

	DIN EN IEC 63044-4 (VDE 0849-44-4)	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 „etx Elektrotechnik + Automation“ bekannt gegeben worden.	VDE

ICS 97.120

Einsprüche bis 2020-07-01

Entwurf

Vorgesehen als Ersatz für
DIN EN 50491-4-1
(VDE 0849-4-1):2012-11

**Allgemeine Anforderungen an die Elektrische Systemtechnik für Heim und Gebäude (ESHG) und an Systeme der Gebäudeautomation (GA) –
Teil 4: Anforderungen an die funktionale Sicherheit für Produkte, die für
den Einbau in ESHG/GA vorgesehen sind
(IEC 23/862/CD:2019);
Text Deutsch und Englisch**

General requirements for Home and Building Electronic Systems (HBES) and Building Automation and Control Systems (BACS) –
Part 4: General functional safety requirements for products intended to be integrated in Building Electronic Systems (HBES) and Building Automation and Control Systems (BACS) (IEC 23/862/CD:2019);
Text in German and English

Anwendungswarnvermerk

Dieser Norm-Entwurf mit Erscheinungsdatum 2020-05-01 wird der Öffentlichkeit zur Prüfung und Stellungnahme vorgelegt.

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

Stellungnahmen werden erbeten

- vorzugsweise online im Norm-Entwurfs-Portal von DIN unter www.din.de/go/entwuerfe bzw. für Norm-Entwürfe der DKE auch im Norm-Entwurfs-Portal der DKE unter www.entwuerfe.normenbibliothek.de, sofern dort wiedergegeben;
- oder als Datei per E-Mail an dke@vde.com möglichst in Form einer Tabelle. Die Vorlage dieser Tabelle kann im Internet unter www.din.de/go/stellungnahmen-norm-entwuerfe oder für Stellungnahmen zu Norm-Entwürfen der DKE unter www.dke.de/stellungnahme abgerufen werden;
- oder in Papierform an die DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE, Stresemannallee 15, 60596 Frankfurt am Main.

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

Gesamtumfang 55 Seiten

DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE

Anwendungsbeginn

Anwendungsbeginn dieser Norm ist

Nationales Vorwort

Das internationale Dokument IEC 23/862/CD:2019-09 "General requirements for Home and Building Electronic Systems (HBES) and Building Automation and Control Systems (BACS) – Part 4: General functional safety requirements for products intended to be integrated in Building Electronic Systems (HBES) and Building Automation and Control Systems (BACS)" (CD, en: Committee Draft) ist unverändert in diesen Norm-Entwurf übernommen worden. Dieser Norm-Entwurf enthält eine noch nicht autorisierte deutsche Übersetzung.

Um Zweifelsfälle in der Übersetzung auszuschließen, ist die englische Originalfassung des CD 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 IEC/TC 23 "Electrical accessories" der Internationalen Elektrotechnischen Kommission (IEC) erarbeitet und den nationalen Komitees zur Stellungnahme vorgelegt.

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. Dokumente, die bei CENELEC als Europäische Norm angenommen und ratifiziert werden, sind unverändert als Deutsche Normen zu übernehmen.

Da der Abstimmungszeitraum für einen FDIS bzw. Schluss-Entwurf FprEN nur 6 Wochen beträgt, und dann keine sachlichen Stellungnahmen mehr abgegeben werden können, sondern nur noch eine "JA/NEIN"-Entscheidung möglich ist, wobei eine "NEIN"-Entscheidung fundiert begründet werden muss, wird bereits der CD als DIN-Norm-Entwurf veröffentlicht, um die Stellungnahmen aus der Öffentlichkeit frühzeitig berücksichtigen zu können.

Für dieses Dokument ist das nationale Arbeitsgremium DKE/K 716 "Elektrische Systemtechnik für Heim und Gebäude (ESHG)" der DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE (www.dke.de) zuständig.

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

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

Der Zusammenhang der zitierten Dokumente mit den entsprechenden deutschen Dokumenten ergibt sich, soweit ein Zusammenhang besteht, grundsätzlich über die Nummer der entsprechenden IEC-Publikation. Beispiel: IEC 60068 ist als EN 60068 als Europäische Norm durch CENELEC übernommen und als DIN EN 60068 ins Deutsche Normenwerk aufgenommen.

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können. IEC ist nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren.

Das Original-Dokument enthält Bilder in Farbe, die in der Papierversion in einer Graustufen-Darstellung wiedergegeben werden. Elektronische Versionen dieses Dokuments enthalten die Bilder in der originalen Farbdarstellung.

Änderungen

Gegenüber **DIN EN 50491-4-1 (VDE 0849-4-1):2012-11** wurden folgende Änderungen vorgenommen:

- a) Die **DIN EN 50491-4-1 (VDE 0849-4-1):2012-11** wurde unverändert übernommen.

Inhalt

Seite

Einleitung	4
1 Anwendungsbereich	5
2 Normative Verweisungen	5
3 Begriffe	5
4 Allgemeine Anforderungen	8
4.1 Allgemeines	8
4.2 Methode der Erstellung der Anforderungen	8
4.2.1 Allgemeines	8
4.2.2 ESHG/GA-Anwendungsumfeld	9
4.2.3 Gefahrenquellen	9
4.2.4 Gefährliche Vorfälle	9
4.2.5 Ableitung von Anforderungen	10
5 Anforderungen an die funktionale Sicherheit	10
5.1 Allgemeines	10
5.2 Spannungsversorgung	10
5.3 Umgebung	11
5.4 Lebensdauer	11
5.5 Vernünftigerweise vorhersehbare Fehlanwendung	11
5.6 Software und Kommunikation	12
5.7 Fernbedienung	13
5.7.1 Allgemeine Empfehlungen	13
5.7.2 Innerhalb eines einzelnen Gebäudes oder in seiner unmittelbaren Umgebung	13
5.7.3 Von außerhalb des Gebäudes	14
5.7.4 Management	14
Anhang A (informativ) Beispiel für eine Methode zur Bestimmung der Sicherheits-Integritätslevel	16
A.1 Allgemeines	16
A.2 Begriffe	16
A.3 Das Konzept „So niedrig wie vernünftigerweise möglich“ (ALARP) und Konzepte für tolerierbares Risiko	17
Anhang B (informativ) Gefährdungen und Definitionsprozess notwendiger Anforderungen an die funktionale Sicherheit	18
Anhang C (informativ) Beispiele für einige nicht sicherheitsbezogene Anwendungen für ESHG/GA-Systeme	29
C.1 Beispiele für nicht sicherheitsbezogene Anwendungen für ESHG/GA-Systeme	29
C.1.1 Allgemeines	29
C.1.2 Beispiel 1: Backofen	29
C.1.3 Beispiel 2: Produkte, die ein hohes potenzielles Gefährdungsrisiko darstellen	29
C.1.4 Beispiel 3: Netzstecker, Steckdosen und Stromkreise	30
C.1.5 Beispiel 4: Einstellung der Wassertemperatur	30
Literaturhinweise	31

Bilder

Bild A.1 – Risikominderung – Allgemeines Konzept	16
--	----

Tabellen

Tabelle 1 – Anforderungen zur Vermeidung unbeabsichtigter Arbeitsgänge und mögliche Vorgehensweisen zu deren Erfüllung	15
Tabelle A.1 – Beispiel der Risikoklassifikation von Unfällen	17
Tabelle A.2 – Interpretation von Risikoklassen	17
Tabelle B.1 – Anforderungen/Risikominderungsmaßnahmen	18

Einleitung

ESHG/GA-Produkte, die in ein ESHG/GA-System integriert sind, sollten für den Gebrauch in den vorgesehenen Anwendungen sicher sein.

Diese Norm richtet sich nach Prinzipien der Grundnorm für funktionale Sicherheit, IEC 61508.

Diese Norm identifiziert Themen der funktionalen Sicherheit von Produkten und ihrer Installation. Den Anforderungen liegt eine Risikoanalyse in Übereinstimmung mit IEC 61508 zugrunde.

Das Ziel dieser Norm ist es, ESHG/GA-Produkten, soweit möglich, alle Sicherheitsanforderungen im Produkt-Lebenszyklus zuzuordnen.

Diese Norm wendet sich an Komitees, die ESHG/GA-Produkt-/Systemnormen erarbeiten und pflegen oder, falls keine geeignete ESHG/GA-Produktnorm für die funktionale Sicherheit verfügbar ist, an die Produkthersteller.

Die ESHG/GA-Produkte in dieser Norm sind für nicht sicherheitsbezogene Anwendungen vorgesehen.

Allgemeine Anforderungen an die Elektrische Systemtechnik für Heim und Gebäude (ESHG) und an Systeme der Gebäudeautomation (GA) – Teil 4: Anforderungen an die funktionale Sicherheit für Produkte, die für den Einbau in ESHG/GA vorgesehen sind

Allgemeine Anforderungen an die Elektrische Systemtechnik für Heim und Gebäude (ESHG) und an Systeme der Gebäudeautomation (GA) – Teil 4: Anforderungen an die funktionale Sicherheit für Produkte, die für den Einbau in ESHG/GA vorgesehen sind

1 Anwendungsbereich

Dieser Teil von IEC 63044 legt die Anforderungen an die funktionale Sicherheit von ESHG/GA fest.

Darüber hinaus werden Anforderungen an die funktionale Sicherheit von Schnittstellen von Betriebsmitteln, die für einen Anschluss an ein ESHG/GA-Netzwerk vorgesehen sind, festgelegt. Dieser Teil gilt nicht für Schnittstellen zu anderen Netzwerken.

ANMERKUNG Ein Beispiel für ein anderes Netzwerk ist ein zweckbestimmtes Netzwerk der Informations- und Kommunikationstechnik nach IEC 62949.

Diese Norm beschreibt keine Anforderungen an die funktionale Sicherheit von sicherheitsbezogenen Systemen.

Diese Norm beschreibt keine Anforderungen an Datenschutz und -sicherheit.

2 Normative Verweisungen

Die folgenden Dokumente werden im Text in solcher Weise in Bezug genommen, dass einige Teile davon oder ihr gesamter Inhalt Anforderungen des vorliegenden Dokuments darstellen. 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 63044-2, *General requirements for Home and Building Electronic Systems (HBES) and Building Automation and Control Systems (BACS) - Part 2: Environmental conditions*

IEC 63044-3, *General requirements for Home and Building Electronic Systems (HBES) and Building Automation and Control Systems (BACS) - Part 3: Electrical safety requirements*

IEC 63044-5 (alle Teile), *General requirements for Home and Building Electronic Systems (HBES) and Building Automation and Control Systems (BACS)*

IEC 61508 (alle Teile), *Functional safety of electrical/electronic/programmable electronic safety-related systems*

IEC 61709:1998, *Electronic components - Reliability - Reference conditions for failure rates and stress models for conversion (IEC 61709:1996)*

ISO 9000, *Quality management systems - Fundamentals and vocabulary (ISO 9000)*

3 Begriffe

Für die Anwendung dieses Dokuments gelten die folgenden Begriffe.

3.2

Authentisierung

(en: authentication)

Methode zur Beglaubigung, dass der Teilnehmer, der eine Nachricht sendet, der ist, der er vorgibt zu sein, und Bestätigung, dass die Nachricht identisch ist mit dem, das gesendet wurde

3.3

Autorisierung

(en: authorisation)

Methode zur Sicherstellung, dass Produkte oder Personen, die auf Informationen, Funktionen oder Services zugreifen, auch die Berechtigung dazu haben

3.4

gestörte Kommunikation

(en: **disturbed communication**)

Kommunikation, bei der aus irgendeinem Grund eine übertragene Nachricht unvollständig, verkürzt oder fehlerhaft ist oder bei korrektem Format Informationen liefert, die außerhalb des Bereichs der erwarteten Parameter für eine solche Nachricht liegen

3.5

funktionale Sicherheit

(en: **functional safety**)

Sicherheit vor nicht akzeptablem Schadensrisiko infolge des Betriebs eines ESHG/GA, einschließlich des Risikos infolge

- 1) normalen Betriebs,
- 2) vernünftigerweise vorhersehbarer Fehlanwendung,
- 3) Fehler, Ausfall,
- 4) zeitlich begrenzter Störungen.

Anmerkung 1 zum Begriff: Funktionale Sicherheit: Teil der Gesamtsicherheit, bezogen auf die EUC und das EUC-Leit- oder Steuerungssystem, der von der korrekten Funktion des sicherheitsbezogenen E/E/PE-Systems und anderer risikomindernder Maßnahmen abhängt [QUELLE: IEC 61508-4:2010, Begriff 3.1.12]

Anmerkung 2 zum Begriff: Die Definitionen nach IEC/TR 61000-2-1 und IEC/TS 61000-1-2 (IEC/TC 77) wurden berücksichtigt.

3.6

Hamming-Distanz

(en: **Hamming distance**)

Anzahl der Bits, in denen sich zwei Binärcodes unterscheiden

3.7

Schaden

(en: **harm**)

physische Verletzung oder Schädigung der Gesundheit von Menschen, entweder direkt oder indirekt als ein Ergebnis von Schäden an Gütern oder der Umwelt

Anmerkung 1 zum Begriff: Schaden: physische Verletzung oder Schädigung der Gesundheit von Menschen oder Schädigung von Gütern oder der Umwelt [QUELLE: IEC 61508-4:2010, 3.1.1]

3.8

Gefährdung

(en: **hazard**)

potenzielle Schadensquelle

[QUELLE: ISO/IEC Guide 51:1999, Begriff 3.5]

[QUELLE: IEC 61508-4:2010, Begriff 3.1.2]

Anmerkung 1 zum Begriff: Der Begriff schließt Gefährdungen von Personen ein, die innerhalb einer kurzen Zeitspanne entstehen (zum Beispiel durch Feuer und Explosion), und auch solche, die eine Langzeitwirkung auf die Gesundheit einer Person haben (zum Beispiel durch Freisetzung einer giftigen Substanz).

3.9

gefährlicher Vorfall

(en: **hazardous event**)

Situation, die im normalen Betrieb oder unter außergewöhnlichen Bedingungen zu einem Schaden führt

Anmerkung 1 zum Begriff: Ob ein gefährlicher Vorfall zu einem Schaden führt, hängt davon ab, ob Personen, Güter oder die Umwelt den Auswirkungen des gefährlichen Vorfalls ausgesetzt sind, und im Fall von Schaden von Personen, ob irgendeine derart ausgesetzte Person den Auswirkungen des Vorfalls ausweichen kann, nachdem dieser aufgetreten ist.

Anmerkung 2 zum Begriff: Angepasst aus IEC 61508-4:2010, Begriff 3.1.4.

3.12

Produkt (en: product)

Gerät in Form von Hardware, Firmware, die zugehörige Software und Konfigurations-Werkzeuge

3.13

Produktdokumentation

(en: product documentation)

vom Hersteller zur Verfügung gestelltes Informationsmaterial zur Installation und zum Betrieb als Katalog oder Broschüre des Herstellers oder als andere gedruckte oder elektronische Produktinformation

3.14

sicherheitsbezogenes System

(en: safety related system)

System, das sowohl

- die erforderlichen Sicherheitsfunktionen ausführt, die notwendig sind, um einen sicheren Zustand für die EUC zu erreichen oder aufrechtzuerhalten, als auch
- dazu vorgesehen ist, selbst oder mit anderen sicherheitsbezogenen E/E/PE-Systemen und anderen risikomindernden Maßnahmen die notwendige Sicherheitsintegrität für die geforderten Sicherheitsfunktionen zu erreichen

Anmerkung 1 zum Begriff: Der Begriff bezieht sich auf jene Systeme, die als sicherheitsbezogene Systeme bezeichnet werden und die zusammen mit den anderen risikomindernden Maßnahmen dazu vorgesehen sind, die notwendige Risikominderung zu erreichen, um das geforderte tolerierbare Risiko zu erreichen.

Anmerkung 2 zum Begriff: Sicherheitsbezogene Systeme werden entworfen, um die EUC am Übergang in einen gefahrbringenden Zustand zu hindern, indem nach Erkennen eines Zustandes, der zu einem gefährlichen Vorfall führen kann, eine angemessene Aktion eingeleitet wird. Der Ausfall eines sicherheitsbezogenen Systems würde demnach zu den Ereignissen hinzugerechnet, die zu den festgestellten Gefährdungen führen. Obwohl es andere Systeme mit Sicherheitsfunktionen geben kann, sind es die sicherheitsbezogenen Systeme, die dazu bestimmt worden sind, das geforderte tolerierbare Risiko zu erreichen. Sicherheitsbezogene Systeme können allgemein in sicherheitsbezogene Leit- oder Steuerungssysteme und sicherheitsbezogene Schutzsysteme eingeteilt werden.

Anmerkung 3 zum Begriff: Die sicherheitsbezogenen Systeme dürfen Bestandteil des EUC-Leit- oder Steuerungssystems oder durch Sensoren und/oder Aktoren mit der EUC verbunden sein. Das heißt, der erforderliche Sicherheits-Integritätslevel darf durch in dem EUC-Leit- oder Steuerungssystem realisierte Sicherheitsfunktionen (und möglicherweise auch durch zusätzliche getrennte und unabhängige Systeme) erreicht werden, oder die Sicherheitsfunktionen dürfen von getrennten und unabhängigen Systemen durchgeführt werden, die der Sicherheit zugeordnet sind.

Anmerkung 4 zum Begriff: Ein sicherheitsbezogenes System darf:

- a) dazu entworfen sein, den gefährlichen Vorfall zu vermeiden (d. h., falls das sicherheitsbezogene System seine Sicherheitsfunktionen ausführt, entsteht kein Schadensereignis);
- b) dazu entworfen sein, die Auswirkungen des Schadensereignisses zu mildern, so dass durch Reduzierung der Auswirkungen das Risiko reduziert wird;
- c) dazu entworfen sein, eine Kombination von a) und b) zu erreichen.

Anmerkung 5 zum Begriff: Eine Person kann Teil eines sicherheitsbezogenen Systems sein. Zum Beispiel könnte eine Person eine Information von einem programmierbaren elektronischen Gerät erhalten und aufgrund dieser eine Sicherheitshandlung oder eine Sicherheitshandlung über ein programmierbares elektronisches Gerät ausführen.

Anmerkung 6 zum Begriff: Ein sicherheitsbezogenes System schließt alle Hardware, Software und Versorgungseinrichtungen (z. B. Stromversorgung) ein, die notwendig sind, die angegebene Sicherheitsfunktion auszuführen (Sensoren, andere Eingabeeinrichtungen, Stellglieder (Aktoren) und andere Ausgabeeinrichtungen sind deshalb im sicherheitsbezogenen System eingeschlossen).

Anmerkung 7 zum Begriff: Ein sicherheitsbezogenes System darf auf einem breiten Bereich, der elektrische, elektronische, programmierbar elektronische, hydraulische und pneumatische Technologien umfasst, basieren.

[QUELLE: IEC 61508-4:2010, Begriff 3.4.1]

3.15

Risiko

(en: risk)

Kombination aus der Wahrscheinlichkeit, mit der ein Schaden auftritt, und dem Ausmaß dieses Schadens

Anmerkung 1 zum Begriff: Für die weitere Diskussion dieses Begriffs siehe IEC 61508-5:2010, Anhang A.

[QUELLE: IEC 61508-4:2010, Begriff 3.1.6]

3.16

vernünftigerweise vorhersehbare Fehlanwendung

(en: **reasonably foreseeable misuse**)

Verwendung eines Produktes, Verfahrens oder einer Dienstleistung in einer Art, die von einem Lieferanten nicht vorgesehen ist, die sich jedoch aus leicht vorhersehbaren menschlichen Verhaltensweisen ergeben kann

[QUELLE: IEC 61508-4:2010, Begriff 3.1.14, ISO/IEC Guide 51:1999, Begriff 3.14]

3.17

Sicherheitsfunktion

(en: **safety function**)

Funktion, die von einem sicherheitsbezogenen E/E/PE-System oder anderen risikomindernden Maßnahmen ausgeführt wird und dazu vorgesehen ist, unter Berücksichtigung eines festgelegten gefährlichen Vorfalls einen sicheren Zustand für die EUC zu erreichen oder aufrechtzuerhalten

Beispiele für Sicherheitsfunktionen sind:

- Funktionen, die erforderlich sind, als positive Handlungen durchgeführt zu werden, um Gefährdungssituationen zu vermeiden (z. B. Ausschalten eines Motors), und
- Funktionen, die verhindern, dass Handlungen ausgeführt werden (z. B. Verhinderung des Anlaufens eines Motors).

[QUELLE: IEC 61508-4:2010, Begriff 3.5.1]

3.18

EUC

Equipment Under Control

[QUELLE: IEC 61508-4:2010, Tabelle 1]

4 Allgemeine Anforderungen

4.1 Allgemeines

Die funktionale Sicherheit eines Systems hängt von der Leistungsfähigkeit sowohl des Netzwerks als auch der angeschlossenen ESHG/GA-Produkte ab:

- 1) Fehler im Netzwerk oder in irgendeinem anderen Teil des ESHG/GA-Systems dürfen nicht dazu führen, dass das System, die Produkte oder die überwachten Geräte unsicher werden.
- 2) Während des Betriebs dürfen sich die einzelnen ESHG/GA-Produkte für ihren sicheren Betrieb nicht allein auf das System verlassen.
- 3) Während des Betriebs darf die Wechselwirkung beliebiger Produkte untereinander nicht zu einem unsicheren Betrieb des Systems führen.

4.2 Methode der Erstellung der Anforderungen

4.2.1 Allgemeines

Für die Festlegung der Anforderungen an die funktionale Sicherheit wurde für die folgenden Aspekte dem Lebenszyklus nach IEC 61508 gefolgt:

- 1) Konzeptphase für das Produkt;
- 2) Anwendungsumfeld;
- 3) Identifizierung der Gefährdungen und der gefährlichen Vorfälle;
- 4) Gefährdungs- und Risikoanalyse, Maßnahmen zur Risikominderung;
- 5) Umsetzung der Maßnahmen zur Risikominderung;
- 6) Validierung;
- 7) Instandhaltung;
- 8) Installation und Inbetriebnahme;
- 9) Außerbetriebsetzung.

Die Technischen Komitees für Produkte bzw. die Produktentwickler müssen die Anforderungen dieser Norm in den Sicherheitsanforderungen ihrer Produkte berücksichtigen, aber es ist nicht notwendig, sich mit dem Verfahren in IEC 61508 selbst zu befassen.

4.2.2 ESHG/GA-Anwendungsumfeld

Das Anwendungsumfeld für ESHG/GA-Systeme wurde berücksichtigt.

4.2.3 Gefahrenquellen

Die im Folgenden aufgeführten Gefahrenquellen wurden berücksichtigt:

- 1) Material und Konstruktion;
- 2) Zuverlässigkeit;
- 3) normaler Betrieb;
- 4) unbeabsichtigte Wechselwirkung mit anderen Produkten;
- 5) Wechselwirkung mit anderen ESHG/GA-Produkten;
- 6) Betrieb unter außergewöhnlichen Bedingungen;
- 7) vorhersehbare Fehlanwendung einschließlich Laden von unzulässigen und bösartigen Codes;

ANMERKUNG Dies schließt unbeabsichtigte Softwareänderungen ein.

- 8) Lebensdauer;
- 9) Umwelt;
- 10) Installation und Instandhaltung.

4.2.4 Gefährliche Vorfälle

Die im Folgenden aufgeführten gefährlichen Vorfälle wurden in der Analyse berücksichtigt (das Bus- und Stromnetz (230 V/400 V) wurden berücksichtigt):

- 1) Ausfall des Stromnetzes;
- 2) Kurzschluss einer Buslinie;
- 3) Überspannungen auf dem Bus;
- 4) Überspannungen im Stromnetz;
- 5) Beschädigung der Isolierung (z. B. Temperatur, Spannungsstoß, mechanisch);
- 6) falsche Verdrahtung, Verbindung;
- 7) Übertemperatur;
- 8) Feuer;
- 9) mechanischer Stoß, Vibrationen;
- 10) Korrosion;
- 11) elektromagnetische Störungen;
- 12) gestörte Kommunikation;
- 13) Verschmutzung;
- 14) Lebensdauerende von Komponenten bzw. Produkten;
- 15) vernünftigerweise vorhersehbare Fehlanwendung;
- 16) Softwarefehler;
- 17) Überlast;
- 18) Verlust von Zuverlässigkeit;
- 19) (mechanischer) Materialbruch;
- 20) ungeeignete Gestaltung/Konstruktion;
- 21) Schalten von beschädigten Produkten und Subsystemen;

- 22) Fernwirken, Fernsteuerung;
- 23) Befehle von zwei Quellen an ein Produkt (z. B. Aktor);
- 24) Systemausfälle.

4.2.5 Ableitung von Anforderungen

Die Risikoanalyse wurde für jedes der gefährlichen Vorfälle ausgeführt, siehe [Anhang B](#). Die Wahrscheinlichkeit für das Auftreten eines Vorfalls wurde abgeschätzt und die Risikoklasse wurde entsprechend dem in [Anhang A](#) beschriebenen Verfahren berücksichtigt.

In allen Fällen, in denen die abgeschätzte Risikoklasse ein nicht akzeptables Risiko ergibt, sind Maßnahmen zur Risikominderung erforderlich sowie die Angabe der Wirkung der Risikominderung und die Validierung/Bestätigung der Minderungsmaßnahme. Einige Risikominderungsmaßnahmen werden vorgeschlagen und es wird auch angegeben, was üblicherweise von der entsprechenden Produktnorm abgedeckt wird. Wenn Hersteller beabsichtigen, ESHG/GA-Produkte/-Systeme zu entwickeln, die gefährliche Vorfälle zur Folge haben, die nicht von [4.2.4](#) abgedeckt sind, muss die Risikoanalyse dafür nach IEC 61508 durchgeführt werden.

5 Anforderungen an die funktionale Sicherheit

ANMERKUNG Verweisungen auf die gefährlichen Vorfälle von [4.2.4](#) sind in Klammern () angefügt.

5.1 Allgemeines

Die Analyse entsprechend IEC 61508 zeigt, dass funktionale Sicherheit sowohl von der Gestaltung und der Herstellung der Produkte als auch von der richtigen Anwendung der Produkte in Anlagen/Installationen abhängt.

5.2 bis 5.7 enthalten Anforderungen an ESHG/GA-Produkte und an die Bereitstellung der Informationen, die für die/den ordnungsgemäße(n) Installation, Betrieb und Instandhaltung dieser Produkte notwendig sind.

Wenn notwendig, wird die Einhaltung der Anforderungen an die Produkte und die Bereitstellung der Information geprüft.

Alle Produktprüfungen, auf die verwiesen wird, sind Typprüfungen.

Die Grundlage und die Hintergründe der folgenden Anforderungen sind in [Anhang B](#) zusammengestellt.

5.2 Spannungsversorgung

5.2.1 Im Falle eines Spannungsausfalls müssen die Produkte den Betrieb gefahrlos wieder aufnehmen, wenn die Spannungsversorgung wiederhergestellt wurde. (1)

ANMERKUNG Die gefahrlose Wiederaufnahme des Betriebs kann erreicht werden durch:

- Speicherung der Zustandsinformationen und Verwendung dieser Informationen zur Wiederaufnahme des Betriebs nach Wiederherstellung der Spannungsversorgung;
- Übergang in einen definierten Zustand des Produkts, abhängig von dessen Anwendung;
- Ermitteln des sicheren Zustands auf Grundlage der vom System zur Verfügung gestellten Informationen (von einem Steuergerät/Controller, sofern vorhanden, bzw. von den einzelnen Produkten);
- Aufrechterhaltung der Energieversorgung (durch Vorsehen einer geeigneten Pufferzeit entweder im Produkt und/oder in der Spannungsversorgung), um angeschlossenen Produkten den Übergang in einen sicheren Zustand zu ermöglichen.

5.2.2 Die Kennzeichnung des Produkts und seine Betriebsanleitung müssen so gestaltet sein, dass ein falsches Anschließen verhindert wird. (3) (6)

Die Kennzeichnung der Produkte muss lesbar und haltbar sein.

ANMERKUNG Es wird empfohlen, die Kennzeichnung sprachunabhängig zu gestalten.

Die Übereinstimmung muss durch Begutachtung der Produktdokumentation und, falls zutreffend, durch Prüfung der Lesbarkeit und Haltbarkeit der Aufschriften nach der entsprechenden Produktnorm überprüft werden.

5.2.3 Das Produkt muss so gestaltet und konstruiert sein, dass ein falsches Anschließen verhindert wird. Dies kann durch eine geeignete Gruppierung der Anschlüsse unterstützt werden. (6)

Die Übereinstimmung muss durch Begutachtung des Produkts überprüft werden.

5.3 Umgebung

5.3.1 Die Produkte müssen für die vorgesehene Umgebung ausgelegt sein und müssen unter diesen Bedingungen ordnungsgemäß arbeiten. (7, 8, 9, 13)

Die Übereinstimmung muss durch Prüfung des Produkts nach der entsprechenden Produktnorm und, falls eine solche nicht vorhanden ist oder sie die Umgebung nicht behandelt, nach den entsprechenden Sicherheitsgrundnormen überprüft werden.

5.3.2 Die Produkte und Komponenten müssen widerstandsfähig gegen ungewöhnliche Hitze sein und dürfen die Entstehung oder Ausbreitung von Feuer nicht unterstützen. (8)

Die Übereinstimmung muss durch Prüfung des Produkts nach der entsprechenden Produktnorm und, falls eine solche nicht vorhanden ist, nach den entsprechenden Sicherheitsgrundnormen überprüft werden.

5.3.3 Die Produkte müssen widerstandsfähig sein gegenüber den mechanischen Beanspruchungen, die bei der/den Anwendung(en) auftreten. (9)

Die Übereinstimmung muss durch Prüfung des Produkts nach der entsprechenden Produktnorm und, falls eine solche nicht vorhanden ist, nach IEC 63044-2 und den entsprechenden Sicherheitsgrundnormen überprüft werden.

5.4 Lebensdauer

Die Produkte müssen für eine definierte Lebensdauer nach IEC 61709:1998, 5.2 und [Anhang A](#), ausgelegt sein bzw. für eine definierte Anzahl von Schaltspielen unter Normalbedingungen.

Das Datenblatt muss Wartungsanweisungen enthalten, wenn zum Erreichen der festgelegten Lebensdauer erforderlich. (14)

Die Übereinstimmung muss durch Begutachtung der Dokumentation überprüft werden.

5.5 Vernünftigerweise vorhersehbare Fehlanwendung

5.5.1 Das Risiko für unbeabsichtigtes Laden der falschen Anwendungssoftware oder Parameter in die Produkte muss auf ein Minimum reduziert werden. (15)

ANMERKUNG Folgende Maßnahmen können angewendet werden:

- Auslegung des Konfigurationswerkzeugs;
- Identifizierung von Produkten und Vergleich ihrer Profile durch das Netzwerk-Management;
- Kennwort;
- Authentisierung;
- Produktdokumentation;
- Schulung von Installateuren und Bedienern/Benutzern.

Die Übereinstimmung muss durch Prüfung der Produkte und/oder durch Begutachtung der Produktdokumentation überprüft werden.

5.5.2 Die korrekte Konfiguration und die Berücksichtigung der richtigen zugehörigen Parameter müssen sichergestellt sein. (15)

ANMERKUNG Folgende Maßnahmen können angewendet werden:

- Festlegung von Parameterbereichen;
- eingeschränkte Konfigurationsmöglichkeiten für den Endbenutzer;
- Zugang zur Konfiguration nur für Fachpersonal;
- Konsistenzprüfung mit Hilfe von Werkzeugen oder durch den Installateur;
- Überprüfung der Übereinstimmung mit der Konfiguration.

Die Übereinstimmung muss durch Überprüfung der Übereinstimmung der vorhandenen mit der vorgesehenen Konfiguration überprüft werden.

5.5.3 Es müssen Maßnahmen zur Ermittlung und/oder Anzeige von fehlenden oder unvollständig konfigurierten Produkten während des Konfigurationsprozesses vorhanden sein. (15)

ANMERKUNG Folgende Maßnahmen können angewendet werden:

- Auslegung des Konfigurationswerkzeugs;
- formalisierte Installationsverfahren.

Die Übereinstimmung muss durch Prüfung der Produkte oder durch Begutachtung der Produktdokumentation überprüft werden.

5.6 Software und Kommunikation

5.6.1 Der Entwicklungsprozess für Software muss ISO 9000 oder ähnlichen Normen entsprechen. (16)

Die Übereinstimmung muss durch Begutachtung der Prozessdokumentation oder durch entsprechende Zertifikate überprüft werden.

5.6.2 Es müssen Maßnahmen zur Überprüfung des korrekten Funktionierens der Software und der Konsistenz der Konfiguration vorhanden sein. Wenn nicht ordnungsgemäßer Betrieb festgestellt wird, muss das Produkt die korrekten Werte wiederherstellen oder in einen definierten Zustand übergehen. (16)

Die Übereinstimmung muss durch Begutachtung der Dokumentation des Produktsoftwaredesigns überprüft werden.

5.6.3 Wenn die Anwendung es erfordert, müssen Maßnahmen innerhalb der Produkte vorhanden sein, um die Buslast auf dem Kommunikationsmedium zu begrenzen. (12) (17)

ANMERKUNG Folgende Maßnahmen können angewendet werden:

- Begrenzung zyklischer Übertragung;
- Begrenzung der Anzahl der Nachrichten je Produkt und Zeiteinheit;
- Begrenzung der Teilnehmerabfragezyklen (polling).

Die Übereinstimmung muss durch Begutachtung der Produktdokumentation und, wenn möglich, durch Produktprüfungen überprüft werden.

5.6.4 Das Empfangen von Nachrichten von mehreren Teilnehmern darf das ordnungsgemäße Funktionieren des Produkts nicht stören und darf keine Gefährdung bewirken. (23)

ANMERKUNG Folgende Maßnahmen können angewendet werden:

- Überprüfung der Quelladresse, sofern es eine Hierarchie der Quellen gibt;
- Anwendung der Regel: wer zuerst empfangen wird, wird auch zuerst verarbeitet (first in, first out);
- Anwendung der Regel: Vorrang der letzten Nachricht;
- Sicherung des Prozesses durch Abarbeitung, bevor neue Nachrichten das Verhalten ändern können;
- Sicherung des Prozesses durch Anhalten und Neustart des Prozesses;
- Sicherung des Prozesses durch Deaktivieren bzw. Aktivieren des Prozesses.

Die Übereinstimmung muss durch Begutachtung der Produktdokumentation und, wenn möglich, durch Produktprüfungen überprüft werden.

5.6.5 Die Produkte müssen bei Rücksetzen des Systems („System Reset“), sofern ein solcher erfolgt, in einen definierten Zustand gehen. (24)

Die Übereinstimmung muss durch Begutachtung der Produktdokumentation und, wenn möglich, durch Produktprüfungen überprüft werden.

5.6.6 Es muss möglich sein, den Zugang zur manuellen Konfiguration der Systemparameter einzuschränken. (24)

ANMERKUNG Folgende Maßnahmen oder Ausnahmen können angewendet werden:

- Einsatz eines Werkzeugs (Hardware oder Software);

- Verwendung eines Kennworts bzw. Authentisierung;
- Sicherstellung, dass unerlaubter Zugang nicht möglich ist;
- Kombination oder Folge von Aktionen;
- im Hintergrund ablaufende Einrichtungen für die Konfiguration;
- Ausnahme: Wenn die manuelle Konfiguration in der Betriebsanleitung explizit beschrieben wird (gilt auch für den Fall der automatischen Konfiguration).

Die Übereinstimmung muss durch Begutachtung der Produktdokumentation und, wenn möglich, durch Produktprüfungen überprüft werden.

5.6.7 Gestörte Kommunikation

5.6.7.1 Der sichere Betrieb eines Produkts muss unabhängig sein vom Betrieb anderer Produkte in dem System oder der Anwendung. (12)

ANMERKUNG Folgende Maßnahmen können angewendet werden:

- zyklische Übertragung;
- Überprüfung des zulässigen Bereichs empfangener Variablen.

Die Übereinstimmung muss durch Begutachtung der Ergebnisse einer Produktprüfung oder durch Begutachtung der Produktdokumentation überprüft werden.

5.6.7.2 Es müssen Maßnahmen zur Erkennung von gestörten Nachrichten vorhanden sein. Wird eine gestörte Nachricht entdeckt, muss dafür gesorgt werden, dass der sichere Betrieb sichergestellt ist. (11) (12)

Diese Anforderung kann ggf. durch eine Hamming-Distanz von 2 erfüllt werden.

ANMERKUNG Folgende Maßnahmen können angewendet werden:

- die Nachricht wird vom empfangenden Produkt zurückgewiesen oder korrigiert;
- die Nachricht wird vom Sender wiederholt.

Die Übereinstimmung muss durch Begutachtung der Ergebnisse einer Produktprüfung oder durch Begutachtung der Produktdokumentation überprüft werden.

5.6.7.3 Die Aussendung von falschen, formal korrekten Nachrichten muss verhindert werden.

Die Übereinstimmung wird durch die entsprechende EMV-Prüfung nach IEC 63044-5 (alle Teile) überprüft.

5.6.7.4 Es müssen Maßnahmen zur Anzeige von Nachrichtenverlust oder zur Wiederholung der Nachrichten im Fall des Nachrichtenverlustes vorhanden sein. (12) (17)

ANMERKUNG Folgende Maßnahmen können angewendet werden:

- Empfangsbestätigung auf der Kommunikationsebene oder auf der Anwendungsebene;
- Rückmeldungsstatusanzeige oder visuelle Effekte;
- geeignete ständige Wiederholung im Fall unidirektionaler Produkte.

Die Übereinstimmung muss durch Begutachtung der Ergebnisse einer Produktprüfung oder durch Begutachtung der Produktdokumentation überprüft werden.

5.7 Fernbedienung

5.7.1 Allgemeine Empfehlungen

Eine Fernsteuerung innerhalb eines Raums ist durch die vorangehenden Anforderungen abgedeckt.

Ferngesteuerte Steckdosen sollten so gekennzeichnet sein, dass sie für den Anwender klar zu erkennen sind, oder sie sollten so konstruiert sein, dass übliche Stecker für nicht ferngesteuerte Steckdosen darin nicht verwendet werden können. (22)

5.7.2 Innerhalb eines einzelnen Gebäudes oder in seiner unmittelbaren Umgebung

Produkte oder mit dem Produkt verbundene Subsysteme, die Schaden verursachen können und für die Fernsteuerung innerhalb eines einzelnen Gebäudes oder in seiner unmittelbaren Umgebung vorgesehen sind,

müssen über lokale Bedieneinrichtungen verfügen oder über lokale Einrichtungen, mit denen die Fernsteuerung freigegeben/gesperrt werden kann.

ANMERKUNG Folgende Maßnahmen können angewendet werden:

- lokale Bedieneinrichtungen an den potenziell gefährlichen Produkten;
- lokale Bedieneinrichtungen unmittelbar neben den potenziell gefährlichen Produkten;
- Eingänge für die Kommunikation, die den lokalen Betrieb unterstützen.

Die Übereinstimmung muss durch Begutachtung des Produkts oder der Produktdokumentation überprüft werden.

5.7.3 Von außerhalb des Gebäudes

5.7.3.1 Produkte oder Subsysteme, die Schaden verursachen können und die für Fernsteuerung von außerhalb des Gebäudes vorgesehen sind, müssen eine lokale Einrichtung für das bewusste Freischalten des ferngesteuerten Betriebs aufweisen.

ANMERKUNG Folgende Maßnahmen können angewendet werden:

- lokale Einrichtung zum Freischalten des Betriebs an potenziell gefährlichen Produkten;
- lokale Einrichtung zum Freischalten des Betriebs unmittelbar neben den potenziell gefährlichen Produkten;
- Eingänge für die Kommunikation, die die lokale Betriebsfreischaltung unterstützen;
- lokale Einrichtung zur Sperrung der Gebäude-Schnittstelle (des Gateways) oder anderer Produkte mit Fernzugriff.

Die Übereinstimmung muss durch Begutachtung des Produkts oder der Produktdokumentation überprüft werden.

5.7.3.2 Bei einer Fernsteuerung von außerhalb des Gebäudes müssen Verfahren zur Autorisierung und Authentisierung vorhanden sein (siehe auch [Tabelle 1](#)). (22) Dies kann für die Systemebene (Firewall oder Gateway) ebenso wie für die Produktebene gelten.

ANMERKUNG Autorisierung kann bedeuten:

- Autorisierung bzw. Authentisierung mit Passwort;
- Zugang über eine gesonderte Leitung.

Die Übereinstimmung muss durch Begutachtung des Produkts oder der Produktdokumentation überprüft werden.

5.7.4 Management

5.7.4.1 Es müssen Verfahren zur Autorisierung und Authentisierung von Fern-Management, wozu auch die Konfiguration und das Laden von außerhalb des Gebäudes gehören, vorhanden sein (siehe auch [Tabelle 1](#)). Dies kann für die Systemebene (Firewall oder Gateway) ebenso wie für die Produktebene gelten. (22)

ANMERKUNG Autorisierung kann bedeuten:

- Autorisierung bzw. Authentisierung mit Passwort;
- Zugang über eine gesonderte Leitung.

Die Übereinstimmung muss durch Begutachtung des Produkts oder der Produktdokumentation überprüft werden.

5.7.4.2 Es müssen Maßnahmen vorhanden sein, um die Übereinstimmung des eigentlichen Netzwerks mit seinem externen Abbild sicherzustellen. (22)

ANMERKUNG Folgende Maßnahmen können angewendet werden:

- Verfahren, um eine einzig maßgebliche Kopie der Systemdatenbank sicherzustellen;
- Verfahren, um die externe Systemdatenbank mit dem eigentlichen Netzwerk abzugleichen;
- Selbst-Dokumentationsfunktion im System (zentral oder dezentral).

Die Übereinstimmung muss durch Begutachtung des Produkts oder der Produktdokumentation überprüft werden.

Tabelle 1 – Anforderungen zur Vermeidung unbeabsichtigter Arbeitsgänge und mögliche Vorgehensweisen zu deren Erfüllung

Anforderungen	Optionen für die Umsetzung
Vermeidung der unbeabsichtigten Ausführung von Arbeitsgängen	Begrenzung externer Arbeitsgänge auf das, was <ul style="list-style-type: none"> • eindeutig vom Hausbewohner/Eigentümer freigegeben wurde, z. B. mit verzögerter Ausführung, • in der Gebäude-Schnittstelle (Gateway) festgelegt wurde.
Eine ungewollte Ausführung von Netzwerk-Management-Funktionen sollte nicht möglich sein.	Die Ausführung derartiger Funktionen sollte nur mit einem Werkzeug vorgenommen werden können; mechanisch, mit Software oder mit folgender Zugriffs-Kodierung: <ul style="list-style-type: none"> • einfache Zugangskodierung, 4 Stellen • lange Zugangskodierung (die einfache und lange Zugangskodierung können für geschlossene Kommunikationsmedien angewandt werden, für offene Medien reichen sie jedoch nicht aus, da dort die Kodierung übertragen wird) • Verschlüsselung bzw. Authentisierung
Überprüfung der Identität des Zielprodukts + Überprüfung der Identität des Teilnehmers, der Nachrichten/Informationen aus dem System lädt	z. B. „beglaubigtes Software-Paket“

Anhang A (informativ)

Beispiel für eine Methode zur Bestimmung der Sicherheits-Integritätslevel

A.1 Allgemeines

Mit dieser Methode kann das tolerierbare Risiko für die folgenden Systeme/Einrichtungen beschrieben werden:

- elektrische/elektronische/programmierbar elektronische (E/E/PE) sicherheitsbezogene Systeme;
- sicherheitsbezogene Systeme auf Basis anderer Technologien;
- externe risikomindernde Einrichtungen, die zu bestimmen sind.

Bild A.1 – [Quelle: IEC 61508-5:2010, Bild A.1] zeigt das allgemeine Konzept der Risikominderung.

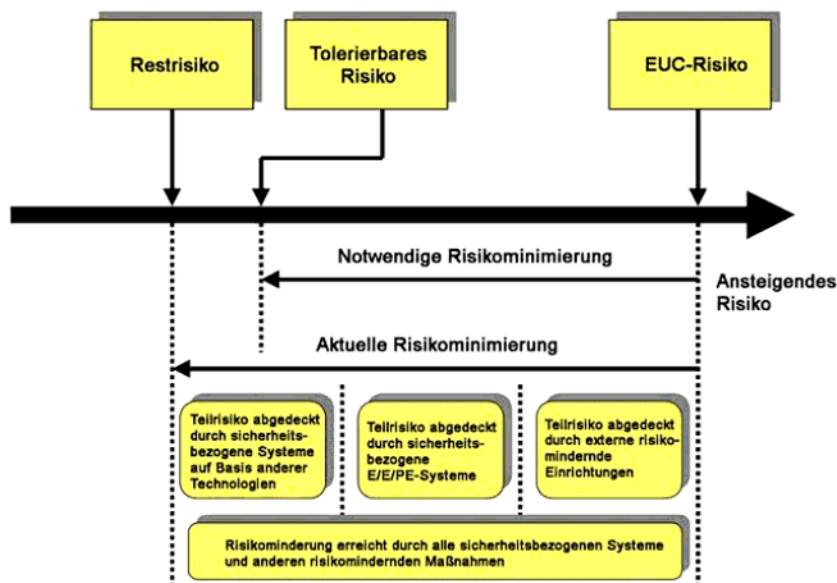


Bild A.1 – Risikominderung – Allgemeines Konzept

A.2 Begriffe

Für die Anwendung dieses Anhangs gelten die folgenden Begriffe.

A.2.1

Sicherheitsintegrität (en: safety integrity)

Wahrscheinlichkeit, dass ein sicherheitsbezogenes System die geforderten Sicherheitsfunktionen unter allen festgelegten Bedingungen innerhalb eines festgelegten Zeitraumes anforderungsgemäß aufrechterhält

[QUELLE: IEC 61508-4:2010, Begriff 3.5.4]

Anmerkung 1 zum Begriff: Je höher der Sicherheits-Integritätslevel, umso geringer ist die Wahrscheinlichkeit, dass das sicherheitsbezogene System bei Vorliegen einer Anforderung die festgelegten Sicherheitsfunktionen nicht ausführen oder einen festgelegten Zustand nicht annehmen wird.

Anmerkung 2 zum Begriff: Es gibt vier Stufen der Sicherheitsintegrität (siehe IEC 61508-4:2010, 3.5.8).

Anmerkung 3 zum Begriff: Für die Bestimmung der Sicherheitsintegrität sollten alle Ursachen von Ausfällen (sowohl zufällige Hardwareausfälle als auch systematische Ausfälle), die zu einem nicht sicheren Zustand führen können, berücksichtigt werden, z. B. Hardwareausfälle, Ausfälle durch Software und Ausfälle infolge elektrischer Störbeeinflussung. Einige dieser Ausfallarten, insbesondere zufällige Hardwareausfälle, können z. B. unter Verwendung der mittleren Häufigkeit von Ausfällen mit gefährbringender Ausfallart oder der Ausfallwahrscheinlichkeit eines sicherheitsbezogenen Schutzsystems bei Anforderung quantifiziert werden. Die Sicherheitsintegrität hängt jedoch auch von vielen Faktoren ab, die nicht genau quantifiziert, sondern nur qualitativ betrachtet werden können.

Anmerkung 4 zum Begriff: Die Sicherheitsintegrität beinhaltet die Sicherheitsintegrität der Hardware und die systematische Sicherheitsintegrität.

Anmerkung 5 zum Begriff: Diese Definition bezieht sich auf die Zuverlässigkeit der sicherheitsbezogenen Systeme, die Sicherheitsfunktionen auszuführen (siehe IEC 191-12-01, Begriff der Zuverlässigkeit).

A.2.2

Sicherheits-Integritätslevel

SIL

(en: safety integrity level)

eine von vier diskreten Stufen, die einem Wertebereich der Sicherheitsintegrität entsprechen, wobei der Sicherheits-Integritätslevel 4 die höchste Stufe der Sicherheitsintegrität und der Sicherheits-Integritätslevel 1 die niedrigste darstellt

Anmerkung 1 zum Begriff: Die Ausfallgrenze (siehe 3.5.17) für die vier Sicherheits-Integritätslevel sind in IEC 61508-1:2010, Tabellen 2 und 3, festgelegt.

Anmerkung 2 zum Begriff: Sicherheits-Integritätslevel werden zur Festlegung der Anforderungen an die Sicherheitsintegrität der Sicherheitsfunktionen, die dem sicherheitsbezogenen E/E/PE-System zugeordnet werden, verwendet.

Anmerkung 3 zum Begriff: Ein Sicherheits-Integritätslevel (SIL) ist keine Eigenschaft eines Systems, Teilsystems, Elements oder Bauteils. Die korrekte Deutung der Redensart „sicherheitsbezogenes System mit SIL n “ (wobei n 1, 2, 3 oder 4 ist) ist, dass das System möglicherweise fähig ist, Sicherheitsfunktionen mit einem Sicherheits-Integritätslevel bis zu n zu unterstützen.

[QUELLE: IEC 61508-4:2010, Begriff 3.5.8]

A.3 Das Konzept „So niedrig wie vernünftigerweise möglich“ (ALARP) und Konzepte für tolerierbares Risiko

Es gilt IEC 61508-5:2010, Anhang B. Ein Teil der Informationen aus IEC 61508-5:2010, Anhang B, wird in diesem Anhang in Auszügen wiederholt.

Tabelle A.1 enthält ein Beispiel, das den Zusammenhang von Risikowahrscheinlichkeiten (Häufigkeiten), Auswirkungen und Risikoklassen illustriert. Tabelle A.2 zeigt die Interpretation der Risikoklassen unter Verwendung von ALARP (en: as low as reasonably practicable).

Tabelle A.1 – Beispiel der Risikoklassifikation von Unfällen

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

ANMERKUNG Die tatsächlichen Risikoklassen I, II, III, IV sind abhängig vom Einsatzgebiet sowie davon, was die tatsächlichen 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.

Tabelle A.2 – Interpretation von 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