller Parameterwerte die definierten Risikokriterien erreicht werden. In der Beispielkalibrierung der Tabelle E.2 wird ein Faktor "D" eingeführt, um den Bereich der Anforderungsraten im Zusammenhang mit jedem W-Faktor so anzupassen, dass ein tolerierbares Risiko erreicht wird. In einigen Fällen sollten Bereiche die anderen Risikofaktoren zugeordnet sind, angepasst werden, um den Parameterwerten in der Breite der zu berücksichtigen Anwendungen gerecht zu werden. Die Kalibrierung ist ein iterativer Prozess und wird solange fortgesetzt, bis die spezifizierten Risikoakzeptanzkriterien für alle Kombinationen von Parameterwerten erfüllt sind.

Die Kalibrierung ist nicht bei jeder SIL-Bestimmung, für eine spezielle Anwendung, erneut durchzuführen. Diese Arbeit ist in der Regel nur für Organisationen einmal notwendig, für ähnliche Gefährdungen. Anpassungen können für bestimmte Projekte notwendig werden, wenn sich die ursprünglichen Annahmen, die während der Kalibrierung gemacht wurden, als ungültig für ein bestimmtes Projekt herausstellen.

Wo Parameterzuweisungen getroffen werden, sollten Informationen zur Verfügung stehen, wie diese Werte hergeleitet wurden.

Es ist wichtig, dass dieser Prozess der Kalibrierung mit einer höheren Ebene innerhalb der Organisation, die die Verantwortung für die Sicherheit trägt, abgestimmt wird. Die getroffenen Entscheidungen bestimmen die erreichte Gesamtsicherheit.

In der Regel wird es für einen Risikographen schwierig sein die Möglichkeit abhängiger Ausfälle zwischen den Quellen einer Anforderung und dem SIS zu berücksichtigen. Dies kann daher zu einer Überschätzung der Wirksamkeit des SIS führen. Wenn Risikographen kalibriert sind um höhere Anforderungsraten als einmal pro Jahr zu beinhalten, können die SIL-Anforderungen die sich aus der Verwendung des Risikographen ergeben höher als notwendig sein, und es wird die Verwendung anderer Verfahren empfohlen.

E.4 Mögliche andere Risikoparameter

Die oben festgelegten Risikoparameter werden als ausreichend allgemein gültig betrachtet, um einen weiten Anwendungsbereich abzudecken. Es können jedoch Anwendungen existieren, die Aspekte enthalten, die die Einführung zusätzlicher Risikoparameter erforderlich machen. Zum Beispiel die Verwendung neuer Technologien in dem EUC-Leit- oder Steuerungssystem. Der Zweck zusätzlicher Parameter würde eine genauere Einschätzung der notwendigen Risikominderung sein (siehe Bild A.1).

E.5 Anwendung des Risikographen: allgemeines Schema

Die Kombination der oben beschriebenen Risikoparameter ermöglicht es, einen Risikographen wie in Bild E.1 zu entwickeln. Bezogen auf Bild E.1 gilt: $C_A < C_B < C_C < C_D$; $F_A < F_B$; $P_A < P_B$;$W_1 < W_2 < W_3$. Erklärung des Risikographen:

- Die Verwendung der Risikoparameter *C*, *F* und *P* führt zu einer Anzahl von Ergebnissen X_1, X_2, X_3..... X_n (die genaue Anzahl hängt von dem vom Risikographen abzudeckenden besonderen Anwendungsgebiet ab). Bild E.1 zeigt die Situation ohne zusätzliche Wichtung für ernsthaftere Auswirkungen. Jedes Einzelergebnis ist auf eine von drei Skalen abgebildet (W_1, W_2 und W_3). Jeder Punkt dieser Skalen ist ein Anhaltspunkt für die erforderliche Sicherheitsintegrität, die durch das betrachtete sicherheitsbezogene E/E/PE-System erreicht werden muss. In der Praxis gibt es Situationen, in denen für bestimmte Auswirkungen ein einzelnes sicherheitsbezogenes E/E/PE-System nicht ausreicht, um die notwendige Risikominderung zu gewährleisten.
- Die Abbildung auf W_1, W_2 oder W_3 lässt einen Beitrag anderer Maßnahmen zur Risikominderung zu. Die Verschiebung der Skalen für W_1, W_2 oder W_3 erlaubt es, drei unterschiedliche Stufen zur Risikominderung durch andere Maßnahmen zu berücksichtigen. Das bedeutet, dass die Skala W_3 für einen kleinsten Beitrag durch andere Maßnahmen zur Risikominderung steht (d. h., die höchste Wahrscheinlichkeit des unerwünschten Beitrags ist vorhanden), die Skala W_2 für einen mittleren Beitrag und die Skala W_1 für einen höchsten Beitrag. Für ein bestimmtes Zwischenergebnis des Risikographen (d. h. X_1, X_2... oder X_6) und für ein bestimmtes Maß von *W* (d.h. W_1, W_2 oder W_3) gibt das Endergebnis des Risikographen den Sicherheits-Integritätslevel des sicherheitsbezogenen E/E/PE-Systems (d. h. 1,2,3 oder 4) an und ist ein Maß für die geforderte Risikominderung für dieses System. Zusammen mit den Risikominderungen anderer Maßnahmen, die durch den Mechanismus der *W*-Skalen berücksichtigt werden (z.B. durch sicherheitsbezogene Systeme anderer Technologie und externe Einrichtungen zur Risikominderung), liefert diese Risikominderung die für die bestimmte Situation notwendige Risikominderung.

Es kann notwendig sein, die in Bild E.1 aufgezeigten Parameter (C_A, C_B, C_C, C_D, F_A, F_B, P_A, P_B, W_1, W_2, W_3) und ihre Gewichtungen für jede bestimmte Situation oder jeden bestimmten Bereich vergleichbarer Industrien genau festzulegen. Außerdem kann es notwendig sein, diese in anwendungsbezogenen Internationalen Normen festzulegen.

E.6 Beispiel eines Risikographen

Ein Beispiel der Anwendung des Risikographen, das auf den Beispieldaten in Tabelle E.1 beruht, ist in Bild E.2 dargestellt. Die Verwendung der Risikoparameter *C*, *F* und *P* führt zu einem von acht Ergebnissen. Jedes einzelne Ergebnis ist auf eine von drei Skalen abgebildet (W_1, W_2 und W_3). Jeder Punkt auf diesen Skalen (a, b, c, d, e, f, g und h) ist ein Anhaltspunkt für die notwendige Risikominderung, die durch das sicherheitsbezogene System erreicht werden muss.

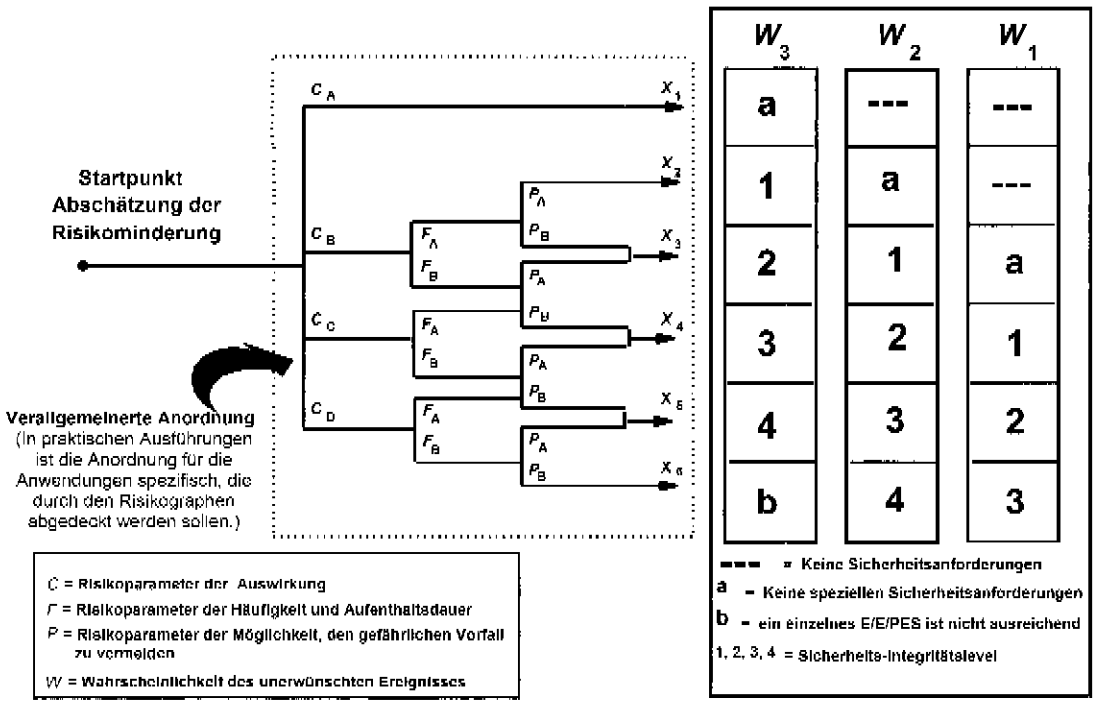


Bild E.1 – Risikograph: Allgemeine Darstellung

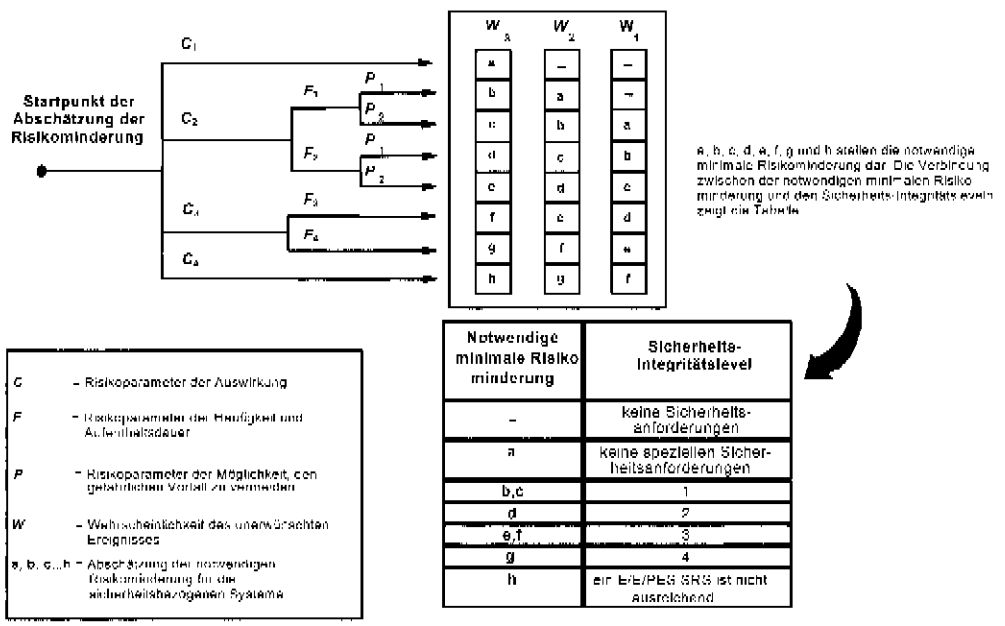


Bild E.2 – Risikograph: Beispiel (zeigt nur allgemeine Prinzipien auf)

Tabelle E.1 – Beispieldaten, die sich auf das Beispiel des Risikographen (Bild E.2) beziehen

Risikoparameter		Klassifizierung	Erläuterungen
Auswirkung (*C*)	C_1	Geringe Verletzung	1 Das Klassifizierungssystem ist entwickelt worden, um Verletzungen und Tod von Personen zu berücksichtigen. Für Umwelt- und Materialschäden müssten andere Klassifizierungsverfahren entwickelt werden. 2 Bei der Interpretation von C_1, C_2, C_3 und C_4 müssen die Auswirkungen des Unfalls und normale Heilungsprozesse betrachtet werden.
	C_2	Schwere irreversible Verletzung einer oder mehrerer Personen; Tod einer Person	
	C_3	Tod mehrerer Personen	
	C_4	Tod sehr vieler Personen	
Häufigkeit und Aufenthaltsdauer im gefährlichen Bereich (*F*)	F_1	Seltener bis häufiger Aufenthalt im gefährlichen Bereich	3 Siehe Anmerkung 1 oben.
	F_2	Häufiger bis dauernder Aufenthalt im gefährlichen Bereich	
Möglichkeit, den gefährlichen Vorfall zu vermeiden (*P*)	P_1	Möglich unter bestimmten Bedingungen	4 Dieser Parameter zieht in Betracht: – Betrieb eines Prozesses (überwacht (d. h. betrieben durch ausgebildete oder nicht ausgebildete Personen) oder nicht überwacht); – Geschwindigkeit der Entwicklung des gefährlichen Vorfalls (z. B. plötzlich, schnell, langsam); – Leichtigkeit der Erkennung der Gefahr (z. B. unmittelbar erkennbar, durch technische Maßnahmen aufgedeckt, ohne technische Maßnahmen aufgedeckt); Vermeidung des gefährlichen Vorfalls (z. B. Fluchtwege möglich, nicht möglich oder unter bestimmten Bedingungen möglich); aktuelle Sicherheitserfahrung (diese Erfahrung kann von identischen oder ähnlichen EUC oder ähnlichen EUC herrühren, oder kann nicht vorhanden sein).
	P_2	Beinahe unmöglich	
Wahrscheinlichkeit des unerwünschten Ereignisses (*W*)	W_1	Eine sehr geringe Wahrscheinlichkeit, dass die unerwünschten Ereignisse auftreten, und nur wenige unerwünschte Ereignisse sind wahrscheinlich.	5 Der Faktor "*W*" dient zur Bestimmung der Häufigkeit des unerwünschten Ereignisses, ohne die Berücksichtigung jeglicher sicherheitsbezogener Systeme (E/E/PE oder andere Technologie), aber unter Berücksichtigung der externen Einrichtungen zur Risikominderung. 6 Wenn wenig oder gar keine Erfahrungen mit der EUC oder einem ähnlichen EUC oder EUC Leit- oder Steuerungssystem bestehen, kann die Bestimmung des Faktors "*W*" durch Berechnung erfolgen. In solchen Fällen muss eine "Worst Case"-Vorhersage gemacht werden.
	W_2	Eine geringe Wahrscheinlichkeit, dass die unerwünschten Ereignisse auftreten, und wenige unerwünschte Ereignisse sind wahrscheinlich.	
	W_3	Eine relativ hohe Wahrscheinlichkeit, dass die unerwünschten Ereignisse auftreten, und häufige unerwünschte Ereignisse sind wahrscheinlich.	

Tabelle E.2 – Beispielkalibrierung eines allgemeinen Risikographen

Riskoparameter		Klassifizierung	Erläuterungen
Auswirkung (C) Anzahl der Todesopfer Diese kann berechnet werden durch die Bestimmung der Anzahl vorhandener Personen, wenn der exponierte Bereich für die Gefährdung besetzt wird und der Multiplikation mit der Anfälligkeit für die ermittelte Gefährdung. Die Schwachstelle wird bestimmt durch die Art der Gefährdung gegen die diese geschützt werden soll. Die folgenden Faktoren können verwendet werden: V=0,01 Geringe Freisetzung von brennbaren oder toxischen Stoffen V=0,1 Größere Freisetzung von brennbaren oder toxischen Stoffen V= 0,5 Wie oben, aber auch eine hohe Wahrscheinlichkeit Feuer zu fangen oder sehr giftige Stoffe V=1 Bruch oder Explosion	C_A C_B C_C C_D	Geringe Verletzung Bereich 0,01 bis 0,1 Bereich >0,1 bis 1,0 Bereich > 1,0	1 Das Klassifizierungssystem ist entwickelt worden, um Verletzungen und Tod von Personen zu berücksichtigen. 2 Bei der Interpretation von C_A, C_B, C_C und C_D müssen die Auswirkungen des Unfalls und normale Heilungsprozesse betrachtet werden.
Aufenthaltsdauer (F) Diese wird berechnet, durch die Bestimmung des proportionalen Zeitraums den ein exponierter Bereich für die Gefährdung während eins normalen Arbeitstags ausgesetzt ist. ANMERKUNG 1 – Wenn die Zeit im Gefährdungsbereich von der Arbeitsschicht abhängt, dann sollte das Maximum gewählt werden. ANMERKUNG 2 – F_A zu verwenden ist nur dann angemessen wenn nachgewiesen werden kann, dass die Anforderungsrate zufällig ist und die Aufenthaltsdauer nicht höher als normal. Letzteres ist in der Regel der Fall bei Anforderungen, die auftreten bei Inbetriebnahmen von Einrichtungen und oder bei der Untersuchung von Störungen.	F_A F_B	Seltener bis häufiger Aufenthalt im gefährlichen Bereich Aufenthaltsdauer kleiner als 0,1 Häufiger bis dauernder Aufenthalt im gefährlichen Bereich	3 Siehe Anmerkung 1 oben.
Möglichkeit, den gefährlichen Vorfall zu vermeiden (P) wenn das Schutzsystem ausgefallen ist.	P_A P_B	Gewählt, wenn alle Bedingungen in Spalte 4 erfüllt sind Gewählt, wenn alle Bedingungen nicht erfüllt sind.	4 P_A sollte nur gewählt werden, wenn alle folgenden Bedingungen erfüllt sind: Anlagen zur Verfügung stehen, um den Betreiber anzuzeigen, dass die SIS ausgefallen ist, unabhängige Einrichtungen stehen bereit für eine Abschaltung, so dass die Gefährdung vermieden werden kann oder, die allen Personen die Flucht in einen sicheren Bereich ermöglichen – die Zeit zwischen der Warnung des Bedieners und eines auftretenden gefährlichen Ereignisses mehr als eine Stunde beträgt oder definitiv ausreicht für erforderliche Maßnahmen

Tabelle E.2 *(fortgesetzt)*

Riskoparameter		Klassifizierung	Erläuterungen
Die Anforderungsrate (W) Die Anzahl der gefährlichen Vorfälle die pro Jahr auftretenden würden ohne ein SIS. Für die Ermittlung der Anforderungsrate es ist notwendig alle Quellen eines Ausfalls zu bestimmen, die zu einem gefährlichen Vorfall führen können. Bei der Bestimmung der Anforderungsrate kann begrenztes Vertrauen zugelassen werden, an die Leistungsfähigkeit der Steuerung und deren Eingreifen. Die Leistungsfähigkeit, die geltend gemacht werden kann, wenn die Steuerung nicht nach der IEC 61511 entworfen und betrieben wird, ist auf weniger als die Leistungsfähigkeit von SIL1beschränkt.	W_1 W_2 W_3	Anforderungsrate kleiner als 0,1W pro Jahr Anforderungsrate zwischen 0,1W und W pro Jahr Anforderungsrate zwischen W und 10W pro Jahr Für Anforderungsraten größer als 10W pro Jahr wird eine höhere Integrität benötigt	5 Der Zweck der W-Faktor ist die Schätzung der Häufigkeit der Gefährdung die ohne den Zusatz einer SIS erfolgen würde Wenn die Anforderungsrate sehr hoch ist, ist der SIL durch eine andere Methode zu bestimmen oder der Gefahrengraph ist neu zu kalibrieren. Es sollte darauf hingewiesen werden, dass die Risikograph-Methoden möglicher weise nicht der beste Ansatz für Anwendungen mit kontinuierlicher Anforderung (IEC 61511-1. Abschnitt 3.1.48.2) sind. 6. Der Wert von W sollte bestimmt werden durch Unternehmenskriterien für tolerierbare Risiken unter Berücksichtigung anderer Risiken für die gefährdeten Personen.
ANMERKUNG Dies ist ein Beispiel um die Anwendung der Grundsätze für den Entwurf von Risikographen zu zeigen. Risikographen für bestimmte Anwendungen und besondere Gefahren müssen mit den Beteiligten vereinbart werden unter Berücksichtigung des tolerierbaren Risikos, siehe E.1 bis E.6.			

Anhang F
(informativ)

Semi-quantitative Methode, Verwendung einer Analyse der Schutzebenen (LOPA)

F.1 Allgemeines

F.1.1 Beschreibung

Diese Anlage beschreibt eine Methode, die der Analyse von Schutzebenen (LOPA), ist jedoch nicht gedacht als endgültige Beschreibung der Methode, sondern um die allgemeinen Grundprinzipien zu zeigen.

F.1.2 Anhang Verweis

Dieser Anhang stützt sich auf eine Methode, die im Detail in der AIChE "Layer of Protection Analysis – Simplified Process Risk Assessment" beschrieben ist (siehe Verweis [5] der Literaturhinweise). Dieser Verweis zeigt viele Möglichkeiten zur Anwendung des LOPA-Verfahrens.

In einem Ansatz, werden alle relevanten Parameter auf den nächsthöheren Dekaden Bereich aufgerundet (z. B. eine Wahrscheinlichkeit von $5 \cdot 10^{-2}$ wird auf 10^{-1} aufgerundet). Dies ist ein sehr konservativer Ansatz und kann zu deutlich höheren SIL-Ebenen führen. Unsicherheiten von Daten sollten gewürdigt werden durch Rundung aller Parameterwerte auf die nächst höhere signifikante Ziffer (z. B. $5{,}4 \cdot 10^{-2}$ sollte gerundet werden auf $6 \cdot 10^{-2}$).

F.1.3 Beschreibung der Methode

LOPA analysiert Gefährdungen um festzustellen, ob Sicherheitsfunktionen erforderlich sind und wenn ja, den erforderlichen SIL für jede Sicherheitsfunktion. Um die LOPA-Methode anwenden zu können wird eine Anpassung notwendig sein um die Risiko-Akzeptanzkriterien erfüllen zu können. Das Verfahren beginnt mit den Daten die bei der Identifikation der Gefährdungen ermittelt wurden und berechnet für jede ermittelte Gefährdung durch Dokumentation die auslösenden Ursachen und Schutzebenen die die Gefährdung vermeiden oder mindern. Der Gesamtbetrag der Risikominderung kann dann bestimmt und die Notwendigkeit einer weiteren Risikominderung analysiert werden. Wenn eine zusätzliche Risikominderung erforderlich ist, und wenn dies in Form eines E/E/PES erfolgt, ermöglicht die LOPA-Methode die Bestimmung des geeigneten SIL. Für jede Gefährdung wird ein geeigneter SIL zur Verringerung der Risiken auf ein tolerierbares Niveau bestimmt. Die Tabelle F.1 zeigt ein typisches LOPA-Format.

F.2 Schadensereignis

Bei Verwendung der Tabelle F.1, wird jede Beschreibung eines Schadensereignisses (Auswirkung), bestimmt durch die Identifikation der Gefährdung, in Spalte 1 der Tabelle F.1 eingetragen.

F.3 Schweregrad

Der Schweregrad des Ereignisses wird in Spalte 2 der Tabelle F.1 eingetragen. Der Schweregrad wird aus einer Tabelle abgeleitet die allgemeine Auswirkungsstufen beschreibt z.B. gering, ernst, katastrophal, mit bestimmten Bereichen der Auswirkung und der maximalen Häufigkeit für jeden Schweregrad. Als Ergebnis legt diese Tabelle Anwender-Toleranzkriterien fest. Es werden Informationen benötigt die es erlauben den Schweregrad und maximale Häufigkeit zu bestimmen die zu Ereignissen mit Konsequenzen für die Sicherheit und Folgen für die Umwelt führen.

F.4 Auslösende Ursache

Alle auslösenden Ursachen des Schadensereignisses werden in Spalte 3 der Tabelle F.1 eingetragen. Schadensereignisse können viele auslösende Ursachen haben und alle sollten aufgeführt werden.

F.5 Eintrittswahrscheinlichkeit

Die Wahrscheinlichkeitswerte jeder der in Spalte 3 der Tabelle F.1 eingetragenen, einleitenden Ursachen, werden in Ereignissen pro Jahr, in Spalte 4 der Tabelle F.1 eingegeben.

Die Eintrittswahrscheinlichkeit kann berechnet werden durch typische Daten der Ausfallraten der Ausrüstung und der Kenntnis der Intervalle für die Wiederholungsprüfungen, oder von Aufzeichnungen über die Einrichtung. Eine geringe Eintrittswahrscheinlichkeit sollte nur verwendet werden, wenn es ausreichende statistische Grundlagen für die Daten gibt.

Tabelle F.1 – LOPA-Report

Schweregrad C = Katastrophal, E = Extrem, S = Bedeutend, M = Gering *Wahrscheinlichkeitswerte sind Ereignisse pro Jahr. Andere numerische Werte sind Durchschnittswahrscheinlichkeiten des Ausfalls bei Anfrage.*													
Ref	**1**	**2**	**3**	**4**	**5**			**6**	**7**	**8**	**9**	**10**	**11**
					Schutzebenen (PLs)								
	Beschreibung des Schadensereignisses F.2	Schweregrad F.3	Auslösende Ursache F.4	Eintrittswahrscheinlichkeit F.5	Allgemeiner Entwurf F.6.1	Steuerungssystem F.6.2	Alarme, usw. F.6.3	Zusätzliche Schadensbegrenzungsmaßnahmen, beschränkter Zugriff F.7	Zusätzliche Schadensbegrenzungsmaßnahmen F.8	Vorläufige Wahrscheinlichkeit für das Ereignis F.9	PFD_{avg} erforderlich für das E/E/PES (und SIL) F.10	Wahrscheinlichkeit der Schadensminderung F.11	Anmerkungen
1	Überhöhte Geschwindigkeit des Rotors führt zum Bruch des Gehäuses	Verlust des Lebens von Personen, die der Nähe zum benachbarten Gehäuse, Todesfälle überschreiten nicht 2	Geschwindigkeitsregelung ausgefallen	0,1	1	1	1	0,1	0,1	10^{-3}	$5 \cdot 10^{-3}$ (SIL 2 mit einer minimalen PFD_{avg} von $5 \cdot 10^{-3}$)	10^{-5}	
			Verlust der Last	1	1	0,1	1	0,1	0,1	10^{-3}			
			Ausfall der Kupplung	0,1	1	0,1	1	0,1	0,1	10^{-4}			
						0,1 Vertrauen an das Steuerungssystem		Aufenthaltsdauer begrenzt, 90% der Zeit keine Personen anwesend	Todesfall tritt nur ein wenn Fragmente Personen treffen	Gesamt $2{,}1 \cdot 10^{-3}$		Tolerierbare Häufigkeit von Todesfällen wenn 5 nicht überschritten	

Tabelle F.1 *(fortgesetzt)*

Schweregrad C = Katastrophal, E = Extrem, S = Bedeutend, M = Gering									
Wahrscheinlichkeitswerte sind Ereignisse pro Jahr. Andere numerische Werte sind Durchschnittswahrscheinlichkeiten des Ausfalls bei Anfrage.									
2	Wiederholung des obigen Falls zu Umweltrisiken								
3				Fortsetzung bei Bedarf.					
.									
.									
N									

ANMERKUNG 1 Die Einheiten in den Spalten 3, 8 und 10 sind Ereignisse pro Jahr.

ANMERKUNG 2 Die Einheiten in den Spalten 4 – 7 und 9 sind dimensionslos. Diese Zahlenwerte, zwischen 0 und 1, sind Faktoren mit denen die Wahrscheinlichkeit multipliziert werden kann um den Effekt der Minderung der zugehörigen Schutzebene darzustellen. So bedeutet 1, keinen mindernden Effekt und 0,1 ist ein Faktor von 10 der Risikominderung

F.6 Schutzebenen (PLs)

F.6.1 Allgemeines

Jede PL besteht aus einer Gruppe von Einrichtungen und/oder administrativen Kontrollen die von anderen Schichten unabhängig funktionieren.

Merkmale des Entwurfs zur Verringerung der Wahrscheinlichkeit eines Schadensereignisses, das bei einer auslösenden Ursache auftritt, werden zuerst in der Spalte 5 der Tabelle F.1 beschrieben.

Die PLs sollten folgende wichtigen Merkmale aufweisen:

- **Bestimmtheit:** Eine PL ist ausschließlich entworfen worden zur Verhinderung oder Minderung der Auswirkungen eines potenziell gefährlichen Vorfalls (z. B. ein außer Kontrolle geraten, die Freisetzung von giftigen Materialien, ein Bruch einer Sicherheitshülle, oder ein Feuer). Mehrere Ursachen können zum gleichen gefährlichen Vorfall führen und daher können mehrere Ereignisszenarien die Aktion einer PL auslösen.
- **Unabhängigkeit:** Eine PL ist unabhängig von den anderen PLs im Zusammenhang mit dem festgestellten gefährlichen Vorfall.
- **Zuverlässigkeit:** Es darf davon ausgegangen werden, dass die PL tun wird, wofür sie entworfen worden ist. Beides, zufällige und systematische Ausfälle werden im Entwurf berücksichtigt.
- **Prüfbarkeit:** Eine PL wird entworfen um die regelmäßige Validierung der Schutzfunktionen zu ermöglichen. Wiederholungsprüfungen und die Instandhaltung des Sicherheitssystems sind erforderlich.

F.6.2 Grundlegendes Steuerungssystem

Der nächste Punkt in der Spalte 5 der Tabelle F.1 ist das EUC-Leit- oder Steuerungssystem. Wenn eine Steuerungsfunktion das Auftreten eines Schadensereignisses verhindert, sollte die auslösende Ursache auftreten, dann wird das Vertrauen auf der Grundlage der PFD_{avg} in Anspruch genommen. Es sollte kein Vertrauen für eine Steuerungsfunktion geltend gemacht werden können, wenn der Ausfall der Funktion eine Anforderung an das E/E/PES ergeben würde. Es sollte auch darauf hingewiesen werden, dass die beanspruchte PFD_{avg} einer Steuerungsfunktion auf das Minimum von 0,1 begrenzt werden sollte wenn die Steuerungsfunktion nicht als Sicherheitssystem entworfen wurde und als solches betrieben wird.

F.6.3 Alarme

Der letzte Punkt in der Spalte 5 der Tabelle F.1 legt Vertrauen in den Alarm, die Alarmierung des Bedieners veranlasst diesen zum Eingreifen. Vertrauen an Alarme sollte nur unter folgenden Umständen geltend gemacht werden:

- Die verwendete Hardware- und Software ist getrennt und unabhängig von der des Steuerungssystems (z.B. sollten Eingangskarten und Prozessoren nicht gemeinsam verwendet werden).
- Der Alarm wird mit einer hohen Priorität in einer ständig besetzten Stelle angezeigt. Vertrauen in einen Alarm sollte die folgenden Aspekte berücksichtigen:
  - ✓ Die Wirksamkeit eines Alarms hängt von der Komplexität der Aufgabe ab die durchgeführt werden soll falls der Alarm auftritt und den anderen Aufgaben die zur gleichen Zeit durchgeführt werden müssen.
  - ✓ Das Vertrauen sollte auf ein Mindestmaß der PFD_{avg} von 0,1 beschränkt werden.
  - ✓ Der Bediener benötigt genügend Zeit und unabhängige Einrichtungen, um die Gefährdung zu beenden. Normalerweise sollte kein Vertrauen geltend gemacht werden, es sei denn, die Zeit zwischen dem Alarm und der Gefährdung beträgt mehr als 15 Minuten.

F.7 Zusätzliche Schadensbegrenzungsmaßnahmen

Schadensbegrenzungsebenen sind üblicherweise mechanischer, struktureller oder verfahrenstechnischer Art. Beispiele beinhalten:

- Beschränkter Zugang;
- Reduzierung der Wahrscheinlichkeit einer Entzündung;
- Alle anderen Faktoren die die Schwachstelle, welche Personen einer Gefährdung aussetzt, verringern.

Schadensbegrenzungsebenen können die Schwere der Auswirkungen des Schadensereignisses mildern, aber nicht verhindern, dass das Ereignis auftritt. Beispiele sind:

- Flutungssysteme in den Fall eines Brandes;
- Gasalarme;
- Evakuierungsverfahren würden zu einer Verringerung der Wahrscheinlichkeit führen, dass Personen der Eskalation eines Ereignisses ausgesetzt werden.

Bei der Schadensbegrenzung kann der prozentuale Anteil der am stärksten exponierten Personen in der Gefahrenzone berücksichtigt werden. Dieser Prozentsatz sollte durch die Festlegung der Anzahl der Stunden in der Gefahrenzone pro Jahr, geteilt durch 8760 Stunden pro Jahr, bestimmt werden.

Die angemessene PFD_{avg} oder gleichwertiges für alle Schadensbegrenzungsebenen sollte bestimmt und in Spalte 6 und 7 der Tabelle F.1 eingetragen werden.

F.8 Vorläufige Wahrscheinlichkeit für das Ereignis

Die vorläufige Wahrscheinlichkeit für das Ereignis wird durch die Multiplikation der folgenden Faktoren berechnet und das Ergebnis als Häufigkeit pro Jahr, in die Spalte 8 der Tabelle F.1 eingetragen:

- die Verletzbarkeit der am stärksten exponierten Person;
- die Eintrittswahrscheinlichkeit (Spalte 4);
- die PFD_{avg} des PLs, Schadensbegrenzungsebenen und PLs (Spalten 5, 6 und 7).

Die gesamte vorläufige Ereignishäufigkeit sollte berechnet werden, durch Addition der vorläufigen Ereignishäufigkeiten jeder Ursache.

Die gesamte vorläufige Ereignishäufigkeit sollte verglichen werden mit der tolerierbaren Risikohäufigkeit für den damit verbundenen Schweregrad. Wenn die gesamte vorläufige Ereignishäufigkeit über der tolerierbaren Risikohäufigkeit liegt, dann ist eine Risikominderung erforderlich. Eigensichere Methoden und Lösungen sollten berücksichtigt werden, bevor zusätzliche PLs in Form von E/E/PES zum Einsatz kommen.

Wenn die Zahlen der vorläufigen Wahrscheinlichkeit für das Ereignis nicht unter das maximale Häufigkeitskriterium reduziert können, dann wird ein E/E/PES erforderlich.

F.9 Sicherheits-Integritätslevel (SILs)

Wenn eine Sicherheitsfunktion erforderlich ist, kann der erforderliche SIL wie folgt bestimmt werden:

- Zur Bestimmung der erforderlichen PFD_{avg} wird die maximale Häufigkeit des damit verbundenen Schweregrads durch den Gesamtwert der vorläufigen Wahrscheinlichkeit für das Ereignis, dividiert;
- Der numerische Grenzwert der PFD_{avg} kann dann in der Spezifikation der Sicherheitsanforderungen zusammen mit den zugehörigen SIL verwendet werden. Der zugehörige SIL kann aus der Tabelle 2 in Teil 1 entnommen werden.
- Wenn der numerische Wert der PFD_{avg} nicht in der Prozess Anforderungsspezifikation angegeben ist sondern nur der erforderliche SIL, dann sollte der SIL einen Level höher sein, so dass eine angemessene Risikominderung erreicht werden kann mit allen Werten der PFD_{avg} im Zusammenhang mit dem angegebenen SIL.

– Wenn der erforderliche PFD_{avg} für das tolerierbare Risiko größer als 0,1 ist, dann wird die Funktion der Einstufung "Keine besonderen Anforderungen an die Sicherheitsintegrität" zugeordnet.

Anhang G
(informativ)

Festlegung der Sicherheits-Integritätslevel – Eine qualitative Vorgehensweise: Matrix des Ausmaßes des gefährlichen Vorfalls

G.1 Allgemeines

Die in Anhang D beschriebene numerische Methode kann nicht angewendet werden, wenn das Risiko (oder dessen Anteil „Häufigkeit") nicht quantifiziert werden kann. Dieser Anhang beschreibt die qualitative Methode "Matrix des Ausmaßes des gefährlichen Vorfalls", die es ermöglicht, die Festlegung des Sicherheits-Integritätslevels eines sicherheitsbezogenen E/E/PE-Systems aus den Kenntnissen über die Risikofaktoren, die mit der EUC und dem EUC-Leit- oder Steuerungssystem verbunden sind, zu bestimmen. Diese Methode ist insbesondere anwendbar, wenn das Risikomodell demjenigen der Bilder A.1 und A.2 entspricht.

Das in diesem Anhang beschriebene Schema nimmt an, dass jedes sicherheitsbezogene System und jede andere Maßnahme zur Risikominderung unabhängig ist.

Dieser Anhang ist nicht als eine endgültige Beschreibung der Methode vorgesehen, sondern zur Erläuterung der allgemeinen Prinzipien, wie solch eine Matrix von denjenigen entwickelt werden kann, die ausreichende Kenntnis von den in Betracht zu ziehenden Parametern haben. Diejenigen, die beabsichtigen, die in diesem Anhang aufgeführten Methoden anzuwenden, sollten das angegebene Quellenmaterial zu Rate ziehen.

ANMERKUNG Für weitere Informationen zur Matrix des gefährlichen Vorfalls siehe Anhang F [1] der Literaturhinweise.

G.2 Matrix des Ausmaßes des gefährlichen Vorfalls

Die folgenden Anforderungen sind die Grundlage der Matrix. Damit die Methode gültig ist, ist die Übereinstimmung mit jeder einzelnen der folgenden Anforderungen notwendig:

a) die sicherheitsbezogenen Systeme (E/E/PE und andere Maßnahmen zur Risikominderung) sind unabhängig;

b) jedes sicherheitsbezogene System (E/E/PE und andere Technologie) und andere Maßnahmen zur Risikominderung werden als Schutzebenen betrachtet, die, wie in Bild A.1 gezeigt, selbst einen Anteil zur Risikominderung beisteuern;

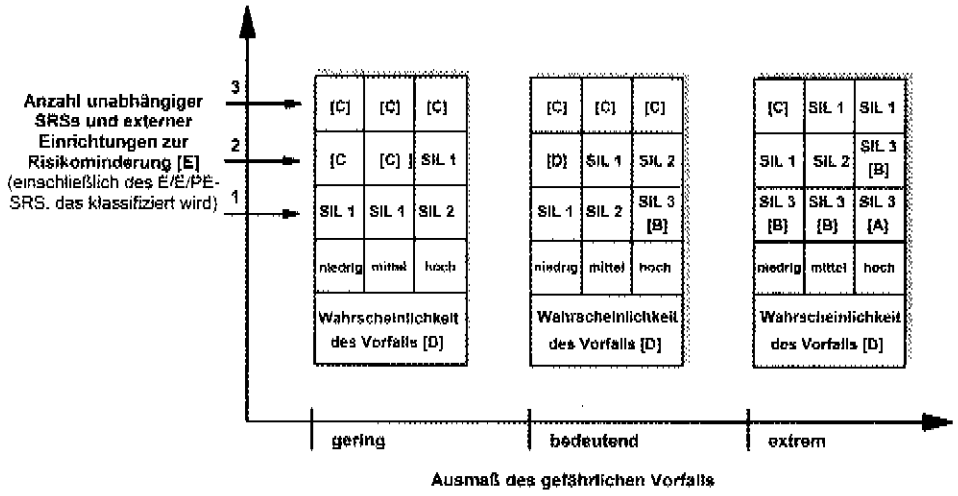
ANMERKUNG 1 Diese Annahme ist nur gültig, falls reguläre Nachweisprüfungen der Schutzebenen durchgeführt werden.

c) wenn eine Schutzebene (siehe b) oben) hinzugefügt wird, dann wird eine Verbesserung der Sicherheitsintegrität um eine Größenordnung erreicht;

ANMERKUNG 2 Diese Annahme ist nur gültig, falls die sicherheitsbezogenen Systeme und die externen Einrichtungen zur Risikominderung eine angemessene Ebene der Unabhängigkeit aufweisen.

d) nur ein sicherheitsbezogenes E/E/PE-System wird verwendet (aber dies kann in Verbindung mit einem sicherheitsbezogenen System anderer Technologie und/oder externen Einrichtungen zur Risikominderung auftreten), für das diese Vorgehensweise den notwendigen Sicherheits-Integritätslevel bestimmt;

e) die oben angegebenen Betrachtungen führen zur "Matrix des Ausmaßes des gefährlichen Vorfalls", die in Bild G.1 gezeigt wird. Es sollte beachtet werden, dass die Matrix mit Beispieldaten ausgefüllt wurde, um die allgemeinen Prinzipien aufzuzeigen. Für jede besondere Situation oder jeden bestimmten Bereich vergleichbarer Industrien kann eine Matrix ähnlich derjenigen in Bild G.1 entwickelt werden.



[A] Ein SIL 3 sicherheitsbezogenes E/E/PE-System liefert in dieser Stufe keine ausreichende Risikominderung. Zusätzliche Maßnahmen zur Risikominderung sind erforderlich.
[B] Ein SIL 3 sicherheitsbezogenes E/E/PE-System könnte in dieser Stufe keine ausreichende Risikominderung liefern. Eine Gefährdungs- und Risikoanalyse ist erforderlich, um festzustellen, ob zusätzliche Maßnahmen zu Risikominderung erforderlich sind.
[C] Ein unabhängiges sicherheitsbezogenes E/E/PE-System ist wahrscheinlich nicht erforderlich.
[D] Die Wahrscheinlichkeit des Ereignisses ist die Wahrscheinlichkeit für das Auftreten des gefahrlichen Vorfalls, ohne jegliches sicherheitsbezogenes System oder jegliche externe Einrichtung zur Risikominderung.
[E] Die Wahrscheinlichkeit des Vorfalls und die Gesamtanzahl unabhängiger Schutzschichten sind in Bezug zu ihrer spezifischen Anwendung definiert.

Bild G.1 – Matrix des Ausmaßes des gefährlichen Vorfalls: Beispiel (stellt nur die allgemeinen Prinzipien dar)

Literaturhinweise

[1] ANSI/ISA S84:1996, *Application of safety Instrumented Systems for the Process Industries*

[2] *Tolerability of risk from nuclear power stations,* Health and Safety Executive (UK) publication, ISBN 011 886368 1

[3] Development guidelines for vehicle based Software, The Motor Industry Reliability Association, Watling St, Nuneaton, Warwickshire, CV10 0TU, United Kingdom, 1994, ISBN 09524156 0 7

[4] Reducing Risks, Protecting People – HSE`s decision making process ISBN 0 7176 2151 0

[5] Layer of Protection Analysis – Simplified Process Risk Assessment – CCPS ISBN 0-8169-0811-7

CONTENTS

INTRODUCTION 5
Annex A (informative) Risk and safety integrity – General concepts 10
Annex B (informative) Selection of methods for determining Safety Integrity Levels 21
Annex C (informative) ALARP and tolerable risk concepts 23
Annex D (informative) Determination of safety integrity levels: a quantitative method 26
Annex E (informative) Determination of safety integrity levels Risk Graph Methods 29
Annex F (informative) Semi-quantitative method using layer of protection analysis (LOPA) 36
Annex G (informative) Determination of safety integrity levels – A qualitative method: hazardous event severity matrix 41
Bibliography 43

Figures

Figure 1 – Overall framework of this standard 8
Figure A.1 – Risk reduction: general concepts (low demand mode of operation) 14
Figure A.2 – Risk and safety integrity concepts 14
Figure A.3 – Risk diagram for high demand applications 15
Figure A.4 – Risk diagram for continuous mode operation 16
Figure A.5 – Illustration of Common Cause Failures (CCFs) of elements in the EUC control system and elements in the E/E/PE safety-related system 17
Figure A.6 – Common cause between two E/E/PEsafety-related systems 18
Figure A.7 – Allocation of safety requirements to the E/E/PE safety-related systems, other technology safety-related systems and external risk reduction facilities 19
Figure C.1 – Tolerable risk and ALARP 24
Figure D.1 – Safety integrity allocation: example for safety-related protection system 28
Figure E.1 – Risk graph: general scheme 32
Figure E.2 – Risk graph: example (illustrates general principles only) 33
Figure G.1 – Hazardous event severity matrix: example (illustrates general principles only) 42

Tables

Table C.1 – Example of risk classification of accidents 25
Table C.2 – Interpretation of risk classes 25
Table E.1 – Example data relating to example risk graph (figure E.2) 34
Table E.2 - Example Calibration of the General Purpose Risk Graph 35
Table F.1 – LOPA report 38

INTERNATIONAL ELECTROTECHNICAL COMMISSION

FUNCTIONAL SAFETY OF ELECTRICAL/ELECTRONIC/PROGRAMMABLE ELECTRONIC SAFETY-RELATED SYSTEMS –

Part 5: Examples of methods for the determination of safety integrity levels

FOREWORD

1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
5) IEC provides no marking procedure to indicate its approval and cannot be rendered responsible for any equipment declared to be in conformity with an IEC Publication.
6) All users should ensure that they have the latest edition of this publication.
7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

International Standard IEC 61508-5 has been prepared by subcommittee 65A: System aspects, of IEC technical committee 65: Industrial-process measurement and control. This second edition cancels and replaces IEC 61508-5: 1998.

It has the status of a basic safety publication according to IEC Guide 104.

The text of this standard is based on the following documents:

FDIS	Report on voting
XX/XX/FDIS	XX/XX/RVD

Full information on the voting for the approval of this standard can be found in the report on voting indicated in the above table.

This publication has been drafted in accordance with the ISO/IEC Directives, Part 2.

IEC 61508 consists of the following parts, under the general title *Functional safety of electrical/electronic/programmable electronic safety-related systems*:

- Part 0: Functional safety and IEC 61508
- Part 1: General requirements
- Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems
- Part 3: Software requirements
- Part 4: Definitions and abbreviations
- Part 5: Examples of methods for the determination of safety integrity levels
- Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3
- Part 7: Overview of techniques and measures

This part 5 should be read in conjunction with part 1.

The committee has decided that the contents of this publication will remain unchanged until the maintenance result date[1)] indicated on the IEC web site under "http://webstore.iec.ch" in the data related to the specific publication. At this date, the publication will be

- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

1) The National Committees are requested to note that for this publication the maintenance result date is 2014

INTRODUCTION

Systems comprised of electrical and/or electronic elements have been used for many years to perform safety functions in most application sectors. Computer-based systems (generically referred to as programmable electronic systems) are being used in all application sectors to perform non-safety functions and, increasingly, to perform safety functions. If computer system technology is to be effectively and safely exploited, it is essential that those responsible for making decisions have sufficient guidance on the safety aspects on which to make these decisions.

This International Standard sets out a generic approach for all safety lifecycle activities for systems comprised of electrical and/or electronic and/or programmable electronic (E/E/PE) elements that are used to perform safety functions. This unified approach has been adopted in order that a rational and consistent technical policy be developed for all electrically-based safety-related systems. A major objective is to facilitate the development of application sector standards.

In most situations, safety is achieved by a number of systems which rely on many technologies (for example mechanical, hydraulic, pneumatic, electrical, electronic, programmable electronic). Any safety strategy must therefore consider not only all the elements within an individual system (for example sensors, controlling devices and actuators) but also all the safety-related systems making up the total combination of safety-related systems. Therefore, while this International Standard is concerned with E/E/PE safety-related systems, it may also provide a framework within which safety-related systems based on other technologies may be considered.

It is recognized that there is a great variety of applications using E/E/PE safety-related systems in a variety of application sectors and covering a wide range of complexity, hazard and risk potentials. In any particular application, the required safety measures will be dependent on many factors specific to the application. This International Standard, by being generic, will enable such measures to be formulated in future application sector international standards and in revisions of those that already exist.

This International Standard

- considers all relevant overall, E/E/PE system and software safety lifecycle phases (for example, from initial concept, through design, implementation, operation and maintenance to decommissioning) when E/E/PE systems are used to perform safety functions;
- has been conceived with a rapidly developing technology in mind; the framework is sufficiently robust and comprehensive to cater for future developments;
- enables application sector international standards, dealing with E/E/PE safety-related systems, to be developed; the development of application sector international standards, within the framework of this standard, should lead to a high level of consistency (for example, of underlying principles, terminology etc.) both within application sectors and across application sectors; this will have both safety and economic benefits;

NOTE 1 References [1] and [2] in the bibliography are application sector international standards.

- provides a method for the development of the safety requirements specification necessary to achieve the required functional safety for E/E/PE safety-related systems;
- adopts a risk-based approach by which the safety integrity requirements can be determined;

  introduces safety integrity levels for specifying the target level of safety integrity for the safety functions to be implemented by the E/E/PE safety-related systems;

NOTE 2 The standard does not specify the safety integrity requirements for any safety function, nor does it mandate how the safety integrity level is determined. Instead it provides a risk-based conceptual framework and example techniques.

- sets target failure measures for safety functions carried out by E/E/PE safety-related systems, which are linked to the safety integrity levels;

  sets a lower limit on the target failure measures for a safety function carried out by a single E/E/PE safety-related system. For E/E/PE safety-related systems operating in

- a low demand mode of operation, the lower limit is set at an average probability of dangerous failure on demand of 10^{-5},
- a high demand or a continuous mode of operation, the lower limit is set at an average frequency of dangerous failure of 10^{-9} [h^{-1}];

NOTE 3 A single E/E/PE safety-related system does not necessarily mean a single-channel architecture.

NOTE 4 It may be possible to achieve designs of safety-related systems with lower values for the target safety integrity for non-complex systems, but these limits are considered to represent what can be achieved for relatively complex systems (for example programmable electronic safety-related systems) at the present time.

- sets requirements for the avoidance and control of systematic faults, which are based on experience and judgement gained from practical experience gained in industry. Even though the probability of occurrence of systematic failures cannot in general be quantified the standard does, however, allow a claim to be made, for a specified safety function, that the target failure measure associated with the safety function can be considered to be achieved if all the requirements in the standard have been met. .
- adopts a broad range of principles, techniques and measures to achieve functional safety for E/E/PE safety-related systems, but does not use the concept of fail safe which may be of value when the failure modes are well defined and the level of complexity is relatively low. The concept of fail safe was considered inappropriate because of the full range of complexity of E/E/PE safety-related systems that are within the scope of the standard.

FUNCTIONAL SAFETY OF ELECTRICAL/ELECTRONIC/PROGRAMMABLE ELECTRONIC SAFETY-RELATED SYSTEMS –

Part 5: Examples of methods for the determination of safety integrity levels

1 Scope

1.1 This part of IEC 61508 provides information on

- the underlying concepts of risk and the relationship of risk to safety integrity (see annex A);
- a number of methods that will enable the safety integrity levels for the E/E/PE safety-related systems to be determined (see annexes B, C, D and E).

The method selected will depend upon the application sector and the specific circumstances under consideration. Annexes B, C, D and E illustrate quantitative and qualitative approaches and have been simplified in order to illustrate the underlying principles. These annexes have been included to illustrate the general principles of a number of methods but do not provide a definitive account. Those intending to apply the methods indicated in these annexes should consult the source material referenced.

NOTE For more information on the approaches illustrated in annexes B, and E, see references [2] and [5] in the bibliography. See also reference [3] in the bibliography for a description of an additional approach.

1.2 Parts 1, 2, 3 and 4 of this standard are basic safety publications, although this status does not apply in the context of low complexity E/E/PE safety-related systems (see 3.4.4 of part 4). As basic safety publications, they are intended for use by technical committees in the preparation of standards in accordance with the principles contained in *IEC Guide 104* and *ISO/IEC Guide 51*. Parts 1, 2, 3, and 4 are also intended for use as stand-alone publications. The horizontal safety function of this international standard does not apply to medical equipment in compliance with the IEC 60601 series.

1.3 One of the responsibilities of a technical committee is, wherever applicable, to make use of basic safety publications in the preparation of its publications. In this context, the requirements, test methods or test conditions of this basic safety publication will not apply unless specifically referred to or included in the publications prepared by those technical committees.

1.4 Figure 1 shows the overall framework for parts 1 to 7 of IEC 61508 and indicates the role that IEC 61508-4 plays in the achievement of functional safety for E/E/PE safety-related systems.

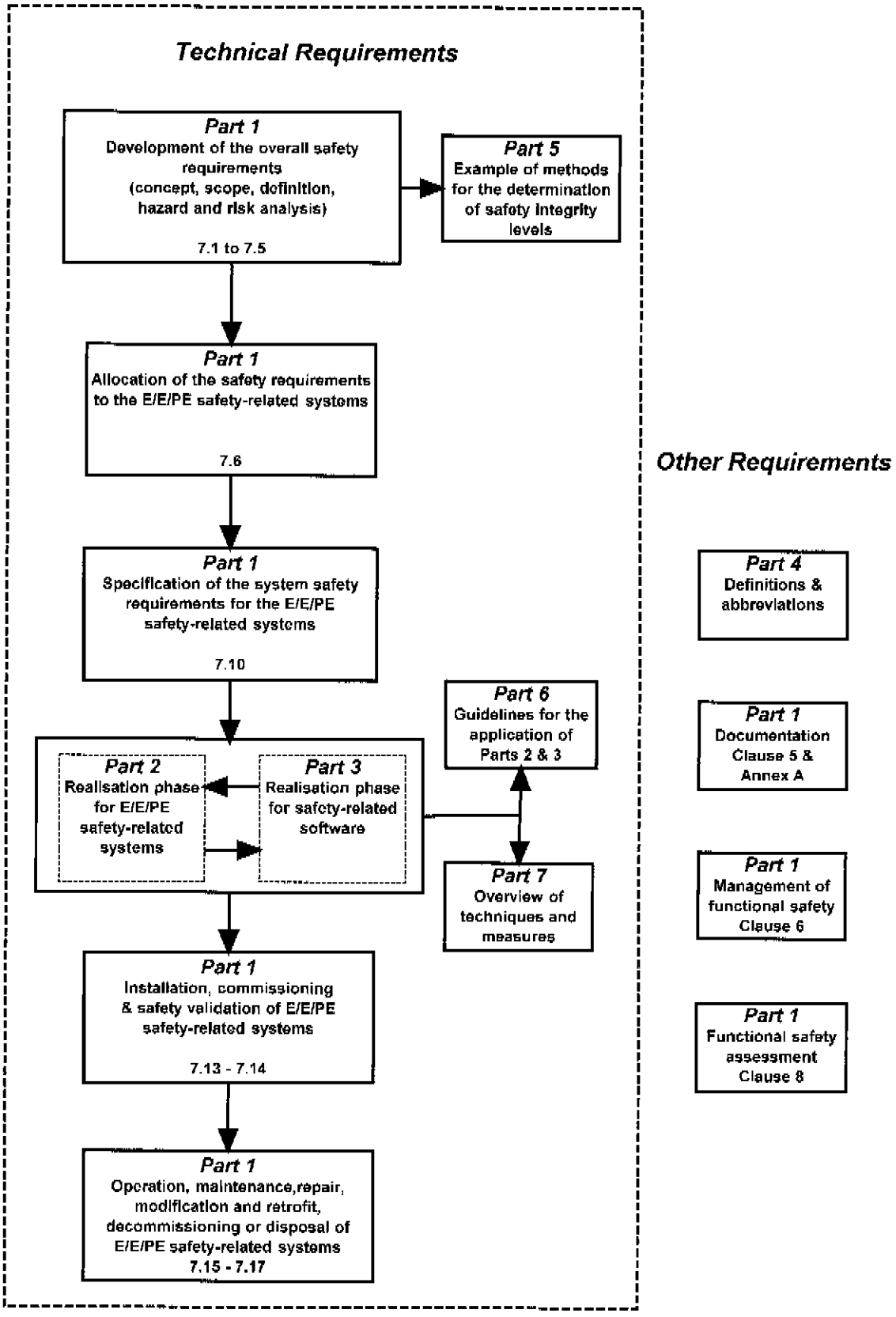


Figure 1 – Overall framework of this standard

2 Normative references

The following normative documents contain provisions which, through reference in this text, constitute provisions of this International Standard. At the time of publication, the editions indicated were valid. All normative documents are subject to revision, and parties to agreements based on this International Standard are encouraged to investigate the possibility of applying the most recent editions of the normative documents indicated below. Members of IEC and ISO maintain registers of currently valid International Standards.

IEC 61508-1:1998, *Functional safety of electrical/electronical/programmable electronic safety-related systems – Part 1: General requirements*

IEC 61508-2,— *Functional safety of electrical/electronical/programmable electronic safety-related systems – Part 2: Requirements for electrical/electronical/programmable electronic safety-related systems* [1)]

IEC 61508-3:1998, *Functional safety of electrical/electronical/programmable electronic safety-related systems – Part 3: Software requirements*

IEC 61508-4:1998, *Functional safety of electrical/electronical/programmable electronic safety-related systems – Part 4: Definitions and abbreviations of terms*

IEC 61508-6,— *Functional safety of electrical/electronical/programmable electronic safety-related systems – Part 6: Guidelines on the application of IEC61508-2 and IEC 61508-3*

IEC 61508-7, — *Functional safety of electrical/electronical/programmable electronic safety-related systems – Part 7: Overview of techniques and measures*

ISO/IEC Guide 51:1990, *Guidelines for the inclusion of safety aspects in standards*

IEC Guide 104:1997, *Guide to the drafting of safety standards, and the role of Committees with safety pilot functions and safety group functions*

3 Definitions and abbreviations

For the purposes of this standard, the definitions and abbreviations given in part 4 apply.

Annex A
(informative)

Risk and safety integrity – General concepts

A.1 General

This annex provides information on the underlying concepts of risk and the relationship of risk to safety integrity.

A.2 Necessary risk reduction

The necessary risk reduction (see 3.5.14 of IEC 61508-4) is the reduction in risk that has to be achieved to meet the tolerable risk for a specific situation (which may be stated either qualitatively[1)] or quantitatively[2)]). The concept of necessary risk reduction is of fundamental importance in the development of the safety requirements specification for the E/E/PE safety-related systems (in particular, the safety integrity requirements part of the safety requirements specification). The purpose of determining the tolerable risk for a specific hazardous event is to state what is deemed reasonable with respect to both the frequency (or probability) of the hazardous event and its specific consequences. Safety-related systems are designed to reduce the frequency (or probability) of the hazardous event and/or the consequences of the hazardous event.

The tolerable risk will depend on many factors (for example, severity of injury, the number of people exposed to danger, the frequency at which a person or people are exposed to danger and the duration of the exposure). Important factors will be the perception and views of those exposed to the hazardous event. In arriving at what constitutes a tolerable risk for a specific application, a number of inputs are considered. These include:

- legal requirements, both general and those directly relevant to the specific application;
- guidelines from the appropriate safety regulatory authority;
- discussions and agreements with the different parties involved in the application;
- industry standards and guidelines;
- international discussions and agreements; the role of national and international standards is becoming increasingly important in arriving at tolerable risk criteria for specific applications;
- the best independent industrial, expert and scientific advice from advisory bodies;

In determining the required safety integrity requirements of the E/E/PE safety-related system(s) and other risk reduction measures, in order to meet the tolerable frequency of a hazardous event, account needs to be taken of the characteristics of the risk that are relevant to the application. The tolerable frequency will depend on the legal requirements in the country of application and on the criteria specified by the user organisation. Issues that may need to be considered together with how they can be applied to E/E/PE safety-related systems are discussed below.

---

1) In achieving the tolerable risk, the necessary risk reduction will need to be established. Annexes E and G of IEC 61508-5 outline qualitative methods, although in the examples quoted the necessary risk reduction is incorporated implicitly by specification of the SIL requirement rather than stated explicitly by a numeric value of risk reduction required.

2) For example, that the hazardous event, leading to a specific consequence, shall not occur with a frequency greater than one in 10^8 h.

A.2.1 Individual risk

Different targets are usually defined for employees and members of the public. The target for individual risk for employees is applied to the most exposed individual and may be expressed as the total risk per year arising from all work activities. The target is applied to a hypothetical person and therefore needs to take into account the percentage of time that the individual spends at work. The target applies to all risks to the exposed person and the target risk for an individual safety function will need to take account of other risks.

Assurance that the total risk is reduced below a specified target can be done in a number of ways. One method is to consider and sum all risks to the most exposed individual. This may be difficult in cases where a person is exposed to many risks and early decisions are needed for system development. An alternative approach is to allocate a percentage of the overall individual risk target to each safety function under consideration. The percentage allocated can usually be decided from previous experience of the type of facility under consideration.

The target applied to an individual safety function should also take into account the conservatism of the method of risk analysis used. All qualitative methods such as risk graphs involve some evaluation of the critical parameters that contribute to risk. The factors that give rise to risk are the consequence of the hazardous event and its frequency. In determining these factors a number of risk parameters may need to be taken into account such as a vulnerability to the hazardous event, number of people who may be affected by the hazardous event (i.e. occupancy) and probability of avoiding the hazardous event.

Qualitative methods generally involve deciding if a parameter lies within a certain range. The descriptions of the criteria when using such methods will need to be such that there can be a high level of confidence that the target for risks is not exceeded. This can involve setting range boundaries for all parameters so applications with all parameters at the boundary condition will meet the specified risk criteria for safety. This approach to setting the range boundaries is very conservative because there will be very few applications where all parameters will be at the worst case of the range. The frequency target for such methods can therefore be higher than the target for quantitative methods provided there is a high level of confidence that the overall risk from all hazards is tolerable.

If members of the public are to be exposed to risk from failure of a E/E/PE safety-related system then a lower target will normally apply.

A.2.2 Societal Risk

This arises where multiple fatalities are likely to arise from single events. Such events are called societal because they are likely to provoke a socio-political response. There can be significant public and organisational aversion to high consequence events and this will need to be taken into consideration in some cases. The criterion for societal risk is often expressed as a maximum accumulated frequency for fatal injuries to a specified number of persons. The criterion is normally specified in the form of an F/N curve where F is the cumulative frequency of hazards and N the number of fatalities arising from the hazards. The relationship is normally a straight line when plotted on logarithmic scales. The slope of the line will depend on the extent to which the organisation is risk averse to higher levels of consequence. The requirement will be to ensure the accumulated frequency for a specified number of fatalities is lower than the accumulated frequency expressed in the F/N curve. (see Reference [4])

A.2.3 Continuous Improvement

The principles of reducing risk to as low as reasonably practicable are discussed in Annex C.

A.2.4 Risk Profile

In deciding risk criteria to be applied for a specific hazard the risk profile over the life of the asset may need to be considered. Residual risk will vary from low just after a proof test or a repair has been performed to a maximum just prior to proof testing. This may need to be taken into consideration by organisations that specify the risk criteria to be applied. If proof test intervals are significant then it may be appropriate to specify the maximum hazard probability that can be accepted just prior to proof testing or that the PFD(t) or PFH(t) is lower than the upper SIL boundary more than a specified percentage of the time (e.g. 90%).

A.3 Role of E/E/PE safety-related systems

E/E/PE safety-related systems contribute towards providing the necessary risk reduction in order to meet the tolerable risk.

A safety-related system both

- implements the required safety functions necessary to achieve a safe state for the equipment under control or to maintain a safe state for the equipment under control, and
- is intended to achieve, on its own or with other E/E/PE safety-related systems or other risk reduction measures, the necessary safety integrity for the required safety functions (3.4.1 of IEC 61508-4).

NOTE 1 The first part of the definition specifies that the safety-related system must perform the safety functions which would be specified in the safety functions requirements specification. For example, the safety functions requirements specification may state that when the temperature reaches x, valve y shall open to allow water to enter the vessel.

NOTE 2 The second part of the definition specifies that the safety functions must be performed by the safety-related systems with the degree of confidence appropriate to the application, in order that the tolerable risk will be achieved.

A person could be an integral part of an E/E/PE safety-related system. For example, a person could receive information, on the state of the EUC, from a display screen and perform a safety action based on this information.

E/E/PE safety-related systems can operate in a low demand mode of operation or high demand or continuous mode of operation (see 3.5.12 of IEC 61508-4).

A.4 Safety integrity

Safety integrity is defined as the probability of a safety-related system satisfactorily performing the required safety functions under all the stated conditions within a stated period of time (3.5.2 of IEC 61508-4). Safety integrity relates to the performance of the safety-related systems in carrying out the safety functions (the safety functions to be performed will be specified in the safety functions requirements specification).

Safety integrity is considered to be composed of the following two elements.

- Hardware safety integrity; that part of safety integrity relating to random hardware failures in a dangerous mode of failure (see 3.5.5 of IEC 61508-4). The achievement of the specified level of safety-related hardware safety integrity can be estimated to a reasonable level of accuracy, and the requirements can therefore be apportioned between subsystems using the normal rules for the combination of probabilities. It may be necessary to use redundant architectures to achieve adequate hardware safety integrity.
- Systematic safety integrity; that part of safety integrity relating to systematic failures in a dangerous mode of failure (see 3.5.4 of IEC 61508-4). Although the mean failure rate due to systematic failures may be capable of estimation, the failure data obtained from design faults and common cause failures means that the distribution of failures can be hard to predict. This has the effect of increasing the uncertainty in the failure probability calculations for a specific situation (for example the probability of failure of a safety-related protection system). Therefore a judgement has to be made on the selection of the best techniques to minimise this uncertainty. Note that it is not the case that measures to reduce the probability of random hardware failure will have a corresponding effect on the probability of systematic failure. Techniques such as redundant channels of identical hardware, which are very effective at controlling random hardware failures, are of little use in reducing systematic failures such as software errors.

A.5 Modes of operation and SIL determination

The mode of operation relates to the the way in which a safety function is intended to be used with respect to the frequency of demands made upon it which may be either:

- **low demand mode:** where frequency of demands for operation made on the safety function is no greater than one per year; or
- **high demand mode:** where frequency of demands for operation made on the safety function is greater than one per year.; or
- **continuous mode:** where demand for operation of the safety function is continuous.

Tables 2 and 3 of IEC 61508-1 detail the target failure measures associated with the four safety integrity levels for each of the modes of operation. The modes of operation are explained further in the following paragraphs:

A.5.1 Safety integrity and risk reduction for low demand mode applications

The required safety integrity of the E/E/PE safety-related systems and other risk reduction measures must be of such a level so as to ensure that

- the average probability of failure on demand of the safety-related systems is sufficiently low to prevent the hazardous event frequency exceeding that required to meet the tolerable risk, and/or
- the safety-related systems modify the consequences of failure to the extent required to meet the tolerable risk.

Figure A.1 illustrates the general concepts of risk reduction. The general model assumes that

- there is a EUC and a control system;
- there are associated human factor issues;
- the safety protective features comprise
  - E/E/PE safety-related systems,
  - other risk reduction measures.

NOTE Figure A.1 is a generalised risk model to illustrate the general principles. The risk model for a specific application will need to be developed taking into account the specific manner in which the necessary risk reduction is actually being achieved by the E/E/PE safety-related systems and/or other risk reduction measures. The resulting risk model may therefore differ from that shown in figure A.1.

The various risks indicated in figure A.1 and A.2 are as follows:

- EUC risk: the risk existing for the specified hazardous events for the EUC, the EUC control system and associated human factor issues: no designated safety protective features are considered in the determination of this risk (see 3.2.4 of IEC 61508-4);
- tolerable risk; the risk which is accepted in a given context based on the current values of society (see 3.1.6 of IEC 61508-4);
- residual risk: in the context of this standard, the residual risk is that remaining for the specified hazardous events for the EUC, the EUC control system, human factor issues but with the addition of, E/E/PE safety-related systems and other risk reduction measures (see also 3.1.7 of IEC 61508-4).

The EUC risk is a function of the risk associated with the EUC itself but taking into account the risk reduction brought about by the EUC control system. To prevent unreasonable claims for the safety integrity of the EUC control system, this standard places constraints on the claims that can be made (see 7.5.2.5 of IEC 61508-1).

The necessary risk reduction is achieved by a combination of all the safety protective features. The necessary risk reduction to achieve the specified tolerable risk, from a starting point of the EUC risk, is shown in figure A.1 (relevant for a safety function operating in low demand mode of operation).

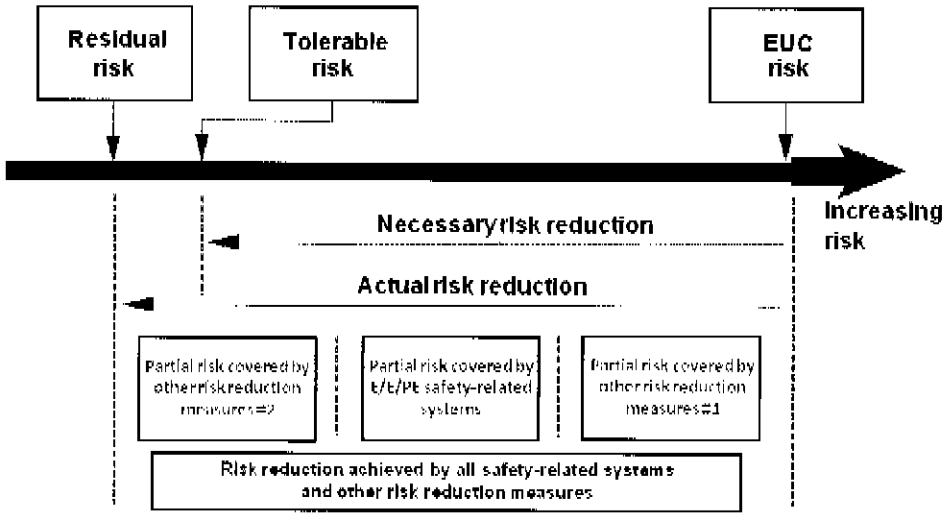


Figure A.1 – Risk reduction: general concepts (low demand mode of operation)

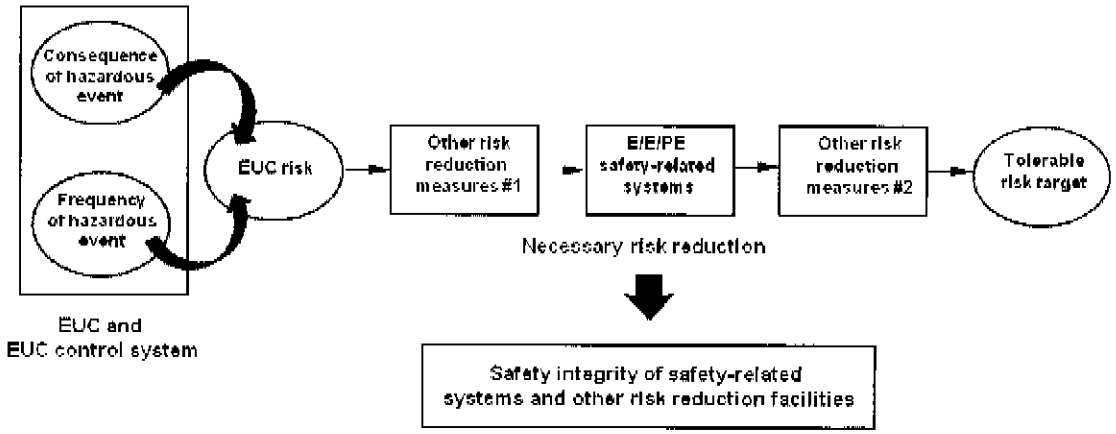


Figure A.2 – Risk and safety integrity concepts

A.5.2 Safety integrity for high demand mode applications

The required safety integrity of the E/E/PE safety-related systems and other risk reduction measures must be of such a level to ensure that

- the average probability of failure on demand of the safety-related systems is sufficiently low to prevent the hazardous event frequency exceeding that required to meet the tolerable risk, and/or
- the average probability of failure per hour of the safety-related system is sufficiently low to prevent the hazardous event frequency exceeding that required to meet the tolerable risk

Figure A.3 illustrates the general concepts of high demand applications. The general model assumes that

- there is a EUC and a control system;
- there are associated human factor issues;
- the safety protective features comprise
  - E/E/PE safety-related system operating in high demand mode

– other risk reduction measures

Various demands on the E/E/PE safety related systems can occur as follows:

- General demands from the EUC
- Demands arising from failures in the EUC control system
- Demands arising from human failures

If the total demand rate arising from all the demands on the system exceeds 1 per year then the critical factor is the dangerous failure rate of the E/E/PE safety-related system. Residual hazard frequency can never exceed the dangerous failure rate of the E/E/PE safety-related system. It can be lower if other risk reduction measures reduce the probability of harm.

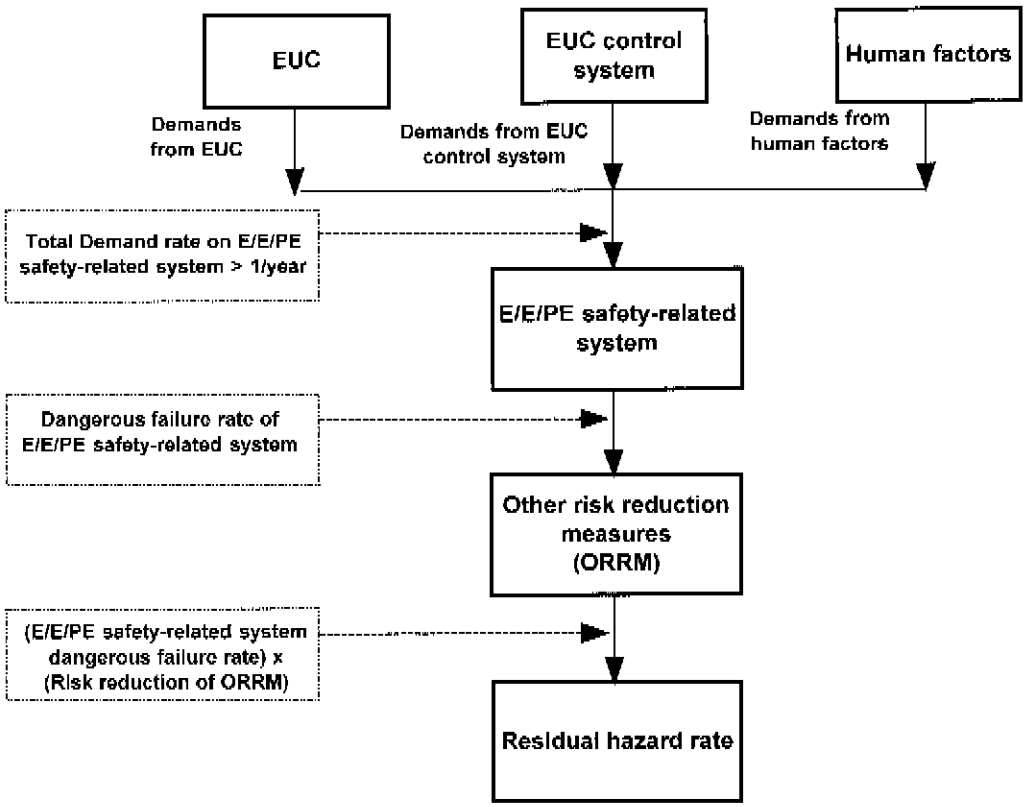


Figure A.3 – Risk diagram for high demand applications

A.5.3 Safety integrity for continuous mode applications

The required safety integrity of the E/E/PE safety-related systems and any other risk reduction measures must be of such a level to ensure that the average probability of a dangerous failure per hour of the safety-related system is sufficiently low to prevent the hazardous event frequency exceeding that required to meet the tolerable risk.

With an E/E/PE safety-related system operating in continuous mode other risk reduction measures can reduce the residual hazard frequency according to the risk reduction provided The model is shown in Figure A.4.

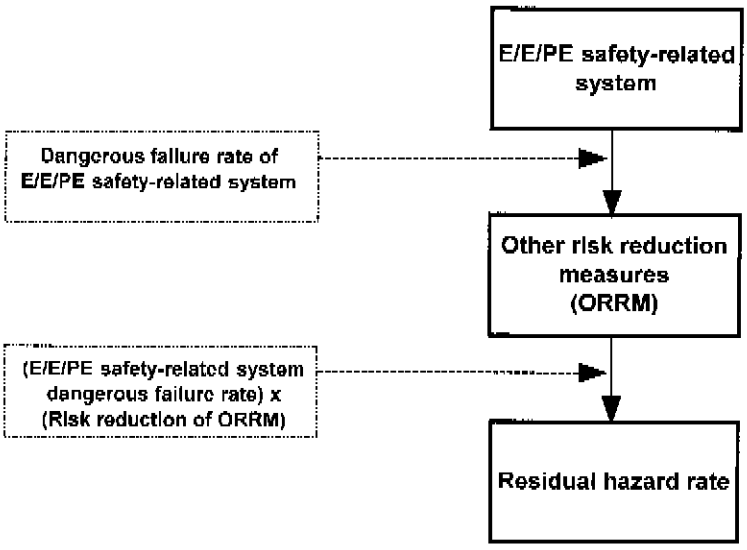


Figure A.4 – Risk diagram for continuous mode operation

A.5.4 Common cause and dependency failures

During the determination of the safety integrity levels it is important to take account of common cause and dependency failures. The models shown above in figures A.1, A.2, A.3 and A.4 are drawn on the basis that each safety system relevant to the same hazard is fully independent. There are many applications where this is not the case. Examples include the following:

1. Where a dangerous failure of an element within the EUC control system can cause a demand on a safety-related system and the safety-related system uses an element subject to failure from the same cause. An example of this could be where the control and protection system sensors are separate but common cause could lead to failure of both (see Figure A.5)
2. Where more than one safety-related system is used and some of the same type of equipment is used within each safety-related system is subject to failure from the same common cause. An example would be where the same type of sensor is used in two separate protection systems both providing risk reduction for the same hazard (see figure A.6).
3. Where more than one protection system is used, the protection systems are diverse but proof testing is carried out on all the systems on a synchronous basis. In such cases the actual PFDavg achieved by the combination of multiple systems will be significantly higher than the PFDavg suggested by the multiplication of the PFDavg of the individual systems.
4. Where the same individual element is used as part of the control system and the safety-related systemWhere more than one protection system is used and where the same individual element is used as part of more than one system

In such cases the effect of common cause/dependency will need to be considered. Consideration should be given as to whether the final arrangement is capable of meeting the necessary Systematic Capability and the necessary probability of dangerous random hardware failure rates relating to the overall risk reduction required. The effect of common cause failures is difficult to determine and often requires the construction of special purpose models (e.g. fault tree or Markov models).

The effect of common cause is likely to be more significant in applications involving high safety integrity levels. In some application it may be necessary to incorporate diversity so that common cause effects are minimised. It should however be noted that incorporation of diversity can lead to problems during design, maintenance and modification. Introducing diversity can lead to errors due to the unfamiliarity and lack of operation experience with the diverse devices.

A.5.5 Safety Integrity levels when multiple layers of protection are used

When multiple layers of protection are used to achieve a tolerable risk frequency there may be interactions between systems themselves and also between systems and causes of demand. As discussed above in A.5.4 there are always concerns about test (de)synchronisation and common cause failures since these can be significant factors when overall risk reduction requirements are high or where demand frequency is low. Evaluation of the interactions between safety layers and between safety layers and causes of demand can be complex and may need the development of a holistic model (e.g. as described in ISO/IEC 31010 ed 1: Risk management -Risk assessment techniques) and based, for example on a top down approach with the top event specified as the tolerable hazard frequency. The model may include all safety layers for calculating the actual risk reduction and all causes of demand for calculating the actual frequency of accident. This allows the identification of minimal cut sets (i.e. failure scenarios), reveals the weak points (i.e. the shortest minimal cut sets: single, double failures, etc.) in the arrangement of systems and facilitate system improvement through sensitivity analysis.

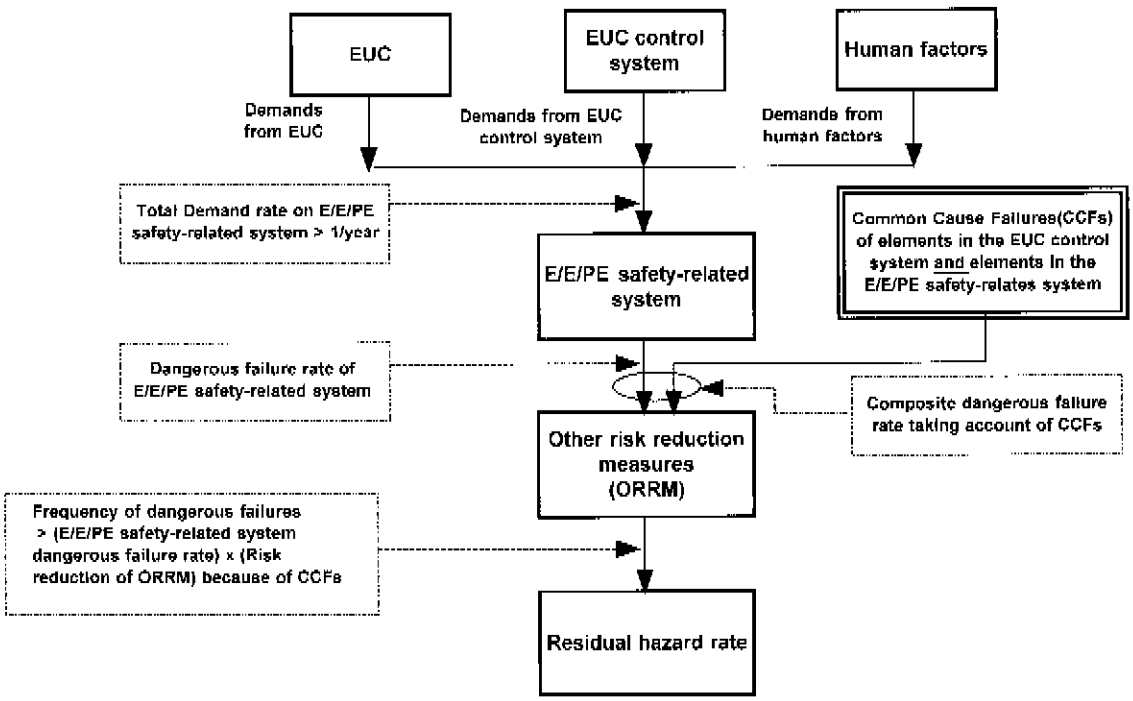


Figure A.5 – Illustration of Common Cause Failures (CCFs) of elements in the EUC control system and elements in the E/E/PE safety-related system

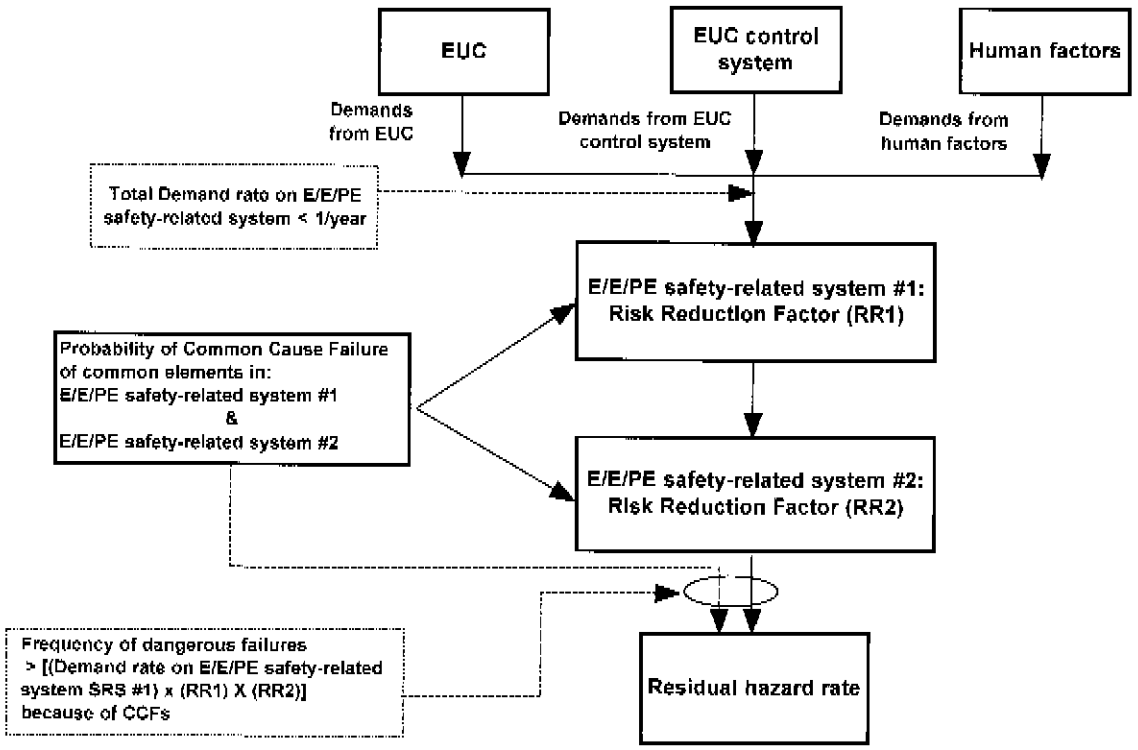


Figure A.6 – Common cause between two E/E/PE safety-related systems

A.6 Risk and safety integrity

It is important that the distinction between risk and safety integrity be fully appreciated. Risk is a measure of the probability and consequence of a specified hazardous event occurring. This can be evaluated for different situations (EUC risk, risk reduction required to meet the tolerable risk, actual risk (see figure A.1). The tolerable risk is determined by consideration of the issues described in A.2. Safety integrity applies solely to the E/E/PE safety-related systems and other risk reduction measures and is a measure of the likelihood of those systems/facilities satisfactorily achieving the necessary risk reduction in respect of the specified safety functions. Once the tolerable risk has been set, and the necessary risk reduction estimated, the safety integrity requirements for the safety-related systems can be allocated (see 7.4, 7.5 and 7.6 of IEC 61508-1).

NOTE The allocation is necessarily iterative in order to optimize the design to meet the various requirements.

A.7 Safety integrity levels and software safety integrity levels

To cater for the wide range of necessary risk reductions that the safety-related systems have to achieve, it is useful to have available a number of safety integrity levels as a means of satisfying the safety integrity requirements of the safety functions allocated to the safety-related systems. Software safety integrity levels are used as the basis of specifying the safety integrity requirements of the safety functions implemented in part by safety-related software. The safety integrity requirements specification should specify the safety integrity levels for the E/E/PE safety-related systems.

In this standard, four safety integrity levels are specified, with safety integrity level 4 being the highest level and safety integrity level 1 being the lowest.

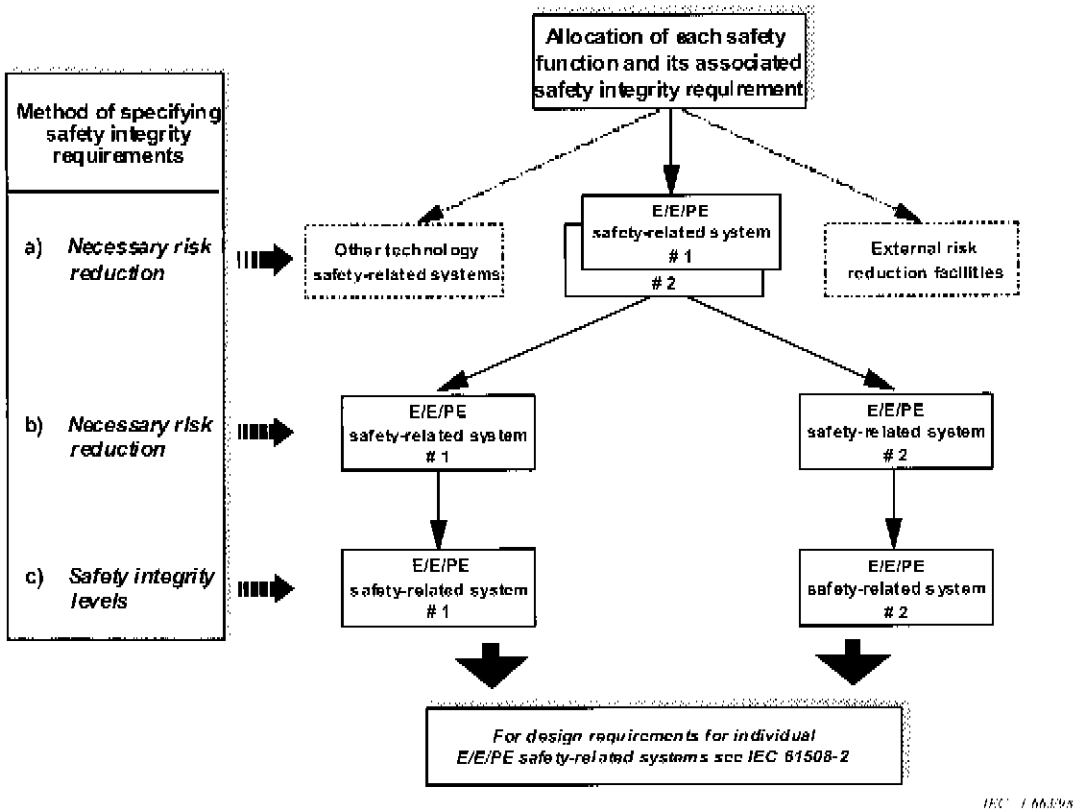
The safety integrity level target failure measures for the four safety integrity levels are specified in tables 2 and 3 of IEC 61508-1. Two parameters are specified, one for safety-related systems operating in a low demand mode of operation and one for safety-related systems operating in a high demand or continuous mode of operation.

NOTE For safety-related systems operating in a low demand mode of operation, the safety integrity measure of interest is the probability of failure to perform its design function on demand. For safety-related systems operating in a high demand or continuous mode of operation, the safety integrity measure of interest is the average probability of a dangerous failure per hour (see 3.5.12 and 3.5.13 of IEC 61508-4).

A.8 Allocation of safety requirements

The allocation of safety requirements (both the safety functions and the safety integrity requirements) to the E/E/PE safety-related systems, other technology safety-related systems and external risk reduction facilities is shown in figure A.7 (this is identical to figure 6 of IEC 61508-1). The requirements for the safety requirements allocation phase are given in 7.6 of IEC 61508-1.

The methods used to allocate the safety integrity requirements to the E/E/PE safety-related systems, other technology safety-related systems and external risk reduction facilities depend, primarily, upon whether the necessary risk reduction is specified explicitly in a numerical manner or in a qualitative manner. These approaches are termed quantitative and qualitative methods respectively (see annexes B, C, D and E).



NOTE 1 Safety integrity requirements are associated with each safety function before allocation (see 7.5.2.6 of IEC 61508-1).

NOTE 2 A safety function may be allocated across more than one safety-related system.

Figure A.7 – Allocation of safety requirements to the E/E/PE safety-related systems, other technology safety-related systems and external risk reduction facilities

A.9 Mitigation Systems

Mitigation systems take action in the event of full or partial failure of other safety-related systems such as E/E/PE safety-systems. The objective is to reduce the consequences associated with a hazardous event rather than its frequency. Examples of mitigation systems include fire and gas systems (detection of fire/gas and subsequent action to put the fire out (e.g. by water deluge), and airbag system in an automobile.

When determining the safety integrity requirements it should be recognised that when making judgements on the severity of the consequence, only the incremental consequences should be considered. That is, determine the increase in the severity of the consequence if the function did not operate over that when it does operate as intended. This can be done by first considering the consequences if the system fails to operate and then considering what difference will be made if the mitigation function operates correctly. In considering the consequences if the system fails to operate there will normally be a number of outcomes all with different probabilities.

Note Guidance on the determination of safety integrity levels for Fire and Gas and Emergency Shut Down systems is included in Annex B of ISO 10418. Petroleum and natural gas industries. – Analysis, design and testing of basic surface process safety systems on offshore production installations – Requirements and Guidelines

Annex B
(informative)

Selection of methods for determining Safety Integrity Levels

B.1 General

This annex lists a number of techniques that can be used for determination of safety integrity levels. None of the methods are suitable for all applications and users will need to select the most suitable. In selecting the most appropriate method consideration should be given to the following factors:

1. The risk acceptance criteria that need to be met. Some of the techniques will not be suitable if it is required to demonstrate that risk has been reduced to as low as reasonably practicable
2. The mode of operation of the safety function. Some methods are only suitable for low demand mode
3. The knowledge and experience of the persons undertaking the SIL determination and what has been the traditional approach in the sector
4. The confidence needed that the resulting residual risk meets the criteria specified by the user organisation. Some of the methods can be linked back to quantified targets but some approaches are qualitative only
5. More than one method may be used. One method may be used for screening purposes followed by another more rigorous approach if the screening method shows the need for high safety integrity levels
6. The severity of the consequences. More rigorous methods may be selected for consequences that include multiple fatalities
7. Whether common cause occurs between the E/E/PE safety related systems or between the E/E/PE safety related system and demand causes

Whatever method is used all assumptions should be recorded for future safety management. All decisions should be recorded so that the SIL assessment can be verified and be subject to independent functional safety assessment.

B.2 Quantitative Method of SIL determination

The quantitative method is described in Annex D. It may be used together with the ALARP method described in Annex C.

The quantitative method can be used for both simple and complex applications. With complex applications fault trees can be constructed to represent the hazard model. The top event will generally be one or more fatalities and logic constructed to represent demand causes and failures of the E/E/PE safety related systems that lead to the top event. Software tools are available to allow modeling of common cause if the same type of equipment is used for control and protection functions. In some complex applications a single failure event may occur in more than one place in the fault tree and this will require a boolean reduction to be carried out. The tools also facilitate sensitivity analysis that show the dominant factors that influence the frequency of the top event. SIL can be established by determining the required risk reduction to achieve the tolerable risk criteria.

The method is suitable for safety functions operating in continuous/high demand mode and low demand mode. The method normally results in low SILs because the risk model is specifically designed for each application and numeric values are used to represent each risk factor rather than the numeric ranges used in calibrated risk graphs. Quantitative methods however require the construction of a specific model for each hazardous event. Modeling requires skill, tools and knowledge of the application and can take considerable time to develop and verify.

The method facilitates demonstration that risk has been reduced to as low as reasonably practicable. This can be done by considering options for further risk reduction, integrating the additional facilities in the fault tree model and then determining the reduction in risk and comparing this with the cost of the option.

B.3 The Risk Graph Method

The risk graph qualitative method is described in Annex E. The method enables the safety integrity level to be determined from knowledge of the risk factors associated with the EUC and the EUC control system. A number of parameters are introduced which together describe the nature of the hazardous situation when safety related systems fail or are not available. One parameter is chosen from each of four sets, and the selected parameters are then combined to decide the safety integrity level allocated to the safety functions. The method has been used extensively within the machinery sector, see ISO 14121-2 and Annex A of ISO 13849-1.

The method can be qualitative in which case the selection of the parameters is subjective and requires considerable judgement. The residual risk cannot be calculated from a knowledge of the parameter values. It will not be suitable if an organisation requires confidence that residual risk is reduced to a specified quantitative value.

The parameters descriptions can include numeric values that are derived by calibrating the risk graph against numeric tolerability risk criteria. The residual risk can be calculated from numeric values used for each of the parameters. It will be suitable if an organisation requires confidence that residual risk is reduced to a specified quantitative value. Experience has shown that use of the calibrated risk graph method can result in high safety integrity levels. This is because calibration is usually carried out using worst case values of each parameter. Each parameter has a decade range so that for applications where all the parameters are average for the range the SIL will be one higher than necessary for tolerable risk. The method is extensively used in the process and offshore sector.

The risk graph method does not take into account common cause failures between causes of demand and cause of the E/E/PE safety related system failure or common cause issues with other layers of protection.

B.4 Layer of Protection Analysis (LOPA)

The basic method is described in a number of books and the technique can be used in a number of different forms. A technique that can be used for SIL determination is described in Annex F.

The method is quantitative and the user will need to decide the tolerable frequencies for each consequence severity level. Numeric credit is given for protection layers that reduce the frequency of individual demand causes. Not all protection layers are relevant to all demand causes so the technique can be used for more complex applications. The numeric values assigned to protection layers can be rounded up to the next significant figure or the next significant decade range. If numeric values of protection layers are rounded to the next significant figure then the method on average gives lower requirements for risk reduction and lower SIL values than calibrated risk graphs.

Since numeric targets are assigned to specified consequence severity levels the user can have confidence that residual risk meets corporate criteria.

The method as described is not suitable for functions that operate in continuous mode and does not take account of common cause failure between causes of demand and the E/E/PE safety related systems. The method can however be adjusted so as to be suitable for such cases.

Annex C
(informative)

ALARP and tolerable risk concepts

C.1 General

This annex considers one particular approach to the achievement of a tolerable risk. The intention is not to provide a definitive account of the method but rather an illustration of the general principles. The approach includes a process of continuous improvement where all options that would reduce risk further are considered in terms of benefits and costs. Those intending to apply the methods indicated in this annex should consult the source material referenced. [6]

C.2 ALARP model

C.2.1 Introduction

Subclause C.2 outlines the main tests that are applied in regulating industrial risks and indicates that the activities involve determining whether

a) the risk is so great that it must be refused altogether, or

b) the risk is, or has been made, so small as to be insignificant, or

c) the risk falls between the two states specified in a) and b) above and has been reduced to the lowest practicable level, bearing in mind the benefits resulting from its acceptance and taking into account the costs of any further reduction.

With respect to c), the ALARP principle requires that any risk must be reduced so far as is reasonably practicable, or to a level which is as low as reasonably practicable (these last 5 words form the abbreviation ALARP). If a risk falls between the two extremes (i.e. the unacceptable region and broadly acceptable region) and the ALARP principle has been applied, then the resulting risk is the tolerable risk for that specific application. This three zone approach is shown in figure C.1.

Above a certain level, a risk is regarded as intolerable and cannot be justified in any ordinary circumstance.

Below that level, there is the tolerability region where an activity is allowed to take place provided the associated risks have been made as low as reasonably practicable. Tolerable here is different from acceptable; it indicates a willingness to live with a risk so as to secure certain benefits, at the same time expecting it to be kept under review and reduced as and when this can be done. Here a cost benefit assessment is required either explicitly or implicitly to weigh the cost and the need or otherwise for additional safety measures. The higher the risk, the more proportionately would be expected to be spent to reduce it. At the limit of tolerability, expenditure in gross disproportion to the benefit would be justified. Here the risk will by definition be substantial, and equity requires that a considerable effort is justified even to achieve a marginal reduction.

Where the risks are less significant, the less, proportionately need be spent to reduce them and at the lower end of the tolerability region, a balance between costs and benefits will suffice.

Below the tolerability region, the levels of risk are regarded as so insignificant that the regulator need not ask for further improvements. This is the broadly acceptable region where the risks are small in comparison with the everyday risks we all experience. While in the broadly acceptable region, there is no need for a detailed working to demonstrate ALARP, it is, however, necessary to remain vigilant to ensure that the risk remains at this level.

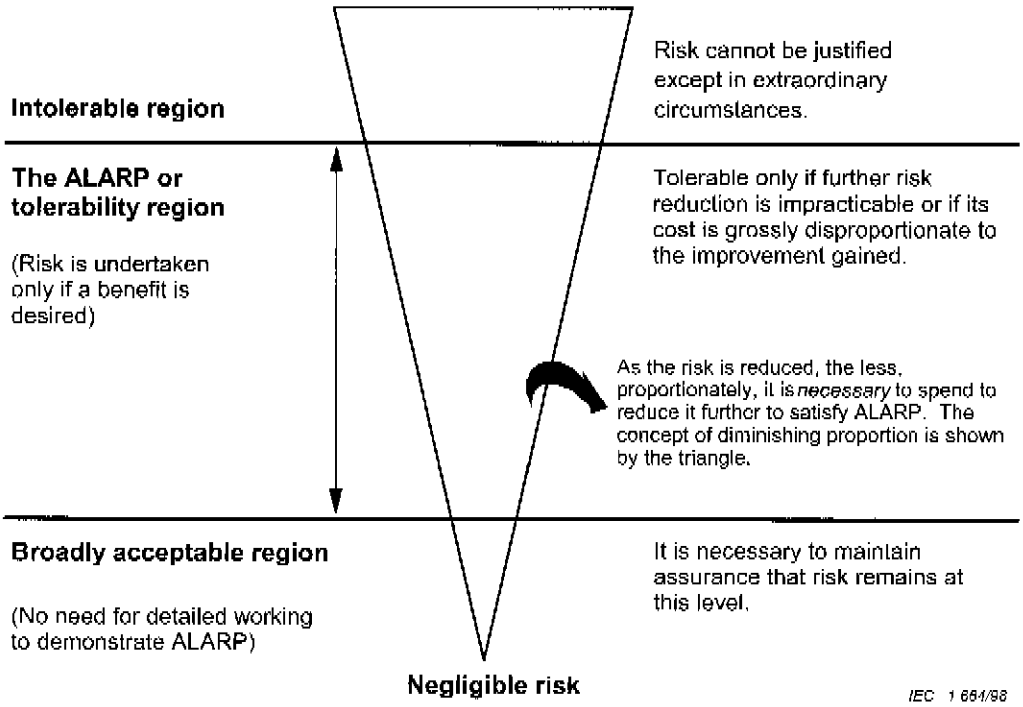


Figure C.1 – Tolerable risk and ALARP

The concept of ALARP can be used when qualitative or quantitative risk targets are adopted. Subclause C.2.2 outlines a method for quantitative risk targets. (Annex D and F outline quantitative methods and annexes E and G outline qualitative methods for the determination of the necessary risk reduction for a specific hazard. The methods indicated could incorporate the concept of ALARP in the decision making.)

NOTE Further information on ALARP is given in reference [6] in the bibliography.

C.2.2 Tolerable risk target

One way in which a tolerable risk target can be obtained is for a number of consequences to be determined and tolerable frequencies allocated to them. This matching of the consequences to the tolerable frequencies would take place by discussion and agreement between the interested parties (for example safety regulatory authorities, those producing the risks and those exposed to the risks).

To take into account ALARP concepts, the matching of a consequence with a tolerable frequency can be done through risk classes. Table C.1 is an example showing four risk classes (I, II, III, IV) for a number of consequences and frequencies. Table C.2 interprets each of the risk classes using the concept of ALARP. That is, the descriptions for each of the four risk classes are based on figure C.1. The risks within these risk class definitions are the risks that are present when risk reduction measures have been put in place. With respect to figure C.1, the risk classes are as follows:

- risk class I is in the unacceptable region;
- risk classes II and III are in the ALARP region, risk class II being just inside the ALARP region;
- risk class IV is in the broadly acceptable region.

For each specific situation, or sector comparable industries, a table similar to table C.1 would be developed taking into account a wide range of social, political and economic factors. Each consequence would be matched against a frequency and the table populated by the risk classes. For example, frequent in table C.1 could denote an event that is likely to be continually experienced, which could be specified as a frequency greater than 10 per year. A critical consequence could be a single death and/or multiple severe injuries or severe occupational illness.

Table C.1 – Example of risk classification of accidents

Frequency	Consequence			
	Catastrophic	Critical	Marginal	Negligible
Frequent	I	I	I	II
Probable	I	I	II	III
Occasional	I	II	III	III
Remote	II	III	III	IV
Improbable	III	III	IV	IV
Incredible	IV	IV	IV	IV

NOTE 1 The actual population with risk classes I, II, III and IV will be sector dependent and will also depend upon what the actual frequencies are for frequent, probable, etc. Therefore, this table should be seen as an example of how such a table could be populated, rather than as a specification for future use.

NOTE 2 Determination of the safety integrity level from the frequencies in this table is outlined in annex D.

Table C.2 – Interpretation of risk classes

Risk class	Interpretation
Class I	Intolerable risk
Class II	Undesirable risk, and tolerable only if risk reduction is impracticable or if the costs are grossly disproportionate to the improvement gained
Class III	Tolerable risk if the cost of risk reduction would exceed the improvement gained
Class IV	Negligible risk

Annex D
(informative)

Determination of safety integrity levels: a quantitative method

D.1 General

This annex outlines how the safety integrity levels can be determined if a quantitative approach is adopted and illustrates how the information contained in tables such as table C.1 can be used. A quantitative approach is of particular value when:

- the tolerable risk is to be specified in a numerical manner (for example that a specified consequence should not occur with a greater frequency than one in 10^4 years);
- numerical targets have been specified for the safety integrity levels for the safety-related systems. Such targets have been specified in this standard (see tables 2 and 3 of IEC 61508-1).

This annex is not intended to be a definitive account of the method but is intended to illustrate the general principles. It is particularly applicable when the risk model is as indicated in figures A.1 and A.2.

D.2 General method

The model used to illustrate the general principles is that shown in figure A.1. The key steps in the method are as follows and will need to be done for each safety function to be implemented by the E/E/PE safety-related system:

- determine the tolerable risk from a table such as table C.1;
- determine the EUC risk;
- determine the necessary risk reduction to meet the tolerable risk;
- allocate the necessary risk reduction to the E/E/PE safety-related systems, other technology safety-related systems and external risk reduction facilities (see 7.6 of IEC 61508-1).

Table C.1 is populated with risk frequencies and allows a numerical tolerable risk target (F_t) to be specified.

The frequency associated with the risk that exists for the EUC, including the EUC control system and human factor issues (the EUC risk), without any protective features, can be estimated using quantitative risk assessment methods. This frequency with which a hazardous event could occur without protective features present (F_{np}) is one of two components of the EUC risk; the other component is the consequence of the hazardous event. F_{np} may be determined by

- analysis of failure rates from comparable situations;
- data from relevant databases;
- calculation using appropriate predictive methods.

This standard places constraints on the minimum failure rates that can be claimed for the EUC control system (see 7.5.2.5 of IEC 61508-1). If it is to be claimed that the EUC control system has a failure rate less than these minimum failure rates, then the EUC control system shall be considered a safety-related system and shall be subject to all the requirements for safety-related systems in this standard.

D.3 Example calculation

Figure D.1 provides an example of how to calculate the target safety integrity for a single safety-related protection system. For such a situation

$$PFD_{avg} \leq F_t / F_{np}$$

where

PFD_{avg} is the average probability of failure on demand of the safety-related protection system, which is the safety integrity failure measure for safety-related protection systems operating in a low demand mode of operation (see table 2 of IEC 61508-1 and 3.5.12 of IEC 61508-4);

F_t is the tolerable hazard frequency;

F_{np} is the demand rate on the safety-related protection system.

Also in figure D.1:

- C is the consequence of the hazardous event;
- F_p is the risk frequency with the protective features in place.

It can be seen that determination of F_{np} for the EUC is important because of its relationship to PFD_{avg} and hence to the safety integrity level of the safety-related protection system.

The necessary steps in obtaining the safety integrity level (when the consequence C remains constant) are given below (as in figure D.1), for the situation where the entire necessary risk reduction is achieved by a single safety-related protection system which must reduce the hazard rate, as a minimum, from F_{np} to F_t:

- determine the frequency element of the EUC risk without the addition of any protective features (F_{np});
- determine the consequence C without the addition of any protective features;
- determine, by use of table C.1, whether for frequency F_{np} and consequence C a tolerable risk level is achieved. If, through the use of table C.1, this leads to risk class I, then further risk reduction is required. Risk class IV or III would be tolerable risks. Risk class II would require further investigation;

NOTE Table C.1 is used to check whether or not further risk reduction measures are necessary, since it may be possible to achieve a tolerable risk without the addition of any protective features.

- determine the probability of failure on demand for the safety-related protection system (PFD_{avg}) to meet the necessary risk reduction (ΔR). For a constant consequence in the specific situation described, $PFD_{avg} = (F_t / F_{np}) = \Delta R$;
- for $PFD_{avg_{avg}} = (F_t / F_{np})$, the safety integrity level can be obtained from table 2 of IEC 61508-1 (for example, for $PFD_{avg} = 10^{-2} - 10^{-3}$, the safety integrity level = 2).

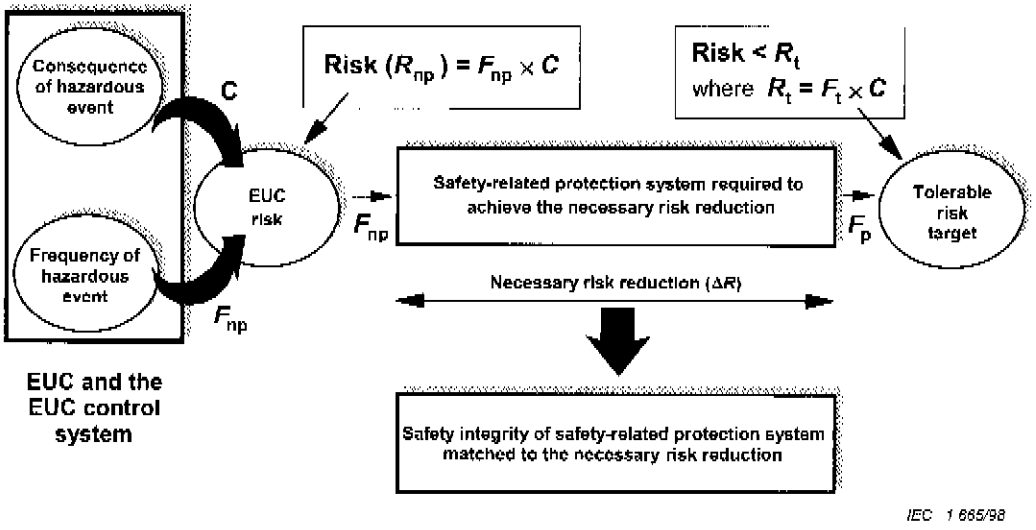


Figure D.1 – Safety integrity allocation: example for safety-related protection system

Annex E
(informative)

Determination of safety integrity levels
Risk Graph Methods

E.1 General

This annex describes the risk graph method, which is a method that enables the safety integrity level of a safety-related system to be determined from a knowledge of the risk factors associated with the EUC and the EUC control system. It is particularly applicable when the risk model is as indicated in figures A.1 and A.2. The method can be used on a qualitative or quantitative basis.

Where this approach is adopted, in order to simplify matters a number of parameters are introduced which together describe the nature of the hazardous situation when safety-related systems fail or are not available. One parameter is chosen from each of four sets, and the selected parameters are then combined to decide the safety integrity level allocated to the safety functions. These parameters

- allow a meaningful graduation of the risks to be made, and
- contain the key risk assessment factors.

This annex is not intended to be a definitive account of the method but is intended to illustrate the general principles.

E.2 Risk graph synthesis

The following simplified procedure is based on the following equation:

$$R = (f) \text{ of a specified } (C)$$

where

R is the risk with no safety-related systems in place;

f is the frequency of the hazardous event with no safety-related systems in place;

C is the consequence of the hazardous event (the consequences could be related to harm associated with health and safety or harm from environmental damage).

The frequency of the hazardous event f is, in this case, considered to be made up of three influencing factors:

- frequency of, and exposure time in, the hazardous zone;
- the possibility of avoiding the hazardous event;
- the probability of the hazardous event taking place without the addition of any safety-related systems (but having in place external risk reduction facilities) – this is termed the probability of the unwanted occurrence.

This produces the following four risk parameters:

- consequence of the hazardous event (C);
- frequency of, and exposure time in, the hazardous zone (F);
- possibility of failing to avoid the hazardous event (P);
- probability of the unwanted occurrence (W).

The risk parameters may be decided on a qualitative basis as described in table E.1 or on a quantative basis as described in table E.2. In deciding the numeric values associated with each parameter in table E.2 a calibration process will be required.

E.3 Calibration

The objectives of the calibration process are as follows:

To describe all parameters in such a way as to enable the SIL assessment team to make objective judgements based on the characteristics of the application;

To ensure the SIL selected for an application is in accordance with corporate risk criteria and takes account of risks from other sources;

To enable the parameter selection process to be verified.

Calibration of the risk graph is the process of assigning numerical values to risk graph parameters. This forms the basis for the assessment of the process risk that exists and allows determination of the required integrity of the safety instrumented function under consideration. Each of the parameters is assigned a range of values such that when applied in combination a graded assessment of the risk which exists in the absence of the particular safety function is produced. Thus a measure of the degree of reliance to be placed on the SIF is determined. The risk graph relates particular combinations of the risk parameters to safety integrity levels. The relationship between the combinations of risk parameters and safety integrity levels is established by considering the tolerable risk associated with specific hazards.

When considering the calibration of risk graphs, it is important to consider requirements relating to risk arising from both the owners' expectations and Regulatory Authority requirements. Risks to life can be considered in a number of ways as described in A.2 and Annex C.

If it is necessary to reduce the frequency of an individual fatality to a specified maximum then it cannot be assumed that all this risk reduction can be assigned to a single SIS. The exposed persons are subject to a wide range of risks arising from other sources (e.g., falls and fire and explosion risks). During calibration the number of hazards that individuals are exposed to and the total time at risk will need to be considered.

When considering the extent of risk reduction required, an organization may have criteria relating to the incremental cost of averting a fatality. This can be calculated by dividing the annualised cost of the additional hardware and engineering associated with a higher level of integrity by the incremental risk reduction. An additional level of integrity is justified if the incremental cost of averting a fatality is less than a predetermined amount.

The above issues need to be considered before each of the parameter values can be specified. Most of the parameters are assigned a range (e.g., If the expected demand rate of a particular process falls between a specified decade range of demands per year then W3 may be used). Similarly, for demands in the lower decade range, W2 would apply and for demands in the next lower decade range, W1 applies. Giving each parameter a specified range assists the team in making decisions on which parameter value to select for a specific application. To calibrate the risk graph, values or value ranges are assigned to each parameter. The risk associated with each of the parameter combinations is then assessed against the defined risk criteria. Parameter descriptions are then modified so that for all combinations of all parameter values the defined risk criteria is achieved. In the example calibration as shown in table E.2 a "D" factor is introduced to enable the range of demands associated with each W factor to be modified so that tolerable risk is achieved. In some cases the ranges associated with other risk factors may need to be modified to reflect the parameter values encountered in the spread of applications being considered. Calibration is an iterative process and continues until the specified risk acceptability criteria is satisfied for all combinations of parameter values.

The calibration activity does not need to be carried out each time the SIL for a specific application is to be determined. It is normally only necessary for organisations to undertake the work once, for similar hazards. Adjustment may be necessary for specific projects if the

original assumptions made during the calibration are found to be invalid for any specific project.

When parameter assignments are made, information should be available as to how the values were derived.

It is important that this process of calibration is agreed at a senior level within the organization taking responsibility for safety. The decisions taken determine the overall safety achieved.

In general, it will be difficult for a risk graph to consider the possibility of dependent failure between the sources of demand and the SIS. It can therefore lead to an over-estimation of the effectiveness of the SIS. If risk graphs are calibrated to include demand rates higher than once per year then the SIL requirements that results from use of the risk graph may be higher than necessary and the use of other techniques is recommended.

E.4 Other possible risk parameters

The risk parameters specified above are considered to be sufficiently generic to deal with a wide range of applications. There may, however, be applications which have aspects which require the introduction of additional risk parameters e.g. the use of new technologies in the EUC and the EUC control system. The purpose of the additional parameters would be to estimate more accurately the necessary risk reduction (see figure A.1).

E.5 Risk graph implementation: general scheme

The combination of the risk parameters described above enables a risk graph such as that shown in figure E.1 to be developed. With respect to figure E.1: $C_A < C_B < C_C < C_D$; $F_A < F_B$; $P_A < P_B$; $W_1 < W_2 < W_3$. An explanation of this risk graph is as follows.

- Use of risk parameters C, F and P leads to a number of outputs X_1, X_2, X_3... X_n (the exact number being dependent upon the specific application area to be covered by the risk graph). Figure E.1 indicates the situation when no additional weighting is applied for the more serious consequences. Each one of these outputs is mapped onto one of three scales (W_1, W_2 and W_3). Each point on these scales is an indication of the necessary safety integrity that has to be met by the E/E/PE safety-related system under consideration. In practice, there will be situations when for specific consequences, a single E/E/PE safety-related system is not sufficient to give the necessary risk reduction:
- The mapping onto W1, W2 or W3 allows the contribution of other risk reduction measures to be made. The offset feature of the scales for W1, W2 and W3 is to allow for three different levels of risk reduction from other measures. That is, scale W3 provides the minimum risk reduction contributed by other measures (i.e. the highest probability of the unwanted occurrence taking place), scale W2 a medium contribution and scale W1 the maximum contribution. For a specific intermediate output of the risk graph (i.e. X1, X2... or X6) and for a specific W scale (i.e. W1, W2 or W3) the final output of the risk graph gives the safety integrity level of the E/E/PE safety-related system (i.e. 1, 2, 3 or 4) and is a measure of the required risk reduction for this system. This risk reduction, together with the risk reductions achieved by other measures (for example by other technology safety-related systems and external risk reduction facilities) which are taken into account by the W scale mechanism, gives the necessary risk reduction for the specific situation.

The parameters indicated in figure E.1 (C_A, C_B, C_C, C_D, F_A, F_B, P_A, P_B, W_1, W_2, W_3), and their weightings, would need to be accurately defined for each specific situation or sector comparable industries, and would also need to be defined in application sector international standards.

E.6 Risk graph example

An example of a risk graph implementation based on the example data in table E.1, is shown in figure E.2. Use of the risk parameters C, F, and P lead to one of eight outputs. Each one of these outputs is mapped onto one of three scales (W1, W2 and W3). Each point on these scales (a, b, c, d, e, f, g and h) is an indication of the necessary risk reduction that has to be met by the safety-related system.

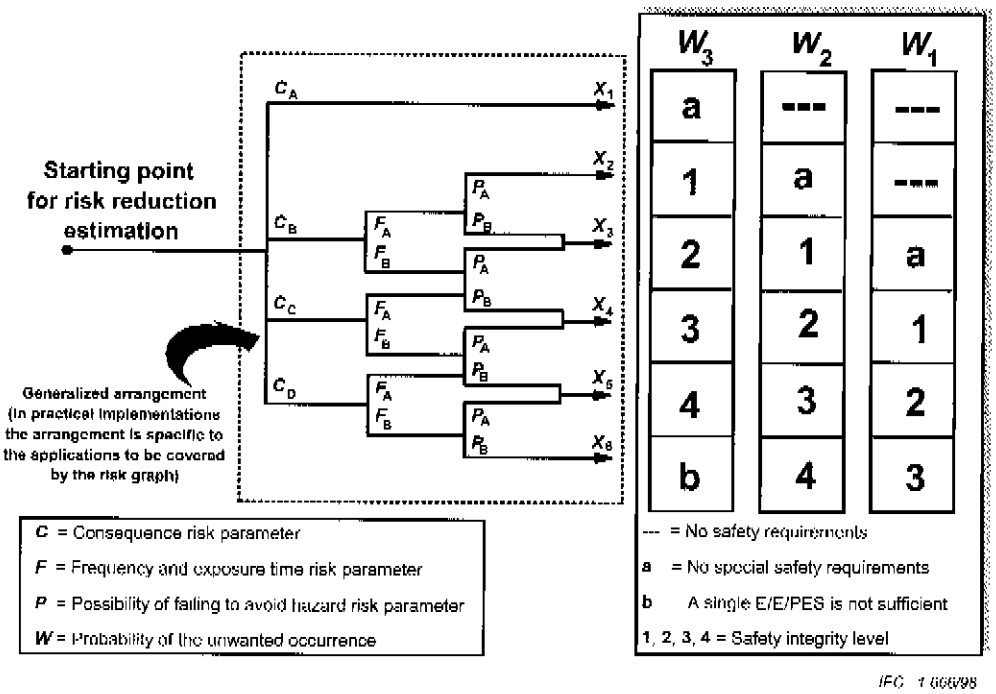
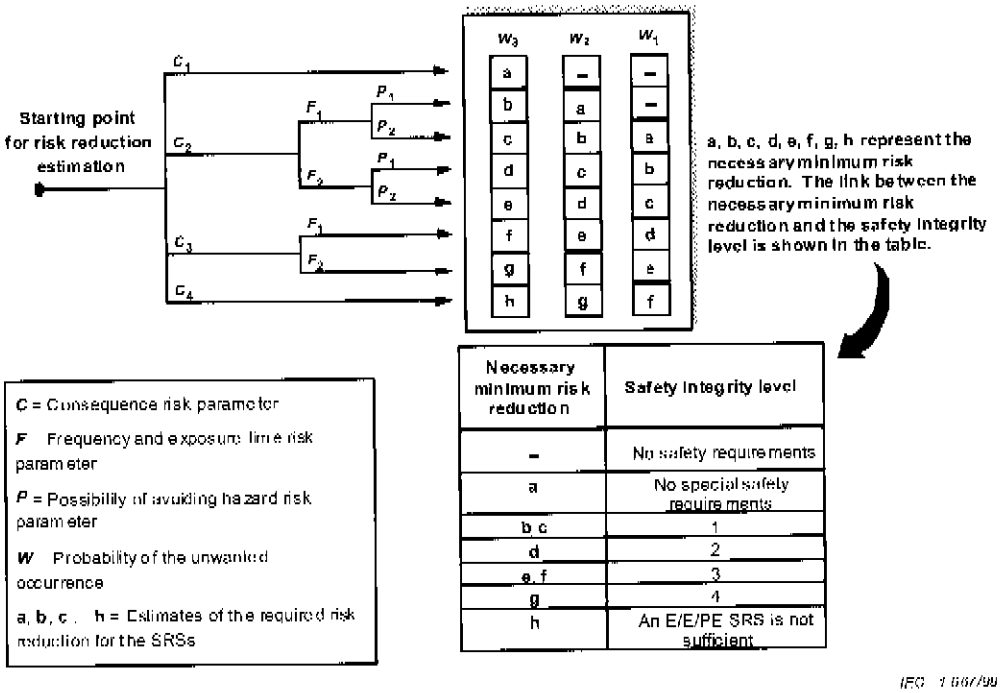


Figure E.1 – Risk graph: general scheme



Necessary minimum risk reduction	Safety integrity level
–	No safety requirements
a	No special safety requirements
b, c	1
d	2
e, f	3
g	4
h	An E/E/PE SRS is not sufficient

Figure E.2 – Risk graph: example (Illustrates general principles only)

Table E.1 – Example data relating to example risk graph (figure E.2)

Risk parameter		Classification	Comments
Consequence (C)	C_1 C_2 C_3 C_4	Minor injury Serious permanent injury to one or more persons; death to one person Death to several people Very many people killed	1 The classification system has been developed to deal with injury and death to people. Other classification schemes would need to be developed for environmental or material damage. 2 For the interpretation of C_1, C_2, C_3 and C_4, the consequences of the accident and normal healing shall be taken into account.
Frequency of, and exposure time in, the hazardous zone (F)	F_1 F_2	Rare to more often exposure in the hazardous zone Frequent to permanent exposure in the hazardous zone	3 See comment 1 above.
Possibility of avoiding the hazardous event (P)	P_1 P_2	Possible under certain conditions Almost impossible	4 This parameter takes into account operation of a process (supervised (i.e. operated by skilled or unskilled persons) or unsupervised); – rate of development of the hazardous event (for example suddenly, quickly or slowly); – ease of recognition of danger (for example seen immediately, detected by technical measures or detected without technical measures); avoidance of hazardous event (for example escape routes possible, not possible or possible under certain conditions); – actual safety experience (such experience may exist with an identical EUC or a similar EUC or may not exist).
Probability of the unwanted occurrence (W)	W_1 W_2 W_3	A very slight probability that the unwanted occurrences will come to pass and only a few unwanted occurrences are likely A slight probability that the unwanted occurrences will come to pass and few unwanted occurrences are likely A relatively high probability that the unwanted occurrences will come to pass and frequent unwanted occurrences are likely	5 The purpose of the W factor is to estimate the frequency of the unwanted occurrence taking place without the addition of any safety-related systems (E/E/PE or other technology) but including any external risk reduction facilities. 6 If little or no experience exists of the EUC, or the EUC control system, or of a similar EUC and EUC control system, the estimation of the W factor may be made by calculation. In such an event a worst case prediction shall be made.

Table E.2 - Example Calibration of the General Purpose Risk Graph

Risk parameter		Classification	Comments
Consequence (C) Number of Fatalities This can be calculated by determining the numbers of people present when the area exposed to the hazard is occupied and multiplying by the vulnerability to the identified hazard. The Vulnerability is determined by the nature of the hazard being protected against. The following factors can be used: V=0,01 Small release of flammable or toxic material V=0,1 Large release of flammable or toxic material V=0.5 As above but also a high probability of catching fire or highly toxic material V=1 Rupture or explosion	C_A C_B C_C C_D	Minor injury Range 0,01 to 0,1 Range >0,1 to 1,0 Range > 1,0	1 The classification system has been developed to deal with injury and death to people. 2 For the interpretation of C_A, C_B, C_C and C_D, the consequences of the accident and normal healing shall be taken into account
Occupancy (F) This is calculated by determining the proportional length of time the area exposed to the hazard is occupied during a normal working period. NOTE 1 - If the time in the hazardous area is different depending on the shift being operated then the maximum should be selected. NOTE 2 - It is only appropriate to use F_A where it can be shown that the demand rate is random and not related to when occupancy could be higher than normal. The latter is usually the case with demands which occur at equipment start-up or during the investigation of abnormalities.	F_A F_B	Rare to more often exposure in the hazardous zone. Occupancy less than 0,1 Frequent to permanent exposure in the hazardous zone	3 See comment 1 above.
Probability of avoiding the hazardous event (P) if the protection system fails to operate.	P_A P_B	Adopted if all conditions in column 4 are satisfied Adopted if all the conditions are not satisfied	4 P_A should only be selected if all the following are true: – facilities are provided to alert the operator that the SIS has failed – independent facilities are provided to shut down such that the hazard can be avoided or which enable all persons to escape to a safe area – the time between the operator being alerted and a hazardous event occurring exceeds 1 hour or is definitely sufficient for the necessary actions.
Demand rate (W) The number of times per year that the hazardous event would occur in absence of a SIS. To determine the demand rate it is necessary to consider all sources of failure that can lead to one hazardous event. In determining the demand rate, limited credit can be allowed for control system performance and intervention. The performance which can be claimed if the control system is not to be designed and maintained according to IEC 61511, is limited to below the performance ranges associated with SIL1.	W_1 W_2 W_3	Demand rate less than 0,1W per year Demand rate between 0.1W and W per year Demand rate between W and 10W per year For demand rates higher than 10W per year higher integrity shall be needed	5 The purpose of the W factor is to estimate the frequency of the hazard taking place without the addition of the SIS If the demand rate is very high the SIL has to be determined by another method or the risk graph recalibrated. It should be noted that risk graph methods may not be the best approach in the case of applications operating in continuous mode (IEC 61511 1, Clause 3.1.48.2). 6. The value of W should be determined from corporate criteria on tolerable risk taking into consideration other risks to exposed persons.
NOTE This is an example to illustrate the application of the principles for the design of risk graphs. Risk graphs for particular applications and particular hazards will need to be agreed with those involved, taking into account tolerable risk, see E.1 to E.6.			

Annex F
(informative)

Semi-quantitative method using layer of protection analysis (LOPA)

F.1 General

F.1.1 Description

This annex describes a method called the Layer of Protection Analysis (LOPA) but is not is not intended to be a definitive account of the method, but rather it is intended to illustrate the general principles.

F.1.2 Annex Reference

This annex is based on a method described in more detail in the AIChE "Layer of Protection Analysis – Simplified Process Risk Assessment" publication (see ref [5] in the bibliography). This reference details many ways of using LOPA techniques.

In one approach, all relevant parameters are rounded to the higher decade range (for example, a probability of $5 \cdot 10^{-2}$ is rounded to 10^{-1}. This is a very conservative approach and can lead to significantly higher SIL levels. Data uncertainty should however be recognised by rounding all parameter values to the next highest significant figure (for example, $5{,}4 \cdot 10^{-2}$ should be rounded to $6 \cdot 10^{-2}$).

F.1.3 Method description

LOPA analyses hazards to determine if safety functions are required and if so, the required SIL of each safety function. The LOPA method needs to be adapted to meet the risk acceptance criteria to be applied. The method starts with data developed in the hazard identification and accounts for each identified hazard by documenting the initiating causes and the protection layers that prevent or mitigate the hazard. The total amount of risk reduction can then be determined and the need for more risk reduction analysed. If additional risk reduction is required and if it is to be provided in the form of an E/E/PES, the LOPA methodology allows the determination of the appropriate SIL. For each hazard an appropriate SIL is determined to reduce risks to tolerable levels. table F.1 shows a typical LOPA format

F.2 Impact event

Using Table F.1, each Impact event description (consequence) determined from the hazard identification is entered in column 1 of table F.1.

F.3 Severity level

The severity level of the event is entered in column 2 of table F.1. The severity level will be derived from a table that specifies general descriptions of consequence levels e.g. minor, severe, catastrophic with specified consequence ranges and maximum frequency for each severity level. In effect this table sets down the user tolerability criteria. Information will be needed to allow severity levels and maximum frequencies to be determined for events leading to safety and environmental consequences.

F.4 Initiating cause

All the initiating causes of the impact event are listed in column 3 of table F.1. Impact events may have many initiating causes, and all should be listed.

F.5 Initiation likelihood

Likelihood values of each of the initiating causes listed in column 3 of table F.1, in events per year, are entered into column 4 of table F.1.

Initiation likelihood can be calculated from generic data on equipment failure rates and knowing proof test intervals, or from facility records. Low initiation likelihood should only be used where there is sufficient statistical basis for the data.

Table F.1 – LOPA report

Severity level C = Catastrophic, E = Extensive, S = Serious, M = Minor

Likelihood values are events per year. Other numerical values are probabilities of failure on demand average.

Ref	1	2	3	4	5			6	7	8	9	10	11
					Protection layers (PLs)								
	Impact Event Description F.2	Severity Level F.3	Initiating Cause F.4	Initiation Likelihood F.5	General Design F.6.1	Control System F.6.2	Alarms, Etc. F.6.3	Additional Mitigation, Restricted Access F.7	Additional Mitigation F.8	Intermediate Event Likelihood F.9	PFD_{avg} required for E/E/PES (and SIL) F.10	Mitigated Event Likelihood F.11	Notes
1	Overspeed of rotor leading to fracture of casing	Loss of life of persons located adjacent to casing, fatalities will not exceed 2	Speed control system fails	0,1	1	1	1	0,1	0,1	10^{-3}	$5 \cdot 10^{-3}$ (SIL 2 with a minimum PFD_{avg} of $5 \cdot 10^{-3}$)	10^{-5}	
			Loss of load	1	1	0,1	1	0,1	0,1	10^{-3}			
			Clutch failure	0,1	1	0,1	1	0,1	0,1	10^{-4}			
						0,1 credit given to control system		Occupancy limited, persons not present 90% of the time	Fatality will only occur if fragments contact persons	Total $2,1 \cdot 10^{-3}$		Tolerable frequency if fatalities do not exceed 5	
2	Repeat above case for environmental risk analysis												
3													
.				Continued as required.									
.													
N													

NOTE 1 Units in columns 3, 8 and 10 are events per year.

NOTE 2 Units in columns 4 – 7 and 9 are dimensionless. These numbers, between 0 and 1, are the factors by which event likelihood may be multiplied to represent the mitigating effect of the associated protection layer. Thus 1 means no mitigating effect and 0,1 means a factor of 10 risk reduction

F.6 Protection layers (PLs)

F.6.1 General

Each PL consists of a grouping of equipment and/or administrative controls that function independently from other layers.

Design features that reduce the likelihood of an impact event from occurring when an initiating cause occurs are listed first in column 5 of table F.1.

PLs should have the following important characteristics:

- Specificity: A PL is designed solely to prevent or to mitigate the consequences of one potentially hazardous event (for example, a runaway reaction, release of toxic material, a loss of containment, or a fire). Multiple causes may lead to the same hazardous event and therefore multiple event scenarios may initiate action of one PL.
- Independence: A PL is independent of the other PLs associated with the identified hazardous event.
- Dependability: A PL can be counted on to do what it was designed to do. Both random and systematic failure modes are addressed in the design.
- Auditability: A PL is designed to facilitate regular validation of the protective functions. Proof testing and maintenance of the safety system are necessary.

F.6.2 Basic control system

The next item in column 5 of table F.1 is the EUC control system. If a control function prevents the impact event from occurring when the initiating cause occurs, credit based on its PFD_{avg} is claimed. No credit should be claimed for a control function if failure of that function would cause a demand on the E/E/PES. It should also be noted that the PFD_{avg} claimed from a control function should be limited to a minimum of 0,1 if the control function is not designed and operated as a safety system.

F.6.3 Alarms

The last item in column 5 of table F.1 takes credit for alarms that alert the operator and utilize operator intervention. Credit for alarms should only be claimed under the following circumstances:

- Hardware and software used are separate and independent of that used for the control system (for example, input cards and processors should not be shared).
- The alarm is displayed with a high priority in a permanently manned location. Credit claimed for alarms should take into account the following:
  - ✓ The effectiveness of an alarm will depend on the complexity of the task that needs to be performed in the event of the alarm and the other tasks that need to be performed at the same time.
  - ✓ The credit should be limited to a minimum PFD_{avg} of 0,1.
  - ✓ The operator needs to have sufficient time and independent facilities to be able to terminate the hazard. Normally, credit should not be claimed unless the time available between the alarm and the hazard exceeds 15 minutes.

F.7 Additional mitigation

Mitigation layers are normally mechanical, structural, or procedural. Examples include:

- Restricted access.
- Reduction of ignition probability.
- Any other factors that reduce the vulnerability of persons exposed to the hazard.

Mitigation layers may reduce the severity of the impact event, but not prevent the event from occurring. Examples include:

- Deluge systems in the case of a fire.
- Gas alarms.
- Evacuation procedures that would reduce the probability of persons being exposed to an escalating event.

Under mitigation the percentage occupancy of the most exposed person in the hazard zone can be taken account of. This percentage should be determined by establishing the number of hours in the hazardous zone per year and dividing by 8760 hours per year.

The appropriate PFD_{avg} or equivalent for all mitigation layers should be determined and listed in column 6 and 7 of table F.1.

F.8 Intermediate event likelihood

The intermediate event likelihood for each cause is calculated by multiplying the following factors and the result in frequency per year entered in column 8 of table F.1:

- Vulnerability of the most exposed person.
- Initiation likelihood (column 4).
- PFD_{avg} of the PLs, mitigation layers and PLs (Columns 5, 6 & 7).

The total intermediate event frequency should be calculated by adding intermediate event frequencies for each cause.

The total intermediate event frequency should be compared with the tolerable risk frequency for the associated severity level. If the total intermediate frequency exceeds the tolerable frequency then risk reduction will be required. Inherently safer methods and solutions should be considered before additional PLs in the form of E/E/PES are applied.

If the intermediate event likelihood figures cannot be reduced below the maximum frequency criteria then an E/E/PES will be required.

F.9 Safety integrity levels (SILs)

If a safety function is needed, the required SIL can be determined as follows:

- Divide the maximum frequency for the associated severity level by the total intermediate event likelihood for to determine the PFD_{avg} required
- The numeric target value of the PFD_{avg} can then be used in the safety requirement specification together with the associated SIL. The associated SIL can be obtained from table 2 in Part 1.
- If the numeric value of PFD_{avg} is not to be in the process requirements specification and only the required SIL is to be stated, the SIL should be one level higher so that adequate risk reduction will be achieved with all values of PFD_{avg} associated with the specified SIL.
- If the PFD_{avg} required for the tolerable risk is greater than 0,1 the function is allocated the classification "No special safety integrity requirements".

Annex G
(informative)

Determination of safety integrity levels – A qualitative method: hazardous event severity matrix

G.1 General

The numeric method described in annex D is not applicable where the risk (or the frequency portion of it) cannot be quantified. This annex describes the hazardous event severity matrix method, which is a qualitative method that enables the safety integrity level of an E/E/PE safety-related system to be determined from knowledge of the risk factors associated with the EUC and the EUC control system. It is particularly applicable when the risk model is as indicated in figures A.1 and A.2.

The scheme outlined in this annex assumes that each safety-related system and other risk reduction measure is independent.

This annex is not intended to be a definitive account of the method but is intended to illustrate the general principles of how such a matrix could be developed by those having a detailed knowledge of the specific parameters that are relevant to its construction. Those intending to apply the methods indicated in this annex should consult the source material referenced.

NOTE Further information on the hazardous event matrix is given in reference [1] in the bibliography.

G.2 Hazardous event severity matrix

The following requirements underpin the matrix and each one is necessary for the method to be valid:

a) the safety-related systems (E/E/PE and other risk reduction measures are independent;

b) each safety-related system (E/E/PE and other technology) and other risk reduction measures are considered as protection layers which provide, in their own right, partial risk reductions as indicated in figure A.1;

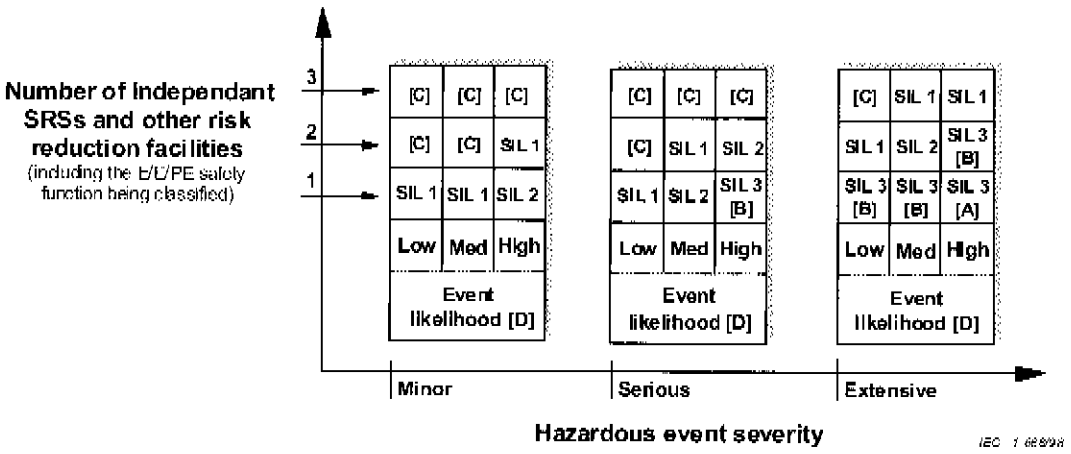
NOTE 1 This assumption is valid only if regular proof tests of the protection layers are carried out.

c) when one protection layer (see b) above) is added, then one order of magnitude improvement in safety integrity is achieved;

NOTE 2 This assumption is valid only if the safety-related systems and external risk reduction facilities achieve an adequate level of independence.

d) only one E/E/PE safety-related system is used (but this may be in combination with an other technology safety-related system and/or external risk reduction facilities), for which this method establishes the necessary safety integrity level

e) The above considerations lead to the hazardous event severity matrix shown in figure G.1. It should be noted that the matrix has been populated with example data to illustrate the general principles. For each specific situation, or sector comparable industries, a matrix similar to figure G.1 would be developed.



[A] One SIL 3 E/E/PE safety function does not provide sufficient risk reduction at this risk level. Additional risk reduction measures are required.
[B] One SIL 3 E/E/PE safety function may not provide sufficient risk reduction at this risk level. Hazard and risk analysis is required to determine whether additional risk reduction measures are necessary.
[C] An independent E/E/PE safety function is probably not required.
[D] Event likelihood is the likelihood that the hazardous event occurs without any safety function or Other risk reduction measure.
[E] Event likelihood and the total number of independent protection layers are defined in relation to the specific application.

Figure G.1 – Hazardous event severity matrix: example (illustrates general principles only)

Bibliography

[1] ANSI/ISA S84:1996, *Application of safety Instrumented Systems for the Process Industries*

[2] *Tolerability of risk from nuclear power stations*, Health and Safety Executive (UK) publication, ISBN 011 886368 1

[3] *Development guidelines for vehicle based software*, The Motor Industry Reliability Association, Watling St, Nuneaton, Warwickshire, CV10 0TU, United Kingdom, 1994, ISBN 09524156 0 7

[4] Reducing Risks, Protecting People – HSE`s decision making process ISBN 0 7176 2151 0

[5] Layer of Protection Analysis – Simplified Process Risk Assessment – CCPS ISBN 0-8169-0811-7