

	DIN EN 61511-2 (VDE 0810-2)	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 25.040.40 Funktionale Sicherheit – Sicherheitstechnische Systeme für die Prozessindustrie – Teil 2: Anleitungen zur Anwendung des Teils 1 (IEC 61511-2:2003); Deutsche Fassung EN 61511-2:2004 Functional safety – Safety instrumented systems for the process industry sector – Part 2: Guidelines for the application of IEC 61511-1 (IEC 61511-2:2003); German version EN 61511-2:2004 Sécurité fonctionnelle – Systèmes instrumentés de sécurité pour le secteur des industries de transformation – Partie 2: Lignes directrices pour l'application de la CEI 61511-1 (CEI 61511-2:2003); Version allemande EN 61511-2:2004 Gesamtumfang 76 Seiten DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE		

Beginn der Gültigkeit

Die von CENELEC am 2004-10-01 angenommene EN 61511-2 gilt als DIN-Norm ab 2005-05-01.

Nationales Vorwort

Vorausgegangener Norm-Entwurf: E DIN IEC 61511-2 (VDE 0810-2):2004-02.

Für die vorliegende Norm 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 zuständig.

Die enthaltene IEC-Publikation wurde vom SC 65A „System aspects“ erarbeitet.

Das IEC-Komitee hat entschieden, dass der Inhalt dieser Publikation bis zum Jahr 2007 unverändert bleiben soll. Zu diesem Zeitpunkt wird entsprechend der Entscheidung des Komitees die Publikation

- bestätigt,
- zurückgezogen,
- durch eine Folgeausgabe ersetzt oder
- geändert.

Die vorliegende Norm enthält eine Anleitung für die Anwendung der **DIN EN 61511-1**.

Sie richtet sich in erster Linie an die für die Errichtung des sicherheitstechnischen Systems verantwortliche Organisation.

Die notwendigen Informationen zu den Anforderungen an die Installation, den Betrieb, die Instandhaltung und Änderung müssen in geeigneter Form zur Verfügung gestellt werden.

Die Betreiberpflichten nach Betriebssicherheitsverordnung bleiben unberührt.

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 nachstehend wiedergegeben.

Tabelle NA.1

Europäische Norm	Internationale Norm	Deutsche Norm	Klassifikation im VDE-Vorschriftenwerk
EN 61511-1:2004	IEC 61511-1:2003 + Corrigendum 2004	DIN EN 61511-1 (VDE 0810-1):2005-05	VDE 0810-1
EN 61511-3:2004	IEC 61511-3:2003 + Corrigendum 2004	DIN EN 61511-3 (VDE 0810-3):2005-05	VDE 0810-3
EN 61131-3:2003	IEC 61131-3:2003	DIN EN 61131-3:2003-12	–
prEN 61078:2003	IEC 56/846/CD:2003	E DIN IEC 61078:2003-11	–
prEN 61025:2004	IEC 56/882/CD:2003	E DIN IEC 61025:2004-01	–
–	IEC 56/865/CD:2003	E DIN IEC 61165:2003-11	–
Reihe der Normen EN 61508	Reihe der Normen IEC 61508	Reihe der Normen DIN EN 61508 (VDE 0803)	VDE 0803
–	ISA TR 84.0.02-2	–	–
–	ISA TR 84.0.02-4	–	–

Nationaler Anhang NB (informativ)

Literaturhinweise

DIN EN 61511-1 (VDE 0810-1):2005-05, *Funktionale Sicherheit – Sicherheitstechnische Systeme für die Prozessindustrie – Teil 1: Allgemeines, Begriffe, Anforderungen an Systeme, Software und Hardware (IEC 61511-1:2003 + Corrigendum 2004); Deutsche Fassung EN 61511-1:2004*

DIN EN 61511-3 (VDE 0810-3):2005-05, *Funktionale Sicherheit – Sicherheitstechnische Systeme für die Prozessindustrie – Teil 3: Anleitung für die Bestimmung der erforderlichen Sicherheits-Integritätslevel (IEC 61511-3:2003 + Corrigendum 2004); Deutsche Fassung EN 61511-3:2004*

DIN EN 61131-3:2003-12, *Speicherprogrammierbare Steuerungen – Teil 3: Programmiersprachen (IEC 61131-3:2003); Deutsche Fassung EN 61131-3:2003*

E DIN IEC 61078:2003-11, *Techniken für die Analyse der Zuverlässigkeit – Verfahren mit dem Zuverlässigkeitsblockdiagramm und Boole'sche Verfahren (IEC 56/846/CD:2003); Deutsche Fassung prEN 61078:2003*

E DIN IEC 61025:2004-01, *Störungsbaumanalyse (IEC 56/882/CD:2003); Deutsche Fassung prEN 61025:2004*

E DIN IEC 61165:2003-11, *Anwendung des Markoff-Verfahrens (IEC 56/865/CD:2003)*

Normen der Reihe DIN EN 61508 (VDE 0803), *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme (Normen der Reihe IEC 61508); Deutsche Fassung Normen der Reihe EN 61508*

– Leerseite –

Deutsche Fassung

Funktionale Sicherheit
Sicherheitstechnische Systeme für die Prozessindustrie
Teil 2: Anleitungen zur Anwendung des Teils 1
(IEC 61511-2:2003)

Functional safety
Safety instrumented systems for the process
industry sector
Part 2: Guidelines for the application of
IEC 61511-1
(IEC 61511-2:2003)

Sécurité fonctionnelle
Systèmes instrumentés de sécurité pour le
secteur des industries de transformation
Partie 2: Lignes directrices pour l'application de
la CEI 61511-1
(CEI 61511-2:2003)

Diese Europäische Norm wurde von CENELEC am 2004-10-01 angenommen. Die CENELEC-Mitglieder sind gehalten, die CEN/CENELEC-Geschäftsordnung zu erfüllen, in der die Bedingungen festgelegt sind, unter denen dieser Europäischen Norm ohne jede Änderung der Status einer nationalen Norm zu geben ist.

Auf dem letzten Stand befindliche Listen dieser nationalen Normen mit ihren bibliographischen Angaben sind beim Zentralsekretariat oder bei jedem CENELEC-Mitglied auf Anfrage erhältlich.

Diese Europäische Norm besteht in drei offiziellen Fassungen (Deutsch, Englisch, Französisch). Eine Fassung in einer anderen Sprache, die von einem CENELEC-Mitglied in eigener Verantwortung durch Übersetzung in seine Landessprache gemacht und dem Zentralsekretariat mitgeteilt worden ist, hat den gleichen Status wie die offiziellen Fassungen.

CENELEC-Mitglieder sind die nationalen elektrotechnischen Komitees von Belgien, Dänemark, Deutschland, Estland, Finnland, Frankreich, Griechenland, Irland, Island, Italien, Lettland, Litauen, Luxemburg, Malta, den Niederlanden, Norwegen, Österreich, Polen, Portugal, Schweden, der Schweiz, der Slowakei, Slowenien, Spanien, der Tschechischen Republik, Ungarn, dem Vereinigten Königreich und Zypern.

CENELEC

Europäisches Komitee für Elektrotechnische Normung
European Committee for Electrotechnical Standardization
Comité Européen de Normalisation Electrotechnique

Zentralsekretariat: rue de Stassart 35, B-1050 Brüssel

Vorwort

Der Text der Internationalen Norm IEC 61511-2:2003, ausgearbeitet von dem SC 65A „System aspects“ des IEC TC 65 „Industrial-process measurement and control“, wurde dem Einstufigen Annahmeverfahren unterworfen und von CENELEC am 2004-10-01 ohne irgendeine Abänderung als EN 61511-2 angenommen.

Nachstehende Daten wurden festgelegt:

- spätestes Datum, zu dem die EN auf nationaler Ebene durch Veröffentlichung einer identischen nationalen Norm oder durch Anerkennung übernommen werden muss (dop): 2005-10-01
- spätestes Datum, zu dem nationale Normen, die der EN entgegenstehen, zurückgezogen werden müssen (dow): 2007-10-01

Anerkennungsnotiz

Der Text der Internationalen Norm IEC 61511-2:2003 wurde von CENELEC ohne irgendeine Abänderung als Europäische Norm angenommen.

Inhalt

	Seite
Vorwort.....	2
Einleitung	7
1 Anwendungsbereich	9
2 Normative Verweisungen	9
3 Begriffe und Abkürzungen	9
4 Übereinstimmung mit dieser Internationalen Norm	9
5 Management der funktionalen Sicherheit	9
5.1 Ziel	9
5.2 Anforderungen	9
6 Anforderungen an den Sicherheitslebenszyklus	15
6.1 Ziele	15
6.2 Anforderungen	16
7 Verifikation	16
7.1 Ziel	16
8 Beurteilung des Risikos und der Gefährdung aus dem Prozess	17
8.1 Ziele	17
8.2 Anforderungen	17
9 Zuordnung der Sicherheitsfunktionen zu den Schutzebenen	19
9.1 Ziel	19
9.2 Anforderungen an den Prozess der Zuordnung	19
9.3 Zusätzliche Anforderungen für Sicherheits-Integritätslevel 4	22
9.4 Anforderungen an Betriebseinrichtungen, die als Schutzebene eingesetzt werden	22
9.5 Anforderungen zur Vermeidung von Ausfällen infolge gemeinsamer Ursache, gleichartigen Ausfällen und abhängigen Ausfällen	22
10 Spezifikation der Sicherheitsanforderungen an das SIS	23
10.1 Ziel	23
10.2 Allgemeine Anforderungen	23
10.3 Sicherheitsanforderungen an das SIS	24
11 Entwurf und Planung des SIS	25
11.1 Ziel	25
11.2 Allgemeine Anforderungen	25
11.3 Anforderungen an das Systemverhalten bei Entdeckung eines Fehlers	29
11.4 Anforderungen an die Hardware-Fehlertoleranz	29
11.5 Anforderungen an die Auswahl von Komponenten und Teilsystemen	31
11.6 Feldgeräte	33
11.7 Schnittstellen	33
11.8 Anforderungen an Instandhaltungs- oder Testeinrichtungen	35
11.9 Ausfallwahrscheinlichkeit sicherheitstechnischer Funktionen	36
12 Anforderungen an die Anwendungssoftware und Auswahlkriterien für Software-Hilfsmittel	38

	Seite
12.1 Anforderungen an den Sicherheitslebenszyklus der Anwendungssoftware.....	38
12.2 Spezifikation der Sicherheitsanforderungen an die Anwendersoftware	41
12.3 Validierungsplanung für die Sicherheit der Anwendungssoftware	43
12.4 Entwurf und Erstellung der Anwendungssoftware.....	43
12.5 Integration der Anwendungs-Software in das SIS-Teilsystem	50
12.6 Vorgehen bei Modifikation einer FPL- und LVL-Software	50
12.7 Verifikation der Anwendungssoftware	51
13 Werksendprüfungen (FAT = Factory Acceptance Test)	52
13.1 Ziele	52
13.2 Empfehlungen.....	53
14 SIS-Montage und Inbetriebnahme.....	53
14.1 Ziele	53
14.2 Anforderungen	53
15 SIS-Sicherheits-Validierung.....	53
15.1 Ziel	53
15.2 Anforderungen	54
16 Betrieb und Instandhaltung des SIS	54
16.1 Ziele	54
16.2 Anforderungen	54
16.3 Wiederholungsprüfungen und Inspektionen	55
17 Modifikationen am SIS	56
17.1 Ziele	56
17.2 Anforderungen	56
18 Außerbetriebnahme des SIS	56
18.1 Ziele	56
18.2 Anforderungen	56
19 Anforderungen an die Information und Dokumentation.....	57
19.1 Ziele	57
19.2 Anforderungen	57
Anhang A (informativ) Beispielhafte Methoden zur Berechnung der Wahrscheinlichkeit eines Ausfalles bei Anforderung einer sicherheitstechnischen Funktion	58
A.1 Allgemeines	58
A.2 Methode des Zuverlässigkeitsblockdiagramms.....	58
A.3 Methode der vereinfachten Gleichungen.....	58
A.4 Methode der Fehlerbaumanalyse	58
A.5 Methode der Markov-Modelle	58
Anhang B (informativ) Erstellung einer typischen SIS-Architektur.....	59
B.1 Hintergrund	59
B.1.1 Einführung.....	59
B.1.2 Anleitungen und Praktiken.....	59

	Seite
B.1.3 Instrumentierung.....	59
B.1.4 Logiksystem.....	59
B.2 Arbeitsablauf.....	59
B.2.1 Einführung	59
B.2.2 Typische Schritte im SIS-Lebenszyklus	59
B.2.3 Zuordnung der Sicherheitsanforderung.....	60
B.2.4 Zuordnung der Sicherheitsanforderungen innerhalb des SIS	60
B.2.5 Architekturbezogene Anforderungen an die Software	61
B.2.6 Erstellung der Anwendungssoftware.....	61
B.3 Beispiel 1	61
B.3.1 Einführung	61
B.3.2 Gefährdungsszenario	61
B.3.3 Spezifikation der Sicherheitsanforderungen und SIL	61
B.3.4 Systemarchitektur	61
B.3.5 Zusätzliche auf die Architektur bezogene Sicherheitssoftware.....	62
B.4 Beispiel 2	62
B.4.1 Einführung	62
B.4.2 Gefährliches Szenario	62
B.4.3 Spezifikation der Sicherheitsanforderungen und SIL	62
B.4.4 Systemarchitektur.....	62
B.4.5 Zusätzliche architekturbezogene Sicherheitssoftware	63
Anhang C (informativ) Anwendungseigenschaften einer Sicherheits-SPS	64
C.1 System.....	64
C.2 Arbeitsablauf.....	64
Anhang D (informativ) Beispiel für eine Methode zur Erstellung der Anwendungssoftware für ein SIS-Logiksystem.....	66
D.1 Zusammenfassung des gesamten Integrationsprozesses für ein System.....	66
D.2 Erstellung der Anwendungssoftware für SIS-Logiksysteme	67
D.3 Programmierstandards für den Anwendungsprogrammierer	68
D.4 Weitere Anforderungen für die Konfiguration/die Programmerstellung und Laufzeitsysteme für Sicherheitsanwendungen	68
D.5 Annahmen	69
Anhang E (informativ) Beispiel für die Entwicklung extern aufgebauter Diagnosen für eine programmierbare Sicherheitssteuerung	70
E.1 Intern aufgebaute Diagnosen	70
E.2 Extern aufgebaute Diagnosen	70
E.3 Literaturhinweis	72
Bilder	
Bild 1 – Gesamtrahmen dieser Norm	8
Bild 2 – Unabhängigkeit von BPCS-Funktion und auslösender Ursache	22
Bild 3 – Software-Entwicklungsprozess (das „V-Modell“)	39

	Seite
Bild C.1 – Logiksystem.....	64
Bild E.1 – Zeitdiagramm eines externen Watchdog.....	71
Tabellen	
Tabelle 1 – Typischer Aufbau und Inhalt eines Sicherheitshandbuchs	48

Einleitung

Sicherheitstechnische Systeme sind seit vielen Jahren für sicherheitstechnische Aufgaben in der Prozessindustrie im Einsatz. Wenn der Einsatz der Prozessleittechnik für sicherheitstechnische Funktionen effizient sein soll, dann muss sie bestimmten Mindestanforderungen entsprechen.

Diese Internationale Norm behandelt die Anwendung sicherheitstechnischer Systeme in der Prozessindustrie. Sie fordert außerdem die Durchführung einer Gefährdungs- und Risikoanalyse, um daraus die Spezifikation sicherheitstechnischer Systeme ableiten zu können. Andere Sicherheitssysteme werden nur insofern betrachtet, dass ihr Beitrag bei der Betrachtung der Leistungsanforderung an die sicherheitstechnischen Systeme berücksichtigt werden kann. Das sicherheitstechnische System umfasst dabei alle zur Ausführung der sicherheitstechnischen Funktion erforderlichen Komponenten und Subsysteme vom Sensor bis zum Aktor.

Der „Sicherheitslebenszyklus“ und der „Sicherheits-Integritätslevel“ (SIL) bilden die Grundlage für die Anwendung dieser Internationalen Norm.

Die in dieser Norm betrachteten sicherheitstechnischen Systeme beruhen auf elektrischer (E) /, elektronischer (E) / und programmierbarer elektronischer (PE) Technologie. Wenn andere Technologien zur Realisierung logischer Steuerungen verwendet werden, sollten die grundlegenden Prinzipien dieser Norm in entsprechender Weise angewendet werden. In dieser Norm werden auch die Sensoren und Aktoren sicherheitstechnischer Systeme betrachtet, unabhängig von der Technologie, in der sie ausgeführt sind. Diese Norm ist innerhalb des Rahmens der IEC 61508 zugeschnitten auf die Prozessindustrie (siehe [Anhang A](#)).

Diese Internationale Norm beschreibt die notwendigen Tätigkeiten im Sicherheits-Lebenszyklus, damit die oben genannten Mindestanforderungen erfüllt werden können. Dieser Ansatz wurde gewählt, damit eine überlegte und einheitliche technische Vorgehensweise zustande kommt.

In den meisten Fällen lässt sich die Sicherheit am besten durch den Entwurf eines sicheren Prozesses gewährleisten. Wenn erforderlich kann dies mit einem oder mehreren Schutzsystemen im Hinblick auf jegliche identifizierte Restrisiken verbunden werden. Schutzsysteme können auf unterschiedlichen Technologien (chemische, mechanische, hydraulische, pneumatische, elektrische, elektronische, programmierbar elektronische Einrichtungen etc.) beruhen.

Insbesondere

- fordert diese Norm die Durchführung einer Gefährdungs- und Risiko-Beurteilung, um die übergreifenden Sicherheitsanforderungen festzulegen;
- fordert diese Norm die Zuordnung der Sicherheitsanforderungen zu einzelnen sicherheitstechnischen Systemen;
- arbeitet diese Norm innerhalb eines Betrachtungsrahmens, der alle sicherheitstechnischen Methoden zur Erlangung funktionaler Sicherheit umfasst;
- führt diese Norm den Gebrauch bestimmter Tätigkeiten, wie z. B. Sicherheits-Management, im einzelnen auf, die sich auf alle Methoden zur Erlangung der funktionalen Sicherheit anwenden lassen.

Diese Internationale Norm über sicherheitstechnische Systeme für die Prozessindustrie

- behandelt alle Zeitpunkte innerhalb des Sicherheits-Lebenszyklus vom anfänglichen Konzept, Entwurf, Ausführung, Betrieb und Instandhaltung bis hin zur Außerbetriebnahme;
- erlaubt es, bereits bestehende oder neue landesspezifische Normen für die Prozessindustrie mit dieser Norm zu harmonisieren.

Diese Internationale Norm strebt nach einer hohen Übereinstimmung (beispielsweise bezüglich zugrundeliegender Prinzipien, Terminologie, Dokumentation) innerhalb der Prozessindustrie. Dies sollte sowohl sicherheitstechnische als auch ökonomische Vorteile bringen.

In Staaten, in denen von Seiten des Gesetzgebers (beispielsweise durch Bund, Länder oder Gemeinden) Vorschriften bezüglich Prozessentwurf, Prozessmanagement oder andere Anforderungen erlassen wurden, haben diese Vorrang gegenüber den Anforderungen dieser Norm.

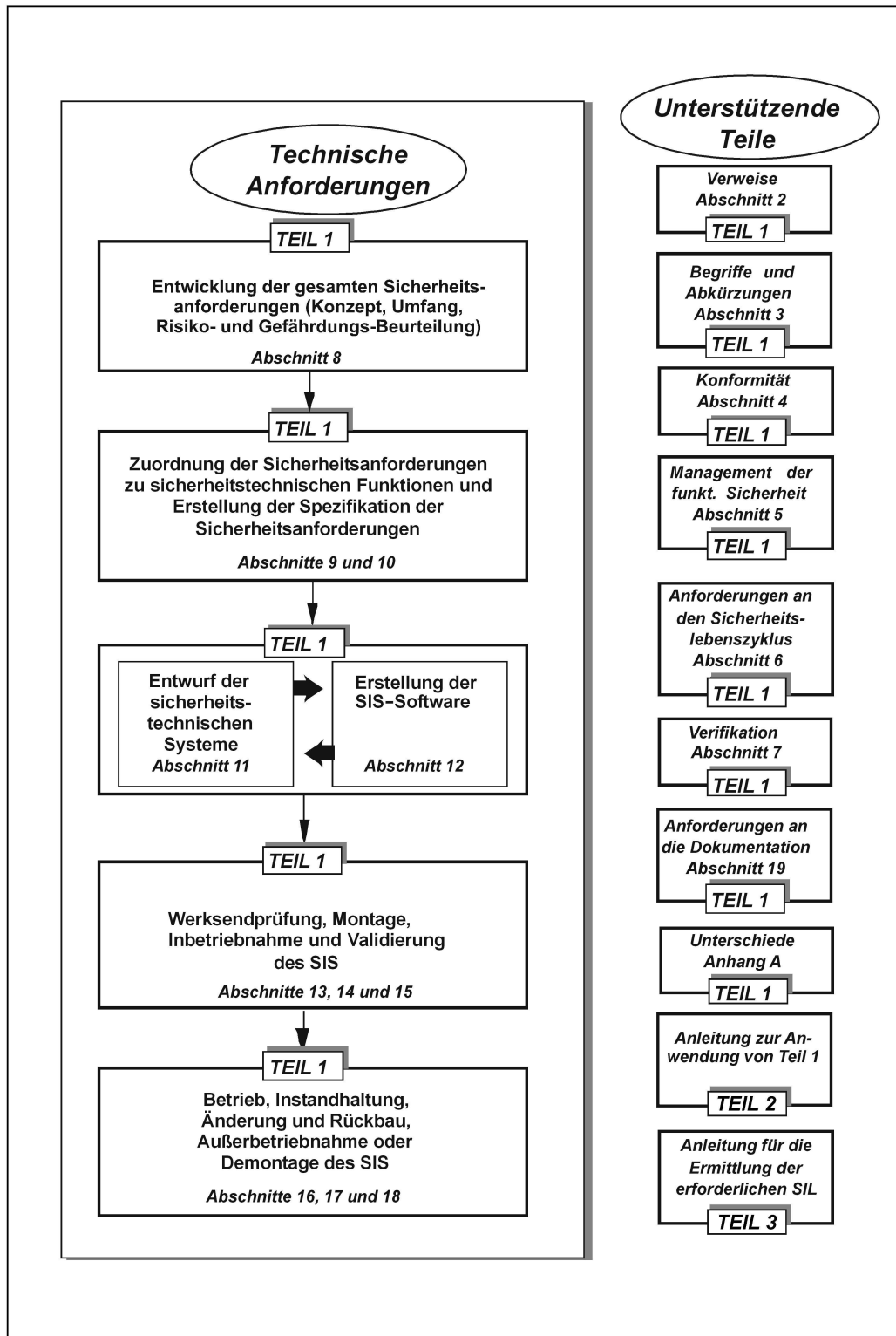


Bild 1 – Gesamtrahmen dieser Norm

1 Anwendungsbereich

IEC 61511-2 ist eine Anleitung zur Spezifikation, zur Planung, zur Errichtung, zum Betrieb und zur Instandhaltung von in IEC 61511-1 definierten sicherheitstechnischen Funktionen und des zugehörigen sicherheitstechnischen Systems. IEC 61511-2 ist so aufgebaut, dass jede Abschnitts- bzw. Unterabschnittsnummer der entsprechenden Abschnittsnummer der IEC 61511-1 entspricht (mit Ausnahme der Anhänge).

2 Normative Verweisungen

Keine weitergehende Anleitung vorgesehen.

3 Begriffe und Abkürzungen

Keine weitergehende Anleitung vorgesehen, außer für 3.2.68 und 3.2.71 der IEC 61511-1.

3.2.68 Eine Sicherheitsfunktion soll ein bestimmtes unerwünschtes Ereignis verhindern, beispielsweise „verhindere einen Druckanstieg im Behälter ABC456 auf über 100 bar“. Eine Sicherheitsfunktion kann realisiert werden durch

- a) ein einzelnes sicherheitstechnisches System (SIS) oder
- b) ein oder mehrere sicherheitstechnische Systeme und/oder andere Schutzebenen.

Im Fall b) muss jedes sicherheitstechnische System oder jede andere Schutzebene in der Lage sein, die Schutzfunktion auszuführen, und ihre Kombination muss die erforderliche Risikoreduzierung erreichen (Zielwert für die Prozesssicherheit).

3.2.71 Sicherheitstechnische Funktionen werden aus einer Sicherheitsfunktion abgeleitet, haben einen zugeordneten Sicherheits-Integritätslevel (SIL) und werden von einem speziellen sicherheitstechnischen System (SIS) ausgeführt, beispielsweise „schließe Ventil XY123 innerhalb von fünf Sekunden, wenn der Druck in Behälter ABC456 100 bar erreicht“. Es ist anzumerken, dass die Komponenten eines sicherheitstechnischen Systems von mehr als einer sicherheitstechnischen Funktion verwendet werden können.

4 Übereinstimmung mit dieser Internationalen Norm

Keine weitergehende Anleitung vorgesehen.

5 Management der funktionalen Sicherheit

5.1 Ziel

Ziel des Abschnitts 5 der IEC 61511-1 ist die Bereitstellung von Anforderungen, wie die für die Erreichung der funktionalen Sicherheitsziele notwendigen Managementtätigkeiten durchzuführen sind.

5.2 Anforderungen

5.2.1 Allgemeines

5.2.1.1 Keine weitergehende Anleitung vorgesehen.

5.2.1.2 Wenn eine Organisation für eine oder mehrere für die funktionale Sicherheit erforderlichen Tätigkeiten verantwortlich ist und diese Organisation entsprechend den Vorgehensweisen der Qualitätssicherung arbeitet, dann werden viele der in diesem Abschnitt beschriebenen Tätigkeiten schon zum Zweck der Qualität durchgeführt werden. In diesen Fällen kann es unnötig sein, diese Tätigkeiten aus

Gründen der funktionalen Sicherheit zu wiederholen. In solchen Fällen sollten die im Rahmen der Qualitätssicherung durchgeführten Vorgehensweisen überprüft werden, um sicherzustellen, dass sie zur Erreichung der Ziele der funktionalen Sicherheit geeignet sind.

5.2.2 Organisation und Mittel

5.2.2.1 Der Aufbau der Organisation, die innerhalb eines Unternehmens/eines Standortes/einer Anlage/eines Projekts mit sicherheitstechnischen Systemen zu tun hat, sollte festgelegt und die Aufgaben und Verantwortlichkeiten jedes Teils der Organisation sollten klar verstanden und kommuniziert werden. Innerhalb der Organisation sollten individuelle Aufgaben einschließlich ihrer Beschreibung und ihres Zweckes festgelegt werden. Für jede Aufgabe sollten unmissverständliche Verantwortlichkeiten festgelegt und diese im Einzelnen auch als solche erkannt werden. Zusätzlich sollte festgelegt werden, wem der Einzelne untersteht und wer dieses Unterstellungsverhältnis festgelegt hat. Damit wird sichergestellt, dass jeder Mitarbeiter einer Organisation seine Aufgabe und Verantwortlichkeit für sicherheitstechnische Systeme versteht.

5.2.2.2 Die Fähigkeiten und Kenntnisse, die für jede Tätigkeit im Sicherheitslebenszyklus sicherheitstechnischer Systeme erforderlich sind, sollten festgelegt werden, außerdem für jede Fähigkeit der entsprechende Qualifikationsgrad. Für jede Fähigkeit sollten die zur Verfügung stehenden Ressourcen hinsichtlich ihrer Qualifikation und der Anzahl der zur Verfügung stehenden Personen überprüft werden. Im Falle erkannter Abweichungen sollten Ausbildungspläne aufgestellt werden, um den erforderlichen Qualifikationsgrad rechtzeitig zu erreichen. Wenn Fähigkeiten fehlen, kann geeignetes qualifiziertes und erfahrenes Personal eingestellt oder zugekauft werden.

5.2.3 Risikobewertung und Risiko-Management

Die Anforderung in **5.2.3 der IEC 61511-1** verlangt, dass Gefährdungen ermittelt, die entsprechenden Risiken bestimmt und die notwendige Risikoreduzierung festgelegt werden. Um diese Arbeiten durchzuführen, existieren zahlreiche verschiedene Methoden. Die **IEC 61511-1** schreibt keine bestimmte Methode vor. Der Leser wird dagegen aufgefordert, zu diesem Thema die in der **IEC 61511-3** beschriebenen Methoden durchzusehen. Siehe **8.2.1** für weitergehende Anleitung.

5.2.4 Planung

5.2.4.1 Mit diesem Unterabschnitt wird sichergestellt, dass innerhalb des Gesamtprojektes eine angemessene Sicherheitsplanung durchgeführt wird, die alle erforderlichen Tätigkeiten in allen Phasen des Lebenszyklus (beispielsweise Planung, Betrieb der Anlage) anspricht. Die Norm legt keine bestimmte Struktur für diese Planungstätigkeiten fest, aber sie verlangt, dass diese regelmäßig überprüft und auf den neuesten Stand gebracht werden.

5.2.5 Ausführung und Überwachung

5.2.5.1 Mit diesem Unterabschnitt wird sichergestellt, dass wirksame Management-Verfahrensweisen in Kraft sind, die:

- sicherstellen, dass alle Empfehlungen aus der Gefährdungsanalyse, der Risikoabschätzung, anderen Beurteilungs- und Auditierungstätigkeiten und den Tätigkeiten im Rahmen der Verifizierung und Validierung in zufrieden stellender Weise umgesetzt werden;
- festlegen, dass das SIS während seiner gesamten Betriebszeit in Übereinstimmung mit der Spezifikation der Sicherheitsanforderungen arbeitet.

5.2.5.2 Der Ausdruck „Hersteller“ schließt in diesem Zusammenhang Planungs- und Instandhaltungsfirmen genauso ein wie Lieferanten von Geräten.

5.2.5.3 Die Leistungsfähigkeit des SIS sollte regelmäßig überprüft werden, um sicherzustellen, dass die ursprünglichen Annahmen, die während der Erstellung der Spezifikation der Sicherheitsanforderungen getroffen wurden, noch immer zutreffen. Beispielsweise sollten die Ausfallraten verschiedener Komponenten des SIS regelmäßig überprüft werden, um sicherzustellen, dass sie immer noch den ursprünglichen Festlegungen entsprechen. Wenn die Ausfallraten schlechter sind als ursprünglich angenommen, kann eine Entwurfsänderung erforderlich werden. In gleicher Weise sollte die Anforderungsrate an das SIS überprüft

werden. Wenn die Anforderungsrate höher ist als ursprünglich angenommen, kann eine Anpassung des SIL erforderlich werden.

5.2.6 Beurteilung, Auditierung und Revisionen

Beurteilungen und Audits sind Hilfsmittel zur Ermittlung und Beseitigung von Fehlern. Die folgenden Absätze zeigen die Unterschiede zwischen diesen beiden Tätigkeiten auf.

Die Beurteilung der funktionalen Sicherheit hat zum Ziel, zu ermitteln, ob die in den einzelnen Phasen des Lebenszyklus getroffenen Vorkehrungen zum Erreichen der Sicherheit angemessen sind. Es werden die von den für die funktionale Sicherheit Verantwortlichen getroffenen Entscheidungen durch Gutachter beurteilt. Vor der Inbetriebnahme würde beispielsweise die Eignung der Vorgehensweisen für die Instandhaltung beurteilt werden.

Auditoren für funktionale Sicherheit bestimmen aus den Aufzeichnungen eines Projekts oder aus der Anlage, ob die erforderlichen Vorgehensweisen in der festgelegten Häufigkeit durch Personen mit der erforderlichen Qualifikation durchgeführt wurden. Auditoren sind nicht erforderlich, die Eignung der betrachteten Arbeiten zu beurteilen; wenn sie jedoch feststellen, dass sich bei Änderungen Vorteile ergeben würden, dann sollte dies in ihrem Bericht vermerkt werden.

Es sollte angemerkt werden, dass sich diese beiden Tätigkeiten, nämlich des Gutachters und des Auditors, in vielen Fällen überschneiden. Beispielsweise kann ein Auditor nicht nur feststellen, ob ein Bediener die erforderliche Ausbildung erhalten hat, sondern auch beurteilen, ob die Ausbildung den erforderlichen Qualifikationsgrad gebracht hat.

5.2.6.1 Beurteilung der funktionalen Sicherheit

5.2.6.1.1 Die Beurteilung der funktionalen Sicherheit ist für den Nachweis, dass ein sicherheitstechnisches System (SIS) hinsichtlich sicherheitstechnischer Funktion(en) und Sicherheits-Integritätslevel (SIL) seine Anforderungen erfüllt, von grundlegender Bedeutung. Grundlegendes Ziel dieser Beurteilung ist der Nachweis der Übereinstimmung des Prozesses der Systemerstellung mit anerkannten Normen und Vorgehensweisen durch eine unabhängige Beurteilung. Eine Beurteilung des SIS kann zu verschiedenen Zeitpunkten im Lebenszyklus erforderlich sein. Aus Gründen der erforderlichen Effizienz sollte eine Vorgehensweise festgelegt werden, die den Umfang dieser Beurteilung zusammen mit einer Anleitung über die Zusammensetzung des Beurteilungsteams vorgibt.

Die folgenden Punkte werden in der Praxis als sinnvoll für eine Beurteilung der funktionalen Sicherheit erachtet:

- Für jede Beurteilung der funktionalen Sicherheit sollte ein Plan aufgestellt werden, der den Umfang der Beurteilung, die Gutachter und ihre Fachkundigkeit und die Informationen, die durch die Beurteilung gewonnen werden sollen, enthält.
- Die Beurteilung der funktionalen Sicherheit sollte andere Normen und Handlungsweisen berücksichtigen, die in externen oder Werksnormen, Handbüchern, Vorgehensweisen oder praktischen Verfahrensanweisungen enthalten sind. Der Plan für die Beurteilung der funktionalen Sicherheit sollte festlegen, was beurteilt wird (System, Anwendungsbereich).
- Die Häufigkeit von Beurteilungen der funktionalen Sicherheit kann zwischen unterschiedlichen Systemen schwanken, sollte jedoch zumindest immer dann stattfinden, bevor die möglichen Gefährdungen vorliegen. Einige Unternehmen führen auch eine Beurteilung vor der Bau- und Montagephase durch, um kostspielige Nacharbeiten später im Lebenszyklus zu vermeiden.
- Die Häufigkeit und Tiefe von Beurteilungen der funktionalen Sicherheit sollte unter Berücksichtigung folgender Systemeigenschaften festgelegt werden:
 - Komplexität;
 - Bedeutung für die Sicherheit;
 - vorliegende Erfahrungen mit ähnlichen Systemen;
 - Standardisierungsgrad der Konstruktionsmerkmale.

- Vor der Beurteilung sollten ausreichende Nachweise für Tätigkeiten im Rahmen der Planung, Montage, Verifizierung und Validierung vorliegen. Die Verfügbarkeit ausreichender Nachweise kann selbst ein Beurteilungskriterium darstellen. Der Nachweis sollte den gegenwärtigen/abgenommenen Zustand der Planung oder Montage widerspiegeln.
- Die Beurteilenden müssen ausreichend unabhängig sein.
- Die Beurteilenden sollten geeignete Erfahrungen und Kenntnisse für die Technologie und den Anwendungsbereich des beurteilten Systems haben.
- Ein systematischer und in sich geschlossener Ansatz sollte für die Beurteilung der funktionalen Sicherheit über den gesamten Lebenszyklus und über die Systeme hinweg beibehalten werden. Da die Beurteilung der funktionalen Sicherheit eine subjektive Tätigkeit darstellt, sollten genaue Richtlinien, möglicherweise in Form von Checklisten, festgelegt werden, was innerhalb einer bestimmten Organisation annehmbar ist, um so diese Subjektivität auf ein Minimum zu reduzieren.

Die während der Beurteilung der funktionalen Sicherheit erstellten Aufzeichnungen sollten vollständig und die daraus gezogenen Schlussfolgerungen mit dem für die funktionale Sicherheit verantwortlichen Management abgestimmt sein, bevor die nächste Phase im Lebenszyklus beginnt.

5.2.6.1.2 Durch die Forderung nach einer vom Projektteam unabhängigen Person soll die Objektivität bei der Beurteilung erhöht werden. Durch eine Persönlichkeit mit bestimmten Eigenschaften (beispielsweise Erfahrung, Ausbildung, Position) wird erreicht, dass Einwände in angemessener Weise zur Kenntnis genommen und behandelt werden. Die Anmerkung empfiehlt, das Team bei großen Projekten oder Überprüfungsteams mit mehr als einer besonders erfahrenen und kompetenten Person zu besetzen, die unabhängig vom Projektteam ist.

Abhängig von der Organisation und der vorliegenden Fachkunde in einem Unternehmen muss die Forderung nach einem unabhängigen Beurteiler möglicherweise durch Nutzung einer externen Organisation erfüllt werden. Umgekehrt können Unternehmen, die über interne Einheiten mit Fähigkeiten in der Risikobeurteilung und der Anwendung sicherheitstechnischer Systeme verfügen, die unabhängig und (hinsichtlich ihrer Führung und anderer Ressourcen) getrennt von den Projektverantwortlichen sind, ihre eigenen Kräfte verwenden, um die Anforderung nach einer unabhängigen Organisation zu erfüllen.

5.2.6.1.3 Der Umfang der Beurteilung hängt von Umfang und Komplexität eines Projekts ab. Es kann möglich sein, die Ergebnisse mehrerer Phasen zum gleichen Zeitpunkt zu beurteilen. Dies trifft besonders bei kleinen Änderungen in einer laufenden Anlage zu.

5.2.6.1.4 In einigen Ländern wird die zum Zeitpunkt 3 stattfindende Beurteilung der funktionalen Sicherheit auch als Sicherheitsbeurteilung vor der Inbetriebnahme bezeichnet.

5.2.6.1.5 Keine weitergehende Anleitung vorgesehen.

5.2.6.1.6 Keine weitergehende Anleitung vorgesehen.

5.2.6.1.7 Dem Beurteilungsteam sollte jegliche Information zur Verfügung stehen, die es für die Durchführung der Beurteilung für erforderlich hält. Dies schließt Informationen aus der Gefährdungs- und Risikoanalyse und der Planungsphase bis zur Montage, Inbetriebnahme und Validierung ein.

5.2.6.2 Auditierung und Revision

5.2.6.2.1 Dieser Unterabschnitt gibt eine Anleitung zum Thema Auditierung und verwendet dazu ein Beispiel, um die Tätigkeiten zu verdeutlichen.

a) Arten von Audits

Die Betriebsleitung sowie die zuständigen Ingenieure für die Instandhaltung und die Planung erhalten aus Audits sicherheitstechnischer Systeme nützliche Informationen. Sie versetzen das Management in die Lage, rechtzeitig reagieren zu können und über den Zustand und die Wirksamkeit ihrer sicherheitstechnischen Systeme informiert zu sein. Es gibt viele Arten von Audits. Die gewählte Art, der Umfang und die Häufigkeit des Audits einer bestimmten Tätigkeit sollte deren möglichen Einfluss auf die Sicherheitsintegrität widerspiegeln.

Arten von Audits sind:

- 1) Audits von unabhängigen Stellen und interne Audits
- 2) Inspektionen
- 3) Sicherheitsrundgänge (Sicherheitsrundgänge in der Anlage und Untersuchungen von Zwischenfällen)
- 4) Überprüfung sicherheitstechnischer Systeme mit Hilfe von Fragebögen

Es besteht ein Unterschied zwischen „Überwachung und Überprüfung“ und Tätigkeiten im Rahmen eines Audits. Überwachung und Überprüfung konzentriert sich darauf, die Wirksamkeit von bestimmten Tätigkeiten im Rahmen des Lebenszyklus zu überprüfen (beispielsweise, dass ein Verantwortlicher den Abschluss einer Instandhaltungstätigkeit überprüft, bevor er eine bestimmte Komponente wieder für den Betrieb freigibt). Im Gegensatz dazu sind Tätigkeiten im Rahmen eines Audits umfassender und befassen sich mit der gesamten Ausführung der sicherheitstechnischen Systeme im Sicherheitslebenszyklus. Ein Audit schließt die Überprüfung ein, ob das Überwachungs- und Überprüfungsprogramm durchgeführt wird.

Audits und Inspektionen können durch Mitarbeiter des eigenen Unternehmens/des Standortes/der Anlage/des Projekts (beispielsweise internes Audit) oder durch unabhängige Personen (beispielsweise Auditoren eines Unternehmens, der Qualitätssicherungsabteilung, von Behörden, von Kunden oder von Dritten) durchgeführt werden.

Die verschiedenen Managementebenen wenden geeignete Arten von Audits an, um Informationen über die Eignung und Wirksamkeit ihrer sicherheitstechnischen Systeme zu erhalten. Informationen aus Audits können verwendet werden, um Vorgehensweisen zu identifizieren, die nicht richtig befolgt wurden, und um ihre Anwendung zu verbessern.

b) Auditstrategie

Für Standorte/Anlagen/Projekte, die Auditprogramme erstellen, kommen rollierende, unabhängige oder interne Audit- und Inspektionsprogramme in Betracht.

Rollierende Programme werden regelmäßig aktualisiert, um die zurückliegende Leistungsfähigkeit der sicherheitstechnischen Systeme und die Ergebnisse von Audits sowie aktuelle Punkte und Prioritäten zu berücksichtigen. Dies betrifft alle auf den Standort/die Anlage/das Projekt bezogenen Tätigkeiten und Gesichtspunkte sicherheitstechnischer Systeme innerhalb eines geeigneten Zeitraums und in einer geeigneten Tiefe.

Der Hauptgrund für Audits und ihr besonderer Wert liegt darin, dass auf Basis der gewonnenen Informationen rechtzeitig reagiert werden kann. Die Maßnahmen sollen die Wirksamkeit der sicherheitstechnischen Systeme verbessern, um beispielsweise das Risiko der Mitarbeiter oder Außenstehender zu verringern, verletzt oder getötet zu werden, und zu einer Verbesserung der Sicherheitskultur sowie dazu beizutragen, dass das Entweichen von Stoffen in die Umwelt so weit wie möglich verhindert wird.

Zusammenfassend lässt sich sagen, dass die Auditstrategie aus einer Mischung verschiedener Arten von Audits bestehen kann, die vom Management oder dem Kunden abhängt und das Ziel hat, allen Stufen des Managements die relevanten Informationen für ein rechtzeitiges Handeln zur Verfügung zu stellen.

c) Durchführung und Dokumentation eines Audits

Das Gesamtziel ist es, einen größtmöglichen Nutzen aus der Durchführung des Audits zu ziehen. Dies kann nur dann erreicht werden, wenn alle Beteiligten (einschließlich Auditoren, Kontaktperson, Betriebsleiter, Abteilungsleiter etc.) die Notwendigkeit des Audits erkennen und es beeinflussen können. Die folgenden Ausführungen zum Thema Durchführung und Dokumentation eines Audits stellen eine gewisse Durchgängigkeit in der Vorgehensweise sicher und helfen somit, diese Ziele zu erreichen. Sie beziehen sich auf die folgenden fünf Hauptschritte bei der Durchführung eines Audits:

1) Auditstrategie und Auditplan

Der Zweck eines jeden Audits sollte klar festgelegt und die Auditgruppen sowie deren Aufgaben und Verantwortlichkeiten sollten bestimmt werden.

Es sollte eine Auditstrategie vorliegen.

Es sollte ein Programm für die Audits festgelegt werden.

Es sollten regelmäßige Reviews zu den Themen Durchführung des Audits, Auditprogramm und Auditstrategie stattfinden.

2) Vorbereitung und Planung eines Audits

Vor Beginn eines Audits benennt der Leiter des Standorts/der Anlage/des Projekts und/oder der zuständige Auditkoordinator eine Kontaktperson für das Audit.

Die Auditoren und die benannte Kontaktperson sollten zu einem frühen Zeitpunkt folgende Punkte diskutieren, ein gemeinsames Verständnis für sie entwickeln und sie einvernehmlich verabschieden:

- den Umfang des Audits;
- den zeitlichen Ablauf des Audits;
- die Personen, die verfügbar sein müssen;
- die Grundlage des Audits oder die entsprechende Norm;
- dass durch besondere Anstrengung in der Vorbereitungsphase und durch Einbindung des Betriebspersonals die Chancen für ein erfolgreiches Audit steigen.

Die folgenden Angaben sollten als Anhaltspunkt für die in jeder Phase erforderliche Zeit verwendet werden:

- Vorbereitung: 30 %
- Durchführung: 40 %
- Ergebnisbericht: 20 %
- Follow-up: 10 %

Der Auditor sollte das Audit durch Sammeln von Informationen, Vorgehensweisen/Vorschriften und Daten und sofern erforderlich durch Erstellen von Checklisten vorbereiten.

Der Auditor sollte besonders darauf hinweisen und erläutern, in welchen Fällen der Umfang des Audits während seines Verlaufs geändert werden kann, wenn besondere Beobachtungen oder Abweichungen festgestellt werden.

3) Durchführung des Audits

Ziel des Auditors ist es, das Audit innerhalb des festgesetzten Zeitraums etappenweise durchzuführen und dabei so der möglichen Arbeitsunterbrechung der Mitarbeiter des Standorts/der Anlage/des Projekts Rechnung zu tragen.

Die benannte Kontaktperson sollte regelmäßig während des Audits über den Stand unterrichtet werden, um so Überraschungen am Ende des Audits zu vermeiden.

Der Auditor sollte versuchen, das betriebliche Personal beim Audit zu beteiligen, um so einen Lerneffekt und Verständnis (der Vorgehensweise und der Feststellungen) und damit Akzeptanz zu erzielen.

Der Erfolg des Audits hängt entscheidend vom Auditor ab – er sollte versuchen, hilfreich, konstruktiv, höflich, zielgerichtet und objektiv zu sein.

Der Auditor sollte auf jeden Fall versuchen, den vereinbarten Umfang und zeitlichen Ablauf einzuhalten – Abweichungen bedürfen der Abstimmung.

4) Ergebnisbericht

Der Auditor sollte eine Abschlussbesprechung am Ende des Audits oder später, in jedem Fall aber vor Veröffentlichung des Abschlussbericht abhalten.

Der entsprechenden Führungsebene sollte Gelegenheit gegeben werden, zum Entwurf des Ergebnisberichts und den dort getroffenen Feststellungen Stellung zu nehmen und diese auf Wunsch bei einem Abschlussgespräch zu diskutieren.

Üblicherweise wird vom Standort/von der Anlage/vom Projekt ein Aktionsplan zu den entsprechenden Feststellungen des Berichts verlangt.

5) Follow-up

Nach Erstellung des Auditberichts ist üblicherweise die Aufstellung eines Aktionsplans erforderlich. Der Auditor kann den erfolgreichen Abschluss der Aktion je nach Erfordernis zu einem bestimmten Zeitpunkt oder beim nächsten Audit kontrollieren.

Der Standort/die Anlage/das Projekt kann geeignete Systeme verwenden, um die Durchführung der Aktionspläne zu verfolgen.

Ein regelmäßiger Rückblick bzw. eine Zusammenfassung der von den einzelnen Auditgruppen in Audits getroffenen Feststellungen sollte erstellt und die Ergebnisse sollten breit gestreut werden.

Die Feststellungen bzw. Ergebnisse der Audits können dazu verwendet werden, die Häufigkeit der Audits anzupassen, und sie sind Grundlage des Management-Reviews der sicherheitstechnischen Systeme.

5.2.6.2.2 Dieser Unterabschnitt betont die Vorgehensweise bei Anlagenänderungen im Auditprozess.

5.2.7 Management der SIS-Konfiguration

5.2.7.1 Anforderungen

5.2.7.1.1 Um die Verfolgbarkeit von Geräten zu ermöglichen und diese während des Lebenszyklus zu erhalten, kann eine Vorgehensweise zur Identifizierung, Erfassung und Verfolgung des Typs bzw. der Versionen jedes Geräts festgelegt werden.

Zum frühestmöglichen Zeitpunkt innerhalb des Sicherheitslebenszyklus sollte jedes einzelne Gerät eine innerhalb der Anlage einzigartige Identifikation erhalten. In einigen Fällen können auch frühere Typen bzw. Versionen, die noch in Gebrauch sind, in gleicher Weise behandelt werden. Dies ist der erste Schritt innerhalb des Konfigurationsmanagements, das die folgenden Überlegungen beinhalten sollte.

Das Konfigurationsmanagementsystem sollte Folgendes einschließen:

- a) Bereitstellung einer Vorgehensweise zur Identifikation aller Einrichtungen während aller Phasen des Lebenszyklus;
- b) eindeutige Identifikation des Typs/der Version und des Stands einschließlich Software jedes Geräts einschließlich des Herstellers, des Datums und sofern zutreffend von Änderungen zu ursprünglich spezifizierten Typen bzw. Versionen;
- c) die Identifikation und Verfolgung aller Maßnahmen und Änderungen aufgrund festgestellter Fehler und Audits;
- d) Verfolgen der Inbetriebnahme mit Stand, Typ bzw. Version der zugehörigen Einrichtungen;
- e) Sicherheitsmaßnahmen zur Verhinderung unbefugter Änderungen während des Betriebs des SIS;
- f) die Identifikation der Version jeder Softwarekomponente, die zu einer bestimmten Version eines Gerätes gehört;
- g) Vorkehrungen für eine Koordination des Updates mehrfacher SIS in einer oder mehreren Anlagen;
- h) schriftliche Genehmigung für die Inbetriebnahme;
- i) eine gültige Unterschriftenliste der für eine Genehmigung der Inbetriebnahme von Geräten Berechtigten;
- j) den Zeitpunkt/die Phase, wann die Geräte der Änderungskontrolle unterworfen werden;
- k) Lenkung der zugeordneten verfügbaren Dokumentation;
- l) Identifikation jedes Typs bzw. jeder Version einer Einrichtung mit ihrer
 - funktionalen Spezifikation;
 - technischen Spezifikation;
- m) alle Abteilungen und Organisationen, die mit dem Management und der Instandhaltung eines SIS betraut sind, liegen fest und die entsprechenden Verantwortlichkeiten sind zugewiesen und von den entsprechenden Beteiligten verstanden.

6 Anforderungen an den Sicherheitslebenszyklus

6.1 Ziele

Die funktionale Sicherheit, die in einer verfahrenstechnischen Anlage erreicht wird, hängt davon ab, dass eine Reihe von Tätigkeiten in zufrieden stellender Art und Weise ausgeführt werden. Der Ansatz eines systematischen Sicherheitslebenszyklus für ein SIS soll dafür sorgen, dass alle die zur Erreichung

funktionaler Sicherheit erforderlichen Tätigkeiten durchgeführt werden und dass Dritten gegenüber ein Nachweis geführt werden kann, dass sie in einer geeigneten Reihenfolge durchgeführt wurden. IEC 61511-1 zeigt in Bild 8 und Tabelle 2 einen typischen Lebenszyklus. Anforderungen für jede Phase des Lebenszyklus sind in den Abschnitten 8 bis 16 der IEC 61511-1 enthalten.

Die Norm lässt zu, dass die Abfolge der festgelegten Tätigkeiten unterschiedlich sein kann, solange sichergestellt ist, dass alle Anforderungen erfüllt werden. Diese Modifikation der Reihenfolge kann Vorteile bieten, wenn dadurch Tätigkeiten, die im Rahmen der Sicherheit durchgeführt werden, besser in normale Projektablaufe integriert werden können. Abschnitt 6 der IEC 61511-1 soll sicherstellen, dass Eingänge und Ausgänge jeder Phase des Lebenszyklus festgelegt und alle wichtigen Anforderungen enthalten sind, wenn ein anderer Sicherheitslebenszyklus verwendet wird.

6.2 Anforderungen

6.2.1 Der Grundgedanke liegt darin, dass der zu verwendende Sicherheitslebenszyklus des SIS im Voraus festgelegt wird. Die Erfahrung zeigt, dass Probleme dann wahrscheinlich sind, wenn dieser Vorgang nicht sauber im Voraus geplant und mit allen verantwortlichen Personen, Abteilungen und Organisationen Übereinstimmung erzielt wurde. Im besten Fall werden Arbeiten verzögert oder müssen wiederholt werden; im schlechtesten Fall kann die Sicherheit beeinträchtigt werden.

6.2.2 Obwohl es nicht als Anforderung definiert ist, so ist es dennoch sinnvoll, zu einem frühen Zeitpunkt den vorgeschlagenen Sicherheitslebenszyklus des SIS mit dem Projektlebenszyklus abzugleichen; dazu gehört auch, welche der Kästchen in Bild 8 der IEC 61511-1 in diesem Projekt zutreffen. Bei diesem Abgleich sollte man sich darüber Gedanken machen, welche Information am Anfang einer Tätigkeit des Sicherheitslebenszyklus erforderlich ist und wer diese Information wahrscheinlich liefern kann. Manchmal kann es vorkommen, dass eine genaue Information über ein spezielles Thema erst spät in der Planungsphase vorliegt. In solchen Fällen kann es nützlich sein, eine Schätzung aufgrund vorliegender Erfahrungen vorzunehmen und die Daten zu einem späteren Zeitpunkt zu bestätigen. In diesem Fall ist es wichtig, dies im Sicherheitslebenszyklus zu vermerken.

6.2.3 Ein weiterer wichtiger Teil bei der Planung des Sicherheitslebenszyklus ist die Festlegung der in jeder Phase anzuwendenden Arbeitstechniken. Die Festlegung solcher Arbeitstechniken ist deshalb wichtig, weil die Notwendigkeit einer bestimmten Arbeitstechnik oft die Mitarbeit einer bestimmten Person oder Abteilung mit den erforderlichen Kenntnissen und der erforderlichen Erfahrung nach sich zieht. Beispielsweise können die Auswirkungen in einer bestimmten Anwendung vom maximalen Druck abhängen, der sich bei einem Ausfallereignis entwickelt, und dieser Druck kann nur über ein dynamisches Modell des Prozesses bestimmt werden. Die erforderlichen Informationen aus der dynamischen Modellbildung haben in diesem Fall einen großen Einfluss auf den Planungsprozess.

7 Verifikation

7.1 Ziel

Mit Hilfe der Verifikation wird sichergestellt, dass die in der Verifikationsplanung festgelegten Tätigkeiten für jede Phase des Sicherheitslebenszyklus tatsächlich ausgeführt wurden und dass die erforderlichen Ergebnisse der Phase in Form von Dokumentation, Hardware oder Software vorliegen und für ihren Zweck geeignet sind.

7.1.1 Anforderungen

7.1.1.1 Die IEC 61511-1 lässt zu, dass Organisationen für die Verifikation ihre eigenen Verfahrensweisen haben, und verlangt nicht, dass diese immer auf die gleiche Art ausgeführt werden. Stattdessen will dieser Unterabschnitt erreichen, dass alle Tätigkeiten im Rahmen der Verifikation zusammen mit zu verwendenden Vorgehensweisen, Maßnahmen und Arbeitstechniken im Voraus geplant werden.

7.1.1.2 Keine weitergehende Anleitung vorgesehen.

7.1.1.3 Es ist wichtig, dass die Ergebnisse der Verifikation vorliegen, so dass gezeigt werden kann, dass eine erfolgreiche Verifikation in allen Phasen des Sicherheitslebenszyklus stattgefunden hat.

8 Beurteilung des Risikos und der Gefährdung aus dem Prozess

8.1 Ziele

Das grundlegende Ziel ist es, die Notwendigkeit für Sicherheitsfunktionen (z. B. Schutzebenen) und zugehörige Leistungsstufen (Risikoreduzierung) festzulegen, die benötigt werden, um einen sicheren Prozess zu gewährleisten. In der Prozessindustrie sind mehrere Schutzebenen üblich, so dass der Ausfall einer einzelnen Ebene nicht zu einer gefährlichen Auswirkung führen wird oder eine solche zulassen kann. **Bild 9 der IEC 61511-1** zeigt typische Schutzebenen.

8.2 Anforderungen

8.2.1 Die Anforderungen an die Gefährdungs- und Risikoanalyse liegen nur in Form der erforderlichen Ergebnisse dieser Aufgabe vor. Dies bedeutet, dass eine Organisation jede Arbeitstechnik verwenden kann, die sie für geeignet hält, vorausgesetzt, ihre Ergebnisse liegen als verständliche Beschreibung der Sicherheitsfunktionen und ihrer zugeordneten Leistungsstufen vor.

Eine Gefährdungs- und Risikoanalyse sollte die Gefährdungen und gefährlichen Ereignisse herausfinden und behandeln, die unter allen vorhersehbaren Umständen vorkommen können (einschließlich Fehlerbedingungen und vernünftigerweise vorhersehbarer Fehlanwendung).

Bei einem typischen Projekt der Prozessindustrie muss eine vorläufige Gefährdungs- und Risikoanalyse frühzeitig während der verfahrenstechnischen Grundplanung durchgeführt werden. Voraussetzung zu diesem Zeitpunkt ist, dass durch Anwendung des Prinzips der Eigensicherheit und der guten Ingenieurpraxis Gefährdungen ausgeräumt oder so weit wie möglich reduziert wurden (dies liegt nicht innerhalb des Anwendungsbereichs der IEC 61511). Für das SIS ist diese vorläufige Gefährdungs- und Risikoanalyse bedeutsam, da die Festlegung, Planung und Implementierung eines SIS komplexe Aufgaben darstellen und eine erhebliche Zeit in Anspruch nehmen können. Ein anderer Grund, warum diese Arbeit frühzeitig erledigt werden sollte, ist, dass die Information über die Systemarchitektur vorliegen muss, bevor die R&I-Schemata abgeschlossen werden können. Im Normalfall liegt genügend Information zur Durchführung der vorläufigen Gefährdungs- und Risikoanalyse vor, sobald ein vollständiges Verfahrensbild vorliegt und die ersten Verfahrensdaten verfügbar sind. Es sollte beachtet werden, dass zusätzliche Gefährdungen im Verlauf der Detailplanung entstehen können. Deshalb kann eine abschließende Gefährdungs- und Risikoanalyse nach Fertigstellung des R&I-Schemas erforderlich sein. Für diese abschließende Analyse wird üblicherweise eine formale und bis ins Einzelne dokumentierte Verfahrensweise wie beispielsweise die HAZOP-Methode verwendet. Sie sollte bestätigen, dass die in der Planung vorgesehenen Schutzebenen die Sicherheit der Anlage sicherstellen können. Während dieser abschließenden Analyse ist zu berücksichtigen, ob durch Ausfälle in den Sicherheitssystemen neue Gefährdungen oder Anforderungen entstehen können. Wenn zu diesem Zeitpunkt neue Gefährdungen erkannt werden, kann es notwendig werden, neue Sicherheitsfunktionen festzulegen. Wahrscheinlicher ist es jedoch, dass zusätzliche Ereignisse identifiziert werden, die zu Gefährdungen führen, die bereits in der vorläufigen Analyse erkannt wurden. In diesem Fall ist es erforderlich, über notwendige Veränderungen der Sicherheitsfunktionen und deren Leistungsanforderungen, die in der ursprünglichen Analyse festgelegt wurden, nachzudenken.

Die zur Identifizierung von Gefährdungen angewendete Vorgehensweise hängt von der betrachteten Anwendung ab. Bei bestimmten einfachen Prozessen, für die breite Anwendungserfahrungen zu einer Standardlösung vorliegen, beispielsweise einfache Bohrplattformen, kann die Anwendung in der Industrie entwickelter Checklisten ausreichen (beispielsweise die Checkliste zur Sicherheitsanalyse in ISO 10418 und in API RC 14C). Im Falle komplexerer Entwürfe oder neuer Prozesse kann eine strukturiertere Vorgehensweise notwendig sein (beispielsweise IEC 60300-3-9:1995).

ANMERKUNG Weiterführende Informationen zur Auswahl geeigneter Techniken sind in ISO 17776 enthalten.

Bei der Betrachtung der Konsequenzen eines bestimmten Ausfallereignisses sollten alle möglichen Folgen berücksichtigt werden und die Häufigkeit des Ausfallereignisses den möglichen Folgen gegenübergestellt werden. Keine denkbare Folge sollte vernachlässigt oder von der Risikoanalyse ausgeschlossen werden. Die Beanspruchung von Rohrleitungen oder Apparaten mit Drücken oberhalb des Auslegungsdrucks hat nicht in allen Fällen einen völligen Produktaustritt zur Folge. In vielen Fällen war ein Gerät Prüfdrücken oberhalb des Auslegungsdrucks ausgesetzt und die einzige Auswirkung war eine Leckage brennbarer Stoffe mit einer möglichen Entzündung. Bei der Ermittlung der Auswirkungen sind die für die mechanische Integrität der

Anlage Verantwortlichen hinzuzuziehen. Diese müssen den ursprünglichen Prüfdruck berücksichtigen, aber auch, ob die ursprüngliche Planung Korrosion berücksichtigte und ob ein Managementprogramm hinsichtlich der Korrosion existiert. Wenn solche Annahmen Grundlage für die Ermittlung der Auswirkungen sind, ist es wichtig, dies klar festzuhalten, so dass entsprechende Vorgehensweisen im Sicherheitsmanagementsystem integriert werden können. Ein weiterer Gesichtspunkt bei der Berücksichtigung der Auswirkungen ist die Anzahl der Personen, die wahrscheinlich von einer bestimmten Gefährdung betroffen sein werden. In vielen Fällen wird Betriebs- und Instandhaltungspersonal nicht häufig im gefährdeten Bereich anwesend sein, was bei der Voraussage der Auswirkungen berücksichtigt werden sollte. Bei diesem statistischen Ansatz ist Sorgfalt erforderlich, denn er wird nicht in allen Fällen gültig sein, beispielsweise wenn die Gefährdung nur während der Anfahrphase auftritt und hierbei das Personal ständig anwesend ist. Ebenso sollte man die möglicherweise erhöhte Anzahl an Menschen in der Nähe des gefährlichen Ereignisses berücksichtigen, die die Gründe während seines Entstehens untersuchen.

Bei der Beurteilung der möglichen Ursachen für eine Anforderung des SIS sollten die folgenden Situationen berücksichtigt werden: Anfahren, Dauerbetrieb, Abfahren, Instandhaltungsfehler, Bedienereingriffe (beispielsweise Regler auf „Hand“), Ausfall von Hilfsenergien (beispielsweise Druckluft, Kühlwasser, Stickstoff, elektrische Energie, Dampf, Begleitheizung).

Bei der Betrachtung der Anforderungshäufigkeit kann es in schwierigen Fällen notwendig sein, eine Fehlerbaumanalyse durchzuführen. Dies ist oft dann erforderlich, wenn schwerwiegende Auswirkungen als Folge gleichzeitiger Ereignisse auftreten (beispielsweise wenn Spannungssammelleitungen nicht für den „worst case“-Fall einer Entspannung aller angeschlossenen Leitungen ausgelegt sind). Eine Abschätzung ist erforderlich, ob Fehler des Bedienungspersonals in die Liste der Ereignisse, die eine Gefährdung verursachen können, aufgenommen werden müssen, sowie die anzusetzende Häufigkeit solcher Ereignisse. Ein Fehler des Bedienungspersonals kann als Anforderung in vielen Fällen dann ausgeschlossen werden, wenn eine Handlung einem Genehmigungsverfahren unterliegt oder Verriegelungsmechanismen vorgesehen sind, die eine unabsichtliche Handlung verhindern. In Fällen, in denen die Anforderungshäufigkeit mit Hilfe einer Handlung des Bedienungspersonals reduziert wird, ist ebenso Sorgfalt erforderlich. In welchem Maße dies berücksichtigt werden kann, hängt davon ab, wie schnell die erforderliche Handlung durchgeführt werden muss und wie komplex die erforderlichen Aufgaben sind. Wenn ein Operator eine Handlung infolge eines Alarms durchführen soll und die angenommene Risikoverminderung größer als 10 ist, ist die Auslegung des Gesamtsystems entsprechend IEC 61511-1 erforderlich. Das System, das die Sicherheitsfunktion ausführt, würde in diesem Falle aus dem Sensor, der die gefährliche Bedingung feststellt, der Darstellung des Alarms, dem Bedieneingriff und der vom Operator verwendeten Einrichtung zur Unterbindung der Gefährdung bestehen. Es bleibt anzumerken, dass eine Risikoverminderung um einen Faktor kleiner als 10 angenommen werden kann, ohne dass gemäß IEC 61511 vorgegangen werden muss. Im Falle solcher Annahmen sollte man die Gesichtspunkte menschlichen Handelns sorgfältig berücksichtigen. Bei jeder Inanspruchnahme eines Alarms für eine Risikoreduzierung sollte die erforderliche Antwort auf den Alarm beschrieben und dokumentiert werden und dass ausreichend Zeit für den Bediener zur Durchführung des erforderlichen Eingriffs zur Verfügung steht und dass der Bediener für die erforderlichen Eingriffe ausgebildet ist.

Ein Alarmierungssystem, das die Anforderungsrate des SIS vermindert, kann unter folgenden Voraussetzungen als eine Möglichkeit zur Risikoreduzierung verwendet werden:

- der im Alarmierungssystem verwendete Sensor wird nicht gleichzeitig für Regelungsaufgaben verwendet, deren Ausfall zu einer Anforderung der sicherheitstechnischen Funktion führen würde;
- der im Alarmierungssystem verwendete Sensor wird nicht im SIS verwendet;
- Beschränkungen hinsichtlich der Risikoreduzierung, die für ein BPCS angesetzt werden können, und die Thematik der Ausfälle gemeinsamer Ursache wurden berücksichtigt.

Beispiele für Vorgehensweisen, die zur Festlegung des SIL sicherheitstechnischer Systeme verwendet werden können, sind in IEC 61511-3 aufgeführt. Dort sind auch Anleitungen enthalten, was bei der Auswahl einer Methode für eine bestimmte Anwendung berücksichtigt werden sollte.

Bei der Festlegung, ob eine Risikoreduzierung erforderlich ist, werden Ziele für die Prozesssicherheit und die Umwelt benötigt. Diese können für einen bestimmten Standort oder für ein Unternehmen festgelegt sein und werden mit dem Risiko ohne zusätzliche Sicherheitsfunktionen verglichen. Nach Festlegung einer erforderlichen Risikoverminderung ist eine Betrachtung erforderlich, welche Funktionen ausgeführt werden müssen, um den Prozess in einen sicheren Zustand zu bringen. Die Funktionen können theoretisch in allgemeiner Weise ohne Bezug zu einer bestimmten Technologie beschrieben werden. Beispielsweise kann

im Fall eines Schutzes vor einem Überdruck die Funktion als Vermeidung eines Druckanstiegs über einen festgelegten Wert beschrieben werden. Diese Funktion könnte dann entweder mit Hilfe eines Überdruckventils oder eines sicherheitstechnischen Systems ausgeführt werden. Wenn die Funktion in der oben beschriebenen Art und Weise definiert ist, würde über die Auswahl der Technologie im nächsten Schritt des Lebenszyklus entschieden werden (Zuordnung sicherheitstechnischer Funktionen zu Schutzebenen). In der Praxis würden die funktionalen Anforderungen vom Typ des ausgewählten Systems abhängen und dieser und der nächste Schritt können in manchen Fällen zusammengefasst werden.

Zusammenfassend sollte die Gefährdungs- und Risikoanalyse Folgendes berücksichtigen:

- jedes ermittelte gefährliche Ereignis und die Ereignisketten, die dazu beitragen;
- die Auswirkungen und Wahrscheinlichkeiten der Ereignisketten, die zu jedem gefährlichen Ereignis gehören; diese können in quantitativer oder qualitativer Form ausgedrückt werden;
- die erforderliche Risikoreduzierung für jedes gefährliche Ereignis;
- die getroffenen Maßnahmen zur Reduzierung oder Ausräumung von Gefährdungen und Risiken;
- die während der Risikoanalyse getroffenen Annahmen, einschließlich der geschätzten Anforderungsraten und Ausfallraten von Einrichtungen; Erleichterungen aufgrund betrieblicher Gründe oder Bedienereingriffe sollten genau angegeben werden;
- Verweise auf grundlegende Informationen zu den sicherheitsbezogenen Systemen für jede Phase des Lebenszyklus (beispielsweise Tätigkeiten im Rahmen der Verifizierung und Validierung).

Die Informationen und Ergebnisse der Risikoanalyse sollten dokumentiert werden.

Möglicherweise ist es erforderlich, die Gefährdungs- und Risikoanalyse in unterschiedlichen Phasen des SIS-Sicherheitslebenszyklus zu wiederholen, wenn Entscheidungen getroffen werden oder vorhandene Informationen deutlicher werden.

8.2.2 In der Prozessindustrie ist ein wichtiger zu berücksichtigender Grund für Anforderungen in vielen Anwendungen ein Ausfall des BPCS. Es soll angemerkt werden, dass ein Ausfall des BPCS durch den Sensor, das Stellglied oder das Leitsystem verursacht werden kann.

In manchen Fällen haben in der Prozessindustrie verwendete Leitsysteme redundante Prozessoren, Sensoren und Stellglieder sind dagegen üblicherweise nicht redundant. Wenn man dem BPCS eine Ausfallrate zuordnet, ist eine wichtige Grenze zu berücksichtigen. Die IEC 61511-1 begrenzt die Rate für gefährliche Ausfälle im Zusammenhang mit einer bestimmten Gefährdung, die in Anspruch genommen werden kann, auf 10^{-5} pro Stunde, wenn das System nicht entsprechend den Anforderungen dieser Norm ausgelegt worden ist. Der Grund für diese Begrenzung ist, dass niedrigere Raten für gefährliche Ausfälle im Bereich der in Tabelle 4 angegebenen Ausfallraten liegen würden. Die Begrenzung stellt sicher, dass nicht ein hohes Vertrauen auf Systeme gesetzt wird, die die Anforderungen der IEC 61511-1 nicht erfüllen.

8.2.3 Keine weitergehende Anleitung vorgesehen.

9 Zuordnung der Sicherheitsfunktionen zu den Schutzebenen

9.1 Ziel

Es ist wichtig, bei der Festlegung der Notwendigkeit für ein SIS und seines zugeordneten SIL zu berücksichtigen, welche anderen Schutzebenen vorhanden sind (oder benötigt werden) und welchen Schutz sie bieten. Nach Berücksichtigung der anderen Schutzebenen sollte dann der Bedarf für eine SIS-Schutzebene festgestellt werden. Wenn eine SIS-Schutzebene benötigt wird, sollte dann der SIL für die sicherheitstechnische(n) Funktion(en) dieses SIS bestimmt werden.

9.2 Anforderungen an den Prozess der Zuordnung

9.2.1 Die in diesem Abschnitt enthaltene Anforderung sieht eine Übereinkunft über die zu verwendenden Schutzebenen und die Zuordnung von Zielwerten für die Leistungsfähigkeit der sicherheitstechnischen Funktionen vor. In der Praxis werden Sicherheitsfunktionen in vielen Fällen nur dann sicherheitstechnischen