

	DIN IEC 63168-2 (VDE 0750-34-2)	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 11.180.01; 97.120

Einsprüche bis 2022-04-18

Entwurf

**Kooperative Mehrfachsysteme in vernetzten Wohnumfeldern –
AAL Anforderungen an funktionale Sicherheit von elektronischen
sicherheitsbezogenen Systemen –
Teil 2: Konzeptphase des Produktdesigns
(IEC SyCAAL/208/CDV:2021);
Text Deutsch und Englisch**

Cooperative multiple systems in connected home environments –
AAL functional safety requirements of electronic safety-related systems –
Part 2: Concept phase of product design
(IEC SyCAAL/208/CDV:2021);
Text in German and English

Anwendungswarnvermerk

Dieser Norm-Entwurf mit Erscheinungsdatum 2022-02-18 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, Merianstraße 28, 63069 Offenbach 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 62 Seiten

DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE

Anwendungsbeginn

Anwendungsbeginn dieser Norm ist ...

Inhalt

	Seite
Nationales Vorwort.....	5
Einleitung.....	6
1 Anwendungsbereich.....	9
2 Normative Verweisungen.....	9
3 Begriffe.....	10
4 Abkürzungen.....	11
5 Überblick über Sicherheitsaktivitäten während der Konzeptphase des Produktdesigns.....	12
6 H-SIL-Konzept.....	13
6.1 Ziele.....	13
6.2 Allgemeines.....	13
6.2.1 Notwendigkeit des H-SIL.....	13
6.2.2 H-SIL für vernetzte Systeme.....	14
6.3 Klassifizierung gefährlicher Ereignisse.....	15
6.3.1 Gefährdungsanalyse und Risikobewertung.....	15
6.3.2 Einschätzung des Schweregrads des Schadens.....	16
6.3.3 Einschätzung der Expositionswahrscheinlichkeit in Betriebssituationen.....	17
6.4 Erläuterung der Zuordnung der Vermeidbarkeit.....	17
6.4.1 Schätzung der Vermeidbarkeit.....	17
6.4.2 Beziehung zwischen Vermeidbarkeit und AAL-Benutzerdomäne.....	18
6.5 Bestimmung des H-SIL.....	19
6.6 Beispiele für die Bewertung der Vermeidbarkeit von Schäden an einem eingeführten Fall.....	21
6.6.1 Zweck.....	21
6.6.2 Beispiel für die Bewertung der Vermeidbarkeit unter der Voraussetzung der Einführung eines Notdienstes.....	21
7 Festlegung der Einheiten.....	23
7.1 Ziel der Festlegung der Einheiten.....	23
7.2 Prozess der Festlegung der Einheiten.....	23
7.2.1 Allgemeines.....	23
7.2.2 Für die Festlegung der Einheiten benötigte Informationen.....	24
7.2.3 Anforderungen an die Festlegung der Einheiten.....	24
7.3 Arbeitsergebnisse der Festlegung der Einheiten.....	24
8 Einleitung des Sicherheitslebenszyklus.....	25
8.1 Ziele der Einleitung des Sicherheitslebenszyklus.....	25
8.2 Prozess der Einleitung des Sicherheitslebenszyklus.....	25
8.2.1 Allgemeines.....	25
8.2.2 Für die Einleitung des Sicherheitslebenszyklus erforderliche Informationen.....	26

8.2.3	Bestimmung der Entwicklungskategorie für jede Einheit.....	26
8.2.4	Wirkungsanalyse und möglicher angepasster Sicherheitslebenszyklus im Fall einer Modifikation...	26
8.3	Arbeitsergebnisse der Einleitung des Sicherheitslebenszyklus.....	27
9	Gefährdungsanalyse und Risikobewertung (HARA).....	27
9.1	Ziele der Gefährdungsanalyse und Risikobewertung.....	27
9.2	Anforderungen und Empfehlungen für die Gefährdungsanalyse und Risikobewertung.....	28
9.2.1	Verfahren für die Vorbereitung der Gefährdungsanalyse und Risikobewertung.....	28
9.2.2	Teilnehmer an der Gefährdungsanalyse und Risikobewertung.....	28
9.2.3	Situationsanalyse und Gefährdungsermittlung.....	28
9.2.4	Klassifizierung des Auftretens von Schäden und Bestimmung des H-SIL.....	29
9.2.5	Ableitung von Sicherheitszielen.....	29
9.2.6	Verifizierung der Gefährdungsanalyse und Risikobewertung.....	29
9.3	Arbeitsergebnisse der Gefährdungsanalyse und Risikobewertung.....	29
10	Einführung des Konzepts der funktionalen Sicherheit.....	29
10.1	Zweck.....	29
10.2	Allgemeines.....	30
10.3	Für die Einführung des Konzepts der funktionalen Sicherheit erforderliche Informationen.....	30
10.4	Anforderungen und Empfehlungen.....	31
10.4.1	Abteilung von Anforderungen an die funktionale Sicherheit.....	31
10.4.2	Zuordnung der Anforderungen an die funktionale Sicherheit.....	31
10.4.3	Kriterien für die Sicherheitsvalidierung.....	31
10.4.4	Verifizierung des Konzepts der funktionalen Sicherheit.....	31
10.5	Arbeitsergebnisse der Einführung des Konzepts der funktionalen Sicherheit.....	32
Anhang A (informativ) Checkliste für technische Unterlagen.....		33
Literaturhinweise		34

Bilder

Bild 1 – Kooperative Mehrfachsysteme.....	6
Bild 2 – Sicherheitslebenszyklus.....	8
Bild 3 – Beziehung zwischen Produktlebenszyklus und Produktsicherheitslebenszyklus.....	12
Bild 4 – Modell des Auftretens eines Schadens.....	13
Bild 5 – Beispiele für ein vernetztes System.....	14
Bild 6 – Beispiel für nebeneinander bestehende Elemente.....	15
Bild 7 – H-SIL-Bestimmungstabelle (dreidimensionaler Ausdruck).....	21
Bild 8 – Beispiel: Hinzufügen eines Notdienstes zum bestehenden System.....	22
Bild 9 – Modell des Auftretens eines Schadens.....	28
Bild 10 – Hierarchie der Sicherheitsziele und der Anforderung an die funktionale Sicherheit.....	30

Tabellen

Tabelle 1 – Struktur von IEC 63168 (alle Teile)/betreffende Leser jedes Teils.....	7
Tabelle 2 – Klassifizierung des Schweregrads eines Schadens.....	17

Tabelle 3 – Klassifizierung der Expositionswahrscheinlichkeit in Betriebssituationen hinsichtlich der Dauer	17
Tabelle 4 – Klassifizierung der Vermeidbarkeit von Schäden.....	18
Tabelle 5 – Einstufung der AAL-Benutzerdomänen für die Schätzung der Vermeidbarkeit.....	18
Tabelle 6 – Bestimmung des H-SIL.....	19
Tabelle 7 – Beispiele: Überprüfung der Vermeidbarkeit von Schäden mit anderen Pflegediensten.....	22
Tabelle A.1 – Checkliste für technische Unterlagen.....	33

Nationales Vorwort

Das internationale Dokument IEC SyCAAL/208/CDV:2021-01 „Cooperative multiple systems in connected home environments – AAL functional safety requirements of electronic safety-related systems – Part 2: Concept phase of product design“ (CDV, en: Committee Draft for Vote) 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 CDV entsprechend der diesbezüglich durch die IEC erteilten Erlaubnis beigelegt. Die Nutzungsbedingungen für den deutschen Text des Norm-Entwurfes gelten gleichermaßen auch für den englischen IEC-Text.

Das internationale Dokument wurde vom IEC/SyC AAL „Active Assisted Living“ der Internationalen Elektrotechnischen Kommission (IEC) erarbeitet und unterliegt dem Copyright der IEC . Das Dokument wurde den nationalen Komitees zur Stellungnahme und Abstimmung vorgelegt. Es wird jedoch nicht zeitgleich (parallel) bei IEC und CENELEC zur Umfrage gestellt. Derzeit ist also nicht vorgesehen, dieses Dokument als Europäische Norm zu übernehmen.

Da der Abstimmungszeitraum für einen FDIS (en: Final Draft International Standard) 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 CDV als DIN-Norm-Entwurf veröffentlicht, um die Stellungnahmen aus der Öffentlichkeit noch vor der Abstimmung berücksichtigen zu können.

Für dieses Dokument ist das nationale Arbeitsgremium DKE/K 801 „System Komitee AAL“ der DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE (www.dke.de) zuständig.

Aktuelle Informationen zu diesem Dokument können über die Internetseiten von DKE (www.dke.de) und DIN (www.din.de) durch eine Suche nach der Dokumentennummer aufgerufen werden.

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 Tabellen und Bilder in Farbe, die in der Papierversion in einer Graustufen-Darstellung wiedergegeben werden. Elektronische Versionen dieses Dokuments enthalten die Bilder in der originalen Farbdarstellung.

Einleitung

IEC 63168 (alle Teile) legt AAL-spezifische Anforderungen an die funktionale Sicherheit von elektrischen/elektronischen (E/E) sicherheitsbezogenen Systemen für kooperative Mehrfachsysteme fest, die gemeinsam in einem vernetzten Wohnumfeld betrieben werden, wie in Bild 1 gezeigt.

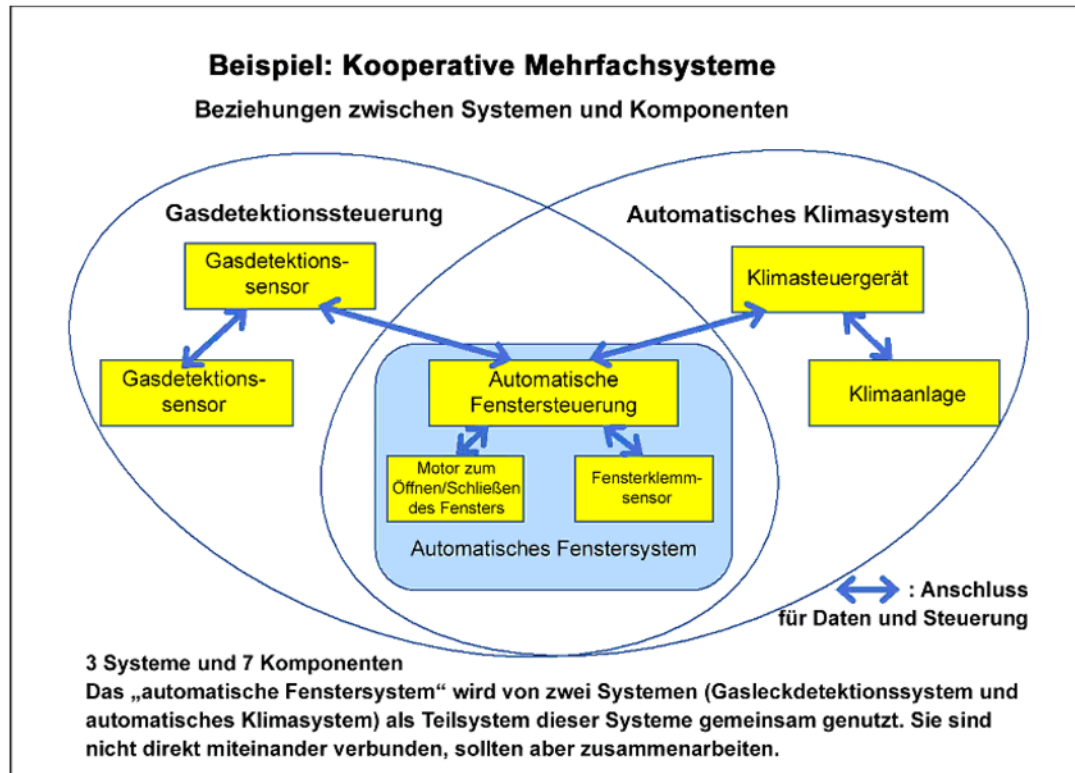


Bild 1 – Kooperative Mehrfachsysteme

IEC 63168 (alle Teile) kann auch für nicht kooperative Systeme in vernetzten Wohnumfeldern angewendet werden, die in Bezug auf die Sicherheitskonzeption nicht zum Anwendungsbereich anderer Normen, Vorschriften oder Gesetze gehören. Bei der Planung eines kooperativen Mehrfachsystems ist die Berücksichtigung der Anbindung oder anderer Faktoren der Elemente (wie Systeme und Sensoren) wichtig. Diese Faktoren der Elemente müssen durch nationale Normen, Leitlinien, Gesetze usw. geregelt werden. Die Elemente ohne Anbindung an kooperative Mehrfachsysteme gehören nicht zum Anwendungsbereich.

ANMERKUNG 1 Wenn z. B. in Europa Brandmeldekomponenten nach EN 14604 und der Normenreihe EN 54, Einbruch- und Überfallmeldeanlagen nach der Normenreihe IEC 62642 (oder der Normenreihe EN 50131), Videoüberwachungsanlagen nach der Normenreihe EN 62676 und Zutrittskontrollanlagen nach der Normenreihe EN 60839-11 in das vernetzte Wohnumfeld integriert werden, können sie als kooperative Systeme betrachtet werden, ohne die Anforderungen von IEC 63168 (alle Teile) zu erfüllen.

Die IEC 63168 (alle Teile) besteht aus vier Teilen:

- Teil 1: Allgemeine Anforderungen an Design und Entwicklung
- Teil 2: Konzeptphase des Produktdesigns
- Teil 3: Produktentwicklung
- Teil 4: Produktion, Betrieb, Modifikation und Unterstützungsprozess

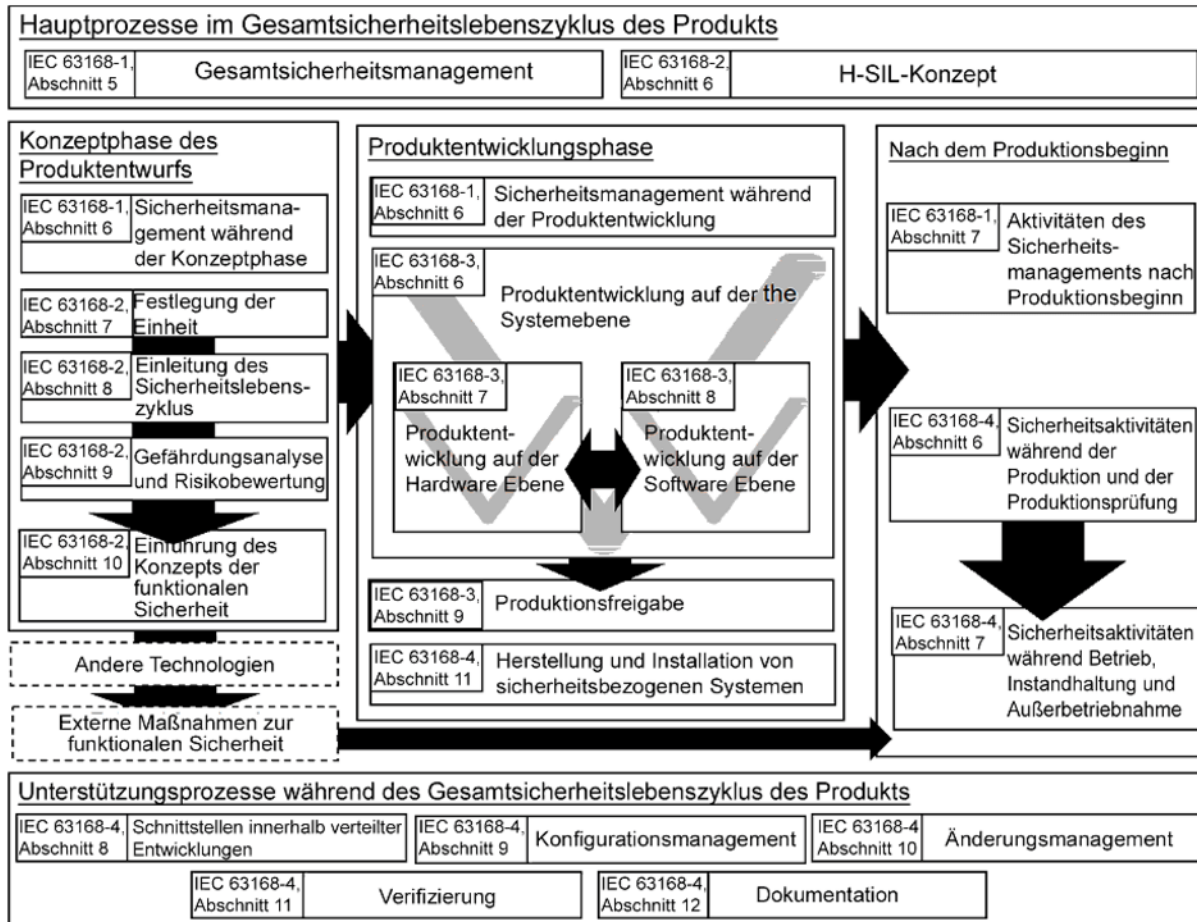
wie in Tabelle 1 angegeben.

Tabelle 1 – Struktur von IEC 63168 (alle Teile)/betreffende Leser jedes Teils

Teil	Titel	Betreffende Leser
1	Allgemeine Anforderungen an Design und Entwicklung	Alle mit Sicherheitsfragen in einem vernetzten Wohnumfeld Beschäftigten
2	Konzeptphase des Produktdesigns	Designer von kooperativen Systemen in einem vernetzten Wohnumfeld
3	Produktentwicklung	Systementwickler von kooperativen Systemen in einem vernetzten Wohnumfeld
4	Produktion, Betrieb, Modifikation und Unterstützungsprozess	Errichter, Instandhaltungsdienstleister, Designer von kooperativen Systemen in einem vernetzten Wohnumfeld

ANMERKUNG 2 Zu Instandhaltungsdienstleistern gehören auch Organisationen von Instandhaltungsdienstleistern.

Dieses Dokument legt die Sicherheitsaktivitäten fest, die in der Konzeptphase durchgeführt werden, d. h. zu Beginn des Sicherheitslebenszyklus, wie in [Bild 2](#) dargestellt. Die relevanten Leser dieses Dokuments sind Designer von kooperativen Systemen in vernetzten Wohnumfeldern, die sicherstellen müssen, dass das System für seinen vorgesehenen AAL-Nutzer ausreichend sicher ist. In dieser Phase des Sicherheitslebenszyklus müssen die kooperativen Systeme unter Berücksichtigung der Tatsache geplant werden, dass die vernetzten Wohnumfelder, in denen die Systeme installiert werden, auch ältere Nutzer und solche mit Behinderungen oder Beeinträchtigungen umfassen werden. Das bedeutet, dass die Einbeziehung von AAL-Aspekten notwendig ist, wenn die Sicherheit des kooperativen Systems geplant wird.



ANMERKUNG 3 In jeder Phase sind Überlegungen zur Harmonisierung der einschlägigen Normen erforderlich.

Bild 2 – Sicherheitslebenszyklus

Dieses Dokument beschreibt die Verfahren, nach denen Designer von kooperativen Systemen in vernetzten Wohnumfeldern vorgehen müssen, um AAL-Aspekte in den Sicherheitsentwurf einzubeziehen, wie z. B. Festlegung der Einheiten, Gefährdungsanalyse und Risikobewertung sowie die Definition der funktionalen Sicherheit. Der Schlüsselgedanke bei der Einbeziehung von AAL-Aspekten in den Sicherheitsentwurf von kooperativen Systemen, der hier behandelt wird, ist „H-SIL (Sicherheits-Integritätslevel für ein vernetztes Wohnumfeld)“ als eines der Verfahren bei der Gefährdungsanalyse und Risikobewertung. Der H-SIL wird ermittelt, indem eine Gefährdungsanalyse und Risikobewertung des Schweregrads und der Wahrscheinlichkeit des Auftretens einer möglichen Gefährdung im vernetzten Wohnumfeld durchgeführt wird.

Kooperative Mehrfachsysteme in vernetzten Wohnumfeldern – AAL Anforderungen an funktionale Sicherheit von elektronischen sicherheitsbezogenen Systemen – Teil 2: Konzeptphase des Produktdesigns

1 Anwendungsbereich

Dieses Dokument legt die Verfahren als „Konzeptphase“ im Sicherheitslebenszyklus fest, nach denen Designer von kooperativen Mehrfachsystemen im vernetzten Wohnumfeld vorgehen, um Sicherheitsmaßnahmen unter Berücksichtigung von AAL-Aspekten zu entwerfen. Es wird der Sicherheits-Integritätslevel für ein vernetztes Wohnumfeld (H-SIL) definiert, wie dieser bestimmt wird und wie er für die Gefährdungsanalyse und Risikobewertung zu nutzen ist.

Die Vermeidbarkeit ist der Schlüsselgedanke bei der Festlegung des H-SIL in der Konzeptphase im Sicherheitslebenszyklus und wird hier behandelt. Die Vermeidbarkeit ermöglicht den Designer von kooperativen Systemen, einen angemessenen H-SIL unter Berücksichtigung der AAL-Stufen des Nutzers, der einfachen Möglichkeit für Nutzer, Schaden oder gefährliche Situationen zu vermeiden, der für Nutzer im Notfall verfügbaren Dienste usw. festzulegen.

ANMERKUNG Die Vermeidbarkeit beruht auf dem Begriff der Beherrschbarkeit nach der Festlegung in ISO 26262-1. Siehe auch 3.1.

Die grundlegenden und allgemeinen Anforderungen werden in Übereinstimmung mit den Grundsätzen der Grundnorm für funktionale Sicherheit, IEC 61508, und anderen verwandten Normen, einschließlich ISO/IEC 14762 und IEC 63044 (alle Teile), festgelegt.

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).

ISO/IEC 14762:2009, *Information technology – Functional safety requirements for Home and Building Electronic Systems (HBES)*

ISO 25119-1:2018, *Tractors and machinery for agriculture and forestry – Safety-related parts of control systems – Part 1: General principles for design and development*

ISO 26262 (all parts):2018, *Road vehicles – Functional safety*

IEC 61508 (all parts):2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems*

IEC 63044 (all parts):2017, *Home and Building Electronic Systems (HBES) and Building Automation and Control Systems (BACS)*

IEC 63168-1:20XX, *Cooperative multiple systems in connected home environments – AAL functional safety requirements of electrical/electronic safety related systems – Part 1: General requirements for design and development*

IEC 63168-3:20XX, *Cooperative multiple systems in connected home environments – AAL functional safety requirements of electrical/electronic safety-related systems – Part 3: Product development*

IEC 63168-4:20XX, *Cooperative multiple systems in connected home environments – AAL functional safety requirements of electrical/electronic safety related systems – Part 4: Production, operation, modification and supporting process*

3 Begriffe

Für die Anwendung dieses Dokuments gelten die Begriffe nach IEC 63168-1.

ISO und IEC stellen terminologische Datenbanken für die Verwendung in der Normung unter den folgenden Adressen bereit:

- IEC Electropedia: verfügbar unter <http://www.electropedia.org/>
- ISO Online Browsing Platform: verfügbar unter <http://www.iso.org/obp>

3.1

Vermeidbarkeit

Fähigkeit, einen Schaden oder eine Beschädigung durch rechtzeitige Reaktionen von Personen oder externe Maßnahmen zu vermeiden oder zu begrenzen

[QUELLE: ISO 26262-1:2018, 3.25, modifiziert – Definition der Beherrschbarkeit]

3.2

Notfallbetrieb

Betriebsmodus eines Elements, um nach der Reaktion auf einen Fehlzustand Sicherheit zu bieten, bis der Übergang in einen sicheren Zustand erreicht ist

[QUELLE: ISO 26262-1:2018, 3.43, modifiziert – Alle Anmerkungen zum Begriff und BEISPIEL wurden gestrichen.]

3.3

Fehlertoleranzzeit

Minstdauer vom Auftreten eines Fehlzustands in einer Einheit bis zum möglichen Auftreten eines gefährlichen Ereignisses, wenn die Sicherheitsmechanismen nicht aktiviert sind

[QUELLE: ISO 26262-1:2018, 3.61, modifiziert – Alle Anmerkungen zum Begriff und BEISPIEL wurden gestrichen.]

3.4

Funktionskonzept

Festlegung der vorgesehenen Funktionen und ihrer Wechselwirkungen, die zum Erreichen des gewünschten Verhaltens erforderlich sind

Anmerkung 1 zum Begriff: Das Funktionskonzept wird in der Konzeptphase entwickelt.

[QUELLE: ISO 26262-1:2018, 3.66]

3.5

Konzept der funktionalen Sicherheit

Festlegung der Anforderungen an die funktionale Sicherheit mit zugehörigen Informationen, deren Zuordnung zu Elementen innerhalb der Architektur und deren Wechselwirkung, die zum Erreichen der Sicherheitsziele erforderlich sind

[QUELLE: ISO 26262-1:2018, 3.68]

3.6

vernünftigerweise vorhersehbare Fehlanwendung

Verwendung einer Maschine in einer Weise, die vom Designer nicht beabsichtigt ist, die sich jedoch aus einem leicht vorhersehbaren menschlichen Verhalten ergeben kann

[QUELLE: ISO 25119-1:2018, 3.37]

3.7

sicherer Zustand

Betriebsmodus einer Einheit bei einem Fehlzustand ohne unangemessenes Risiko

BEISPIEL Ausgeschalteter Zustand (bei Systemen ohne Fehlertoleranz).

[QUELLE: ISO 26262-1:2018, 3.131, modifiziert – Alle Anmerkungen zum Begriff wurden gestrichen.]

3.8

Sicherheitsvalidierung

Zusicherung auf der Grundlage von Untersuchungen und Prüfungen, dass die Sicherheitsziele angemessen sind und mit einem ausreichenden Integritätslevel erreicht wurden

[QUELLE: ISO 26262-1:2018, 3.148, modifiziert – Anmerkung 1 zum Begriff wurde gestrichen.]

3.9

Verifizierung

Bestätigung durch Bereitstellung eines objektiven Nachweises, dass festgelegte Anforderungen erfüllt worden sind

Anmerkung 1 zum Begriff: Die Benennung „verifiziert“ wird zur Bezeichnung des entsprechenden Status verwendet.

Anmerkung 2 zum Begriff: Die Entwicklungsverifizierung ist die Anwendung von Prüfungen und Bewertungen, um die Konformität eines Entwurfs hinsichtlich der festgelegten Anforderungen zu beurteilen.

Anmerkung 3 zum Begriff: Im Fall von Software wird die Verifizierung in unterschiedlichen Entwicklungsstadien durchgeführt, dabei werden die Software und ihre Bestandteile auf Übereinstimmung mit den zu Anfang dieses Stadiums festgelegten Anforderungen hin untersucht.

[QUELLE: IEC 192-01-07]

3.10

Verifizierungsprüfung

Verifizierungsaktivität, um sicherzustellen, dass das Ergebnis einer Entwicklungstätigkeit die Projektanforderungen oder die technischen Anforderungen oder beides erfüllt

Anmerkung 1 zum Begriff: Einzelne Anforderungen an Verifizierungsprüfungen sind in spezifischen Abschnitten einzelner Teile der Normenreihe IEC 63168 enthalten.

Anmerkung 2 zum Begriff: Das Ziel von Verifizierungsprüfungen ist die technische Fehlerfreiheit und Vollständigkeit der Einheit oder des Elements.

BEISPIEL Die Arten der Verifizierungsprüfung können eine technische Überprüfung, eine Begehung oder eine Inspektion sein.

[QUELLE: ISO 26262-1:2018, 3.181, modifiziert – „ISO 26262“ wurde ersetzt durch „IEC 63168“.]

4 Abkürzungen

Für die Anwendung dieses Dokuments gelten die folgenden Abkürzungen sowie die Abkürzungen nach IEC 63168-1.

ADL	Alltagsaktivitäten (en: activities of daily living)
E/E	elektrisch/elektronisch (en: electrical/electronic)
FMEA	Ausfalleffektanalyse (en: failure mode and effects analysis)
FTA	Fehlzustandsbaumanalyse (en: fault tree analysis)

HARA	Gefährdungsanalyse und Risikobewertung (en: hazard analysis and risk assessment)
HAZOP	Gefährdungs-und Betreibbarkeitsuntersuchung (en: hazard and operability study)
H-SIL	Sicherheits-Integritätslevel für ein vernetztes Wohnumfeld (en: safety integrity level for connected home environment)
IADL	instrumentelle Alltagsaktivitäten (en: instrumental activities of daily living)
QM	Qualitätsmanagement des Systems (en: quality management of system)
STAMP/STPA	systemtheoretisches Unfallmodell und Unfallprozesse/systemtheoretische Prozessanalyse (en: system theoretic accident model and processes / system theoretic process analysis)

5 Überblick über Sicherheitsaktivitäten während der Konzeptphase des Produktdesigns

Es werden die Sicherheitsaktivitäten und die Anforderungen an die funktionale Sicherheit beschrieben, die zur Entwicklung von kooperativen Mehrfachsystemen in vernetzten Wohnumfeldern erforderlich sind.

Die in der Konzeptphase des Produktdesigns durchgeführten Sicherheitsaktivitäten sind in die folgenden vier Prozesse unterteilt:

- Festlegung der Einheiten: Unterteilung des Produkts (Gesamtsystem) in mehrere Teilsysteme (Einheiten) ([Abschnitt 7](#));
- Einleitung des Sicherheitslebenszyklus: Bestimmung, ob es sich bei jeder Einheit um eine Neuentwicklung oder eine Modifikation einer vorhandenen Einheit handelt, und Analyse der Auswirkungen der im letzteren Fall erforderlichen Modifikation ([Abschnitt 8](#));
- Gefährdungsanalyse und Risikobewertung: Analyse der Sicherheit des Gesamtsystems und Ableitung der Sicherheitsziele ([Abschnitt 9](#)); und
- Einführung des Konzepts der funktionalen Sicherheit: Zuordnung der von den Sicherheitszielen abgeleiteten Designanforderungen zu den Elementen, aus denen die Einheit besteht ([Abschnitt 10](#)).

[Bild 3](#) zeigt die Beziehung zwischen dem Produktlebenszyklus und dem Produktsicherheitslebenszyklus in der Konzeptphase des Produktdesigns. Der Produktlebenszyklus und der Produktsicherheitslebenszyklus bestehen nicht getrennt voneinander. Der Produktsicherheitslebenszyklus umfasst die Sicherheitsaktivitäten, die im Produktlebenszyklus erforderlich sind, und die Sicherheitsaktivitäten während der Konzeptphase müssen in das Produktdesign einbezogen werden.

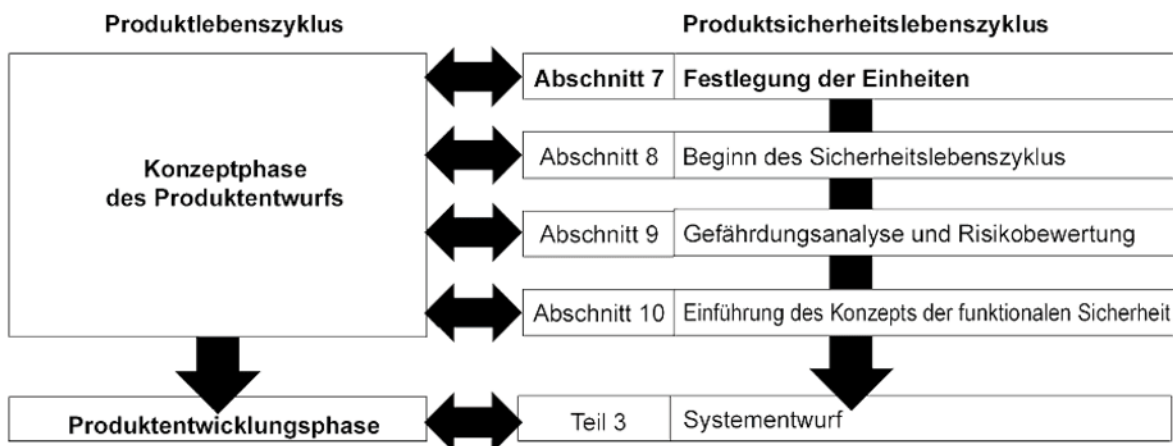


Bild 3 – Beziehung zwischen Produktlebenszyklus und Produktsicherheitslebenszyklus

Bei den Sicherheitsaktivitäten nach der Gefährdungsanalyse und Risikobewertung im Produktsicherheitslebenszyklus muss der H-SIL ([Abschnitt 6](#)) als Indikator für die Beurteilung der Sicherheitsanforderung verwendet werden.

Bei der Umsetzung der Sicherheitsaktivitäten in der Konzeptphase des Produktdesigns sind die Inhalte des Gesamtsicherheitsmanagements (IEC 63168-1:20xx, Abschnitt 5) und des Sicherheitsmanagements während der Konzeptphase und der Produktentwicklung (IEC 63168-1:20xx, Abschnitt 6) zu beachten.

6 H-SIL-Konzept

6.1 Ziele

Bei der Betrachtung der funktionalen Sicherheit wird häufig entweder der Sicherheits-Integritätslevel oder der Performance Level als allgemeiner Kennwert verwendet. Ein neuer Kennwert für den Sicherheitslevel wird eingeführt, wenn es sich um die funktionale Sicherheit von kooperativen Mehrfachsystemen als Produkt in vernetzten Wohnumfeldern handelt. Der Schlüsselgedanke bei der Koordination von Geräten ist, dass die Nutzer der Systeme Bewohner und Besucher sind.

Die Ziele von [Abschnitt 6](#) sind folgende:

- Das erste Ziel ist die Darstellung des H-SIL-Konzepts, das den erreichten Grad der Vollständigkeit der von IEC 63168 (alle Teile) definierten Sicherheitsanforderungen wiedergibt, und die Erläuterung der Notwendigkeit des H-SIL und seiner Bedeutung.
- Das zweite Ziel ist eine Erläuterung, wie der H-SIL zu bestimmen ist. Der H-SIL wird auf der Grundlage der Gefährdungsanalyse und Risikobewertung für gefährliche Ereignisse innerhalb des von IEC 63168 (alle Teile) festgelegten Anwendungsbereichs unter Verwendung des in [6.3](#) angegebenen Klassifizierungsverfahrens ermittelt.

6.2 Allgemeines

6.2.1 Notwendigkeit des H-SIL

Das Konzept des H-SIL gibt ein Maß für die erreichte funktionale Sicherheit einer Einheit an. Damit wird der Grad der Vollständigkeit der Sicherheitsanforderungen in Übereinstimmung mit IEC 63168 (alle Teile) angegeben. Da Sicherheitsanforderungen als Anforderungen zur Vermeidung oder Abschwächung von Gefährdungen durch Ausfälle in E/E-Systemen abgeleitet werden, ist der H-SIL anders formuliert ein Maß, mit dem die Gründlichkeit der Sicherheitsmaßnahmen gegenüber Fehlfunktionen von elektrischen/elektronischen Systemen angegeben wird. Der H-SIL ist als gemeinsames Verständnis der funktionalen Sicherheit im Haus notwendig, um das Maß festzulegen, wie gründlich ein E/E-System entwickelt werden muss.

Bild 4 stellt ein Kausalmodell dafür dar, wie eine Fehlfunktion in einem E/E-System zum Auftreten eines Schadens führt. Dieses Modell zeigt, dass das Auftreten eines gefährlichen Ereignisses als Folge einer Gefährdung in einer bestimmten Betriebssituation eines Systems zu einem Schaden für den Systemnutzer führt, wenn dieser das gefährliche Ereignis nicht vermeiden kann. Der H-SIL wird auf der Grundlage bestimmt, wie die Gefährdung und die Wahrscheinlichkeit ihres Auftretens verringert werden können, um das damit verbundene Risiko auf ein vertretbares Maß herabzusetzen. Daher wird der H-SIL durch die geschätzten Ergebnisse von S (Schweregrad des Schadens), E (Wahrscheinlichkeit, der Betriebssituation ausgesetzt zu sein) und A (Vermeidbarkeit) bestimmt, um den Grad darzustellen, in dem der Schaden für einen Bewohner vermieden werden kann.

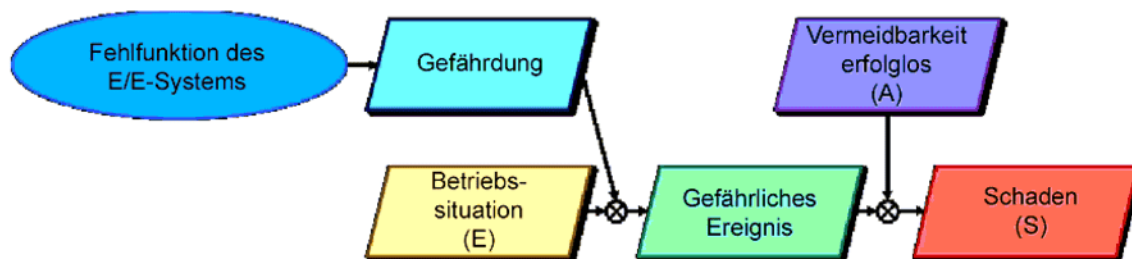


Bild 4 – Modell des Auftretens eines Schadens

ANMERKUNG Die Werte S und E in Bild 4 können in Übereinstimmung mit IEC 61508 ermittelt werden. IEC 63168 (alle Teile), die die funktionale Sicherheit in vernetzten Wohnumfeldern behandelt, geht jedoch davon aus, dass die Bewohner in der Regel nicht als Nutzer von E/E-Systemen in einem solchen Wohnumfeld geübt sind. Außerdem scheint es für den Bewohner schwierig zu sein, Risiken durch die Bedienung von Heimgeräten zu vermeiden. Daher wird A (Vermeidbarkeit) als Kennwert definiert, um die Klasse darzustellen, mit der die Risiken für den Bewohner in Bezug auf die Vorgabezeit für die Bedienung von Heimgeräten, die Umgebungsbedingungen des vernetzten Heims usw. aus Sicht des AAL vermieden werden können. Die Vermeidbarkeit kann durch Funktionen des Heims zur Vermeidung von Schäden verbessert werden (z. B. Verwendung von Materialien und Entwürfen, mit denen sich ein Bewohner nicht so leicht verletzt, wenn er stürzt, Nutzung eines Überwachungsdienstes, durch den dem Bewohner im Notfall geholfen werden kann, usw.). Die Vermeidbarkeit von Schäden wird also in Bezug auf die Fähigkeiten eines Bewohners und die Funktionen des Heims definiert, wie die Verwendung von benutzerfreundlichen Materialien, eine barrierefreie Gestaltung, ein regionaler Hilfsdienst, durch den im Notfall ein Helfer zum Bewohner gehen kann, externe Dienste von medizinischen Einrichtungen oder intelligente Städte (Smart Cities), die für eine Schadensvermeidung ausgelegt sind, usw.

6.2.2 H-SIL für vernetzte Systeme

Ein von IEC 63168 (alle Teile) beschriebenes System ist kein Einzelsystem, sondern ein vernetztes System, in dem mehrere Systeme zusammenwirken. Bild 5 zeigt ein Beispiel für ein vernetztes System, in dem ein Gasleckdetektionssystem und ein automatisches Klimasystem durch die Nutzung eines automatischen Fenstersystems als Teil jedes Systems zusammenwirken.

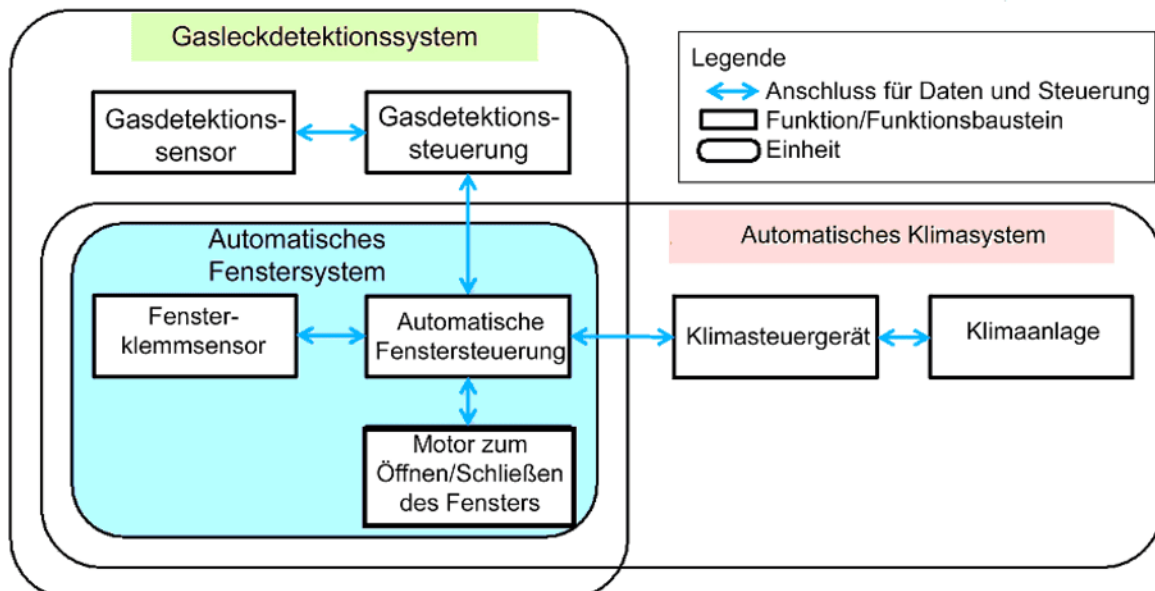


Bild 5 – Beispiele für ein vernetztes System

Der H-SIL wird für jede Einheit bestimmt. Im Beispiel in Bild 5 muss der H-SIL bestimmt werden, indem die Werte von S, E und A für jedes der Systeme ermittelt werden. Zu diesem Zeitpunkt kann die Bestimmung des H-SIL des automatischen Fenstersystems, das gemeinsam vom Gasleckdetektionssystem und vom automatischen Klimasystem verwendet wird, von den ermittelten H-SILs beeinflusst werden, die den Sicherheitsanforderungen der anderen beiden Systeme zugeordnet sind.

Wie beispielsweise in Bild 6 dargestellt, wird das Nebeneinanderbestehen der Elemente der automatischen Fenstersteuerung entsprechend den Schnittstellen mit dem Fensterklemmsensor, der Gasleckdetektionssteuerung und dem Klimasteuergerät hergestellt. Jedem Element werden Sicherheitsanforderungen zugeordnet, wobei für jedes zugehörige System der H-SIL bestimmt wird. Unter der Annahme, dass der H-SIL für das automatische Fenstersystem X ist, der H-SIL für das Gasleckdetektionssystem Y ist und der H-SIL für das automatische Klimasystem Z ist, werden alle Elemente entsprechend dem höchsten H-SIL unter X, Y und Z entwickelt, sofern nicht nachgewiesen wird, dass sich die nebeneinander bestehenden Elemente in der automatischen Fenstersteuerung nicht gegenseitig beeinflussen.

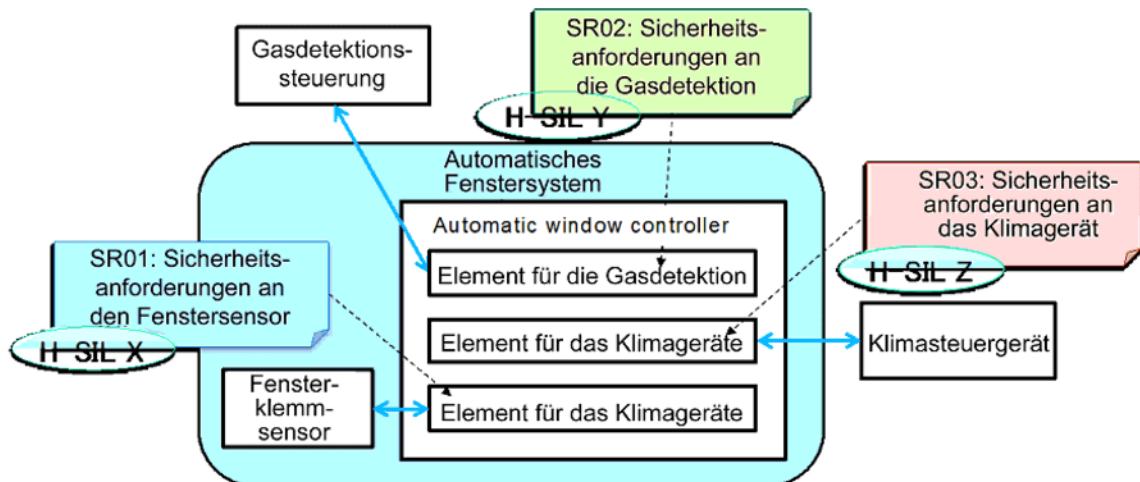


Bild 6 – Beispiel für nebeneinander bestehende Elemente

Bei Heimsystemen kommt es in der Regel zum Austausch von Heimgeräten und zum Hinzufügen/Aktualisieren von Systemfunktionen. In einem solchen Fall muss sichergestellt werden, dass ein neu eingeführtes Element mit einem höheren H-SIL als die bestehenden Elemente nicht beeinflusst wird. Eine Möglichkeit besteht darin, das bestehende System neu zu entwickeln, um dessen H-SIL auf den höheren H-SIL des neuen Elements anzuheben, was in der Regel schwierig ist. Daher ist es notwendig, die Auswirkungen der hinzugefügten Elemente zu analysieren und den Nachweis zu erbringen, dass sich die Elemente nicht gegenseitig beeinflussen.

ANMERKUNG Beeinflussung bedeutet, dass der Ausfall eines Elements mit einem niedrigeren H-SIL einen Ausfall eines Elements mit einem höheren H-SIL nach sich zieht.

6.3 Klassifizierung gefährlicher Ereignisse

6.3.1 Gefährdungsanalyse und Risikobewertung

Als eine Voraussetzung für eine Gefährdungsanalyse und Risikobewertung müssen mögliche Gefährdungen im Anwendungsbereich festgestellt werden. Mit der Gefährdungsanalyse und Risikobewertung müssen der Grad der Auswirkung einer Gefährdung und die Auftretenswahrscheinlichkeit einer Gefährdung untersucht werden.

ANMERKUNG 1 In der Regel wird eine Gefährdung anhand ihrer Auswirkung auf die Gesundheit und das Leben von Menschen definiert. Es besteht die Möglichkeit und gewinnt immer mehr an Bedeutung, Auswirkungen auf die Umwelt sowie „wirtschaftliche Verluste“ und „Geschäftsverluste durch eine Rufschädigung“ in die Diskussion über Gefährdungen einzubeziehen.

ANMERKUNG 2 Zu den im Allgemeinen für eine Gefährdungsanalyse und Risikobewertung benutzten Verfahren gehören HAZOP und FMEA. Verfahren für die Untersuchung der Leistungsgrenzen und der Fehlanwendung sind STAMP/STPA.

Die Gefährdungsanalyse und Risikobewertung muss von mehreren Personen mit Fachwissen aus verschiedenen Abteilungen, z. B. der Entwicklung des elektrischen und elektronischen Steuersystems, der Prüfung, der Verifizierung, den Diensten, und externen Beratern einschließlich einer technischen Prüfstelle durchgeführt werden.

ANMERKUNG 3 In der Regel wird die Gefährdungsanalyse und Risikobewertung im Entwicklungsprozess von den Fachleuten des Entwerfers selbst durchgeführt. Obwohl deren Meinung berücksichtigt werden kann, ist die dritte Partei allein möglicherweise nicht in der Lage, ein Ergebnis in einer begründeten Analyse zu erzielen, da sie nicht unbedingt eine Fachkraft auf dem Gebiet des zu untersuchenden Themas ist.

Bei der Gefährdungsanalyse und Risikobewertung muss jedes festgestellte gefährliche Ereignis klassifiziert werden, sofern es zum Anwendungsbereich von IEC 63168 (alle Teile) gehört. Bild 4 stellt ein Kausalmodell dafür dar, wie eine Fehlfunktion in einem E/E-System zum Auftreten eines Schadens führt. Dieses Modell

zeigt, dass ein gefährliches Ereignis zu einem Schaden für den Nutzer (als Bewohner, Besucher usw.) führt, wenn das gefährliche Ereignis infolge einer in einer bestimmten Betriebssituation eines Systems aufgetretenen Gefährdung entsteht und der Nutzer das gefährliche Ereignis nicht vermeiden kann. Darüber hinaus zeigt dieses Modell die Beziehung der drei Indikatoren, die zur Klassifizierung des gefährlichen Ereignisses mittels H-SIL verwendet werden (Schweregrad des Schadens S, Expositionswahrscheinlichkeit in der Betriebssituation E und Vermeidbarkeit A, um den Grad darzustellen, bis zu dem der Schaden für einen Bewohner vermieden werden kann). Die Klassifizierung des H-SIL des gefährlichen Ereignisses wird durch die Ermittlung von S, E und A nach den in 6.3.2, 6.3.3 und 6.4 beschriebenen Kriterien bestimmt. Wenn die Klassifizierung eines gefährlichen Ereignisses schwierig ist, muss sie konservativ erfolgen, d. h. wenn ein begründeter Zweifel besteht, muss ein höherer H-SIL gewählt werden. Die Klassen dürfen geändert werden, wenn die Einführung einer entsprechenden Umhüllung und/oder von für AAL geeigneten Diensten angenommen wird.

ANMERKUNG 4 Der H-SIL ist der Indikator, der bei der Klassifizierung des Auftretens von Schäden verwendet wird und gleichzeitig ein Maß für das Erreichen der funktionalen Sicherheit für eine Einheit darstellt, aus dem das System besteht. Beim Systemdesign in der Konzeptphase wird erwartet, dass sich S, E, A und H-SIL mit dem Fortschreiten des Risikominderungsprozesses ändern.

ANMERKUNG 5 Die Vermeidbarkeit ist ein Indikator, der den „Möglichkeiten der Vermeidung oder Begrenzung des Schadens“ entspricht, die in „Risikofaktoren“ beschrieben werden (QUELLE: ISO/IEC Guide 51:2014, Abschnitt 5). Der Zweck der Verwendung des Indikators „Vermeidbarkeit“ ist der richtige Umgang mit verschiedenen Situationen, einschließlich der Fähigkeit der Nutzer (Bewohner, Besucher usw.), auf gefährliche Ereignisse zu reagieren. In internationalen Normen zur funktionalen Sicherheit gibt es einen ähnlichen Indikator, und zwar die „Beherrschbarkeit“ (ISO 26262:2018).

6.3.2 Einschätzung des Schweregrads des Schadens

Mögliche schädliche Auswirkungen können sich durch die Betrachtung möglicher Fehlfunktionen und systematischer Ausfälle unter einschlägigen Betriebsbedingungen abgeleitet werden. Der mögliche Schweregrad eines Schadens wird für jedes entsprechende Szenario so genau wie möglich beschrieben. Bei der Beschreibung der Schäden muss eine bestimmte Klassifizierung verwendet werden. Aus diesem Grund erfolgt eine Klassifizierung des Schweregrads des Schadens in fünf Klassen: S0, S1, S2, S3 und S4 (siehe [Tabelle 2](#)).

Der Betreiber der betreffenden Einheit und andere Beteiligte (z. B. Hilfspersonen, andere Betreiber der Einheit, Nutzer des Hauses usw.) müssen in eine genaue Beschreibung des Schadens einbezogen werden.

Bei der Untersuchung des Risikos hinsichtlich der Sicherheitsfunktionen steht die Entstehung der Verletzungen von Personen im Vordergrund. Wenn bei der Analyse eines möglichen Schadens festgestellt werden kann, dass sich die Beschädigung eindeutig auf den Besitz beschränkt und keine Personen verletzt werden, wäre dies kein Grund für eine Klassifizierung als eine sicherheitsbezogene Funktion. Mit der Einführung der Schadensklassifizierung S0 wird diesem Umstand Rechnung getragen. Für Funktionen, die der Schadensklasse S0 zugeordnet werden, muss keine weitere Gefährdungsanalyse und Risikobewertung durchgeführt werden.

Der Schweregrad des Schadens muss für alle Nutzer der Einheit ermittelt werden. Er muss dem Risikomodell in IEC 61508-5:2010, [Anhang C](#), entsprechen. Darüber hinaus wird in diesem Dokument die Kategorie „Keine“ hinzugefügt. Der Schweregrad des Schadens muss durch den Schweregrad der Verletzung bestimmt werden, die als Ergebnis eines Unfalls während der Nutzung einer Einheit erwartet werden kann.

[Tabelle 2](#) zeigt außerdem ein Beispiel für die Klassifizierung des Schweregrads eines Schadens.

Tabelle 2 – Klassifizierung des Schweregrads eines Schadens

Schweregrad	S0	S1	S2	S3	S4
Grad der Verletzung	Keine	Vernachlässigbar	Geringfügig	Kritisch	Katastrophal
Beispiele: - Schaden für einen Bewohner	Keiner	Leichte Verletzung	Ambulante Behandlung	Schwere Verletzung, stationäre Behandlung notwendig	Tod

6.3.3 Einschätzung der Expositionswahrscheinlichkeit in Betriebssituationen

Eine Gefährdungsanalyse und Risikobewertung spiegelt die Auswirkungen möglicher Ausfälle in bestimmten Betriebssituationen wider. Diese Situationen reichen von täglichen Routineaktivitäten bis hin zu extremen, seltenen Situationen. Die Schätzung der Wahrscheinlichkeit einer Exposition in diesen Situationen wird durch die Bewertung der Szenarios bestimmt, die durch die Umgebungsfaktoren, die Gefährdungen verursachen, hervorgerufen werden. Die bewerteten Szenarios umfassen eine Vielzahl von Betriebssituationen. Die Exposition muss in sechs Klassen eingeteilt werden, die mit E0, E1, E2, E3, E4 und E5 bezeichnet werden (Tabelle 3). Die Expositionswahrscheinlichkeit in den Betriebssituationen entspricht dem Risikomodell in IEC 61508-5:2010, Anhang C.

Tabelle 3 zeigt außerdem ein Beispiel für die Expositionsklassifizierung von Schäden.

Tabelle 3 – Klassifizierung der Expositionswahrscheinlichkeit in Betriebssituationen hinsichtlich der Dauer

Expositions-klasse	E0	E1	E2	E3	E4	E5
Grad der Wahrscheinlichkeit	Unvorstellbar	Unwahrscheinlich	Sehr unwahrscheinlich	Gelegentlich	Wahrscheinlich	Häufig
Beispiel: Häufigkeit der Rückrufe [1/h]	weniger als 10 ⁻⁸	10 ⁻⁷ bis 10 ⁻⁸	10 ⁻⁶ bis 10 ⁻⁷	10 ⁻⁵ bis 10 ⁻⁶	10 ⁻⁴ bis 10 ⁻⁵	Über 10 ⁻⁴
ANMERKUNG Für jede spezifische Situation oder für vergleichbare Branchen würde eine Tabelle ähnlich der Tabelle 3 entwickelt werden, die eine Vielzahl von sozialen, politischen und wirtschaftlichen Faktoren berücksichtigt.						

6.4 Erläuterung der Zuordnung der Vermeidbarkeit

6.4.1 Schätzung der Vermeidbarkeit

Die Vermeidbarkeit wird durch die Betrachtung des Grads der Vermeidbarkeit eines Risikos für einen Bewohner in einer bestimmten Situation geschätzt. Dabei wird der Fall mit Bewohnern betrachtet, die pflegerisch betreut werden. Für eine solche Situation sieht dieses Dokument vor, dass die Vermeidbarkeit nicht nur durch die Betrachtung der Fähigkeiten der Bewohner, sondern auch durch die Betrachtung der Verfahren zur Bereitstellung der Sicherheit aus der AAL-Sicht für Heimsysteme eingeschätzt werden muss. Beispiele hierfür sind die Verwendung von benutzerfreundlichen Materialien, eine barrierefreie Gestaltung, ein regionaler Hilfsdienst, durch den im Notfall ein Helfer zum Bewohner gehen kann, externe Dienste von medizinischen Einrichtungen oder intelligente Städte (Smart Cities), die für eine Schadensvermeidung ausgelegt sind, usw. Vermeidbarkeit kann folglich als ein Kennwert definiert werden, der eine bestimmte Hilfsituation einschließt.

Es wurden vier Klassifizierungen aufgestellt, mit denen die Vermeidbarkeit von Schäden bemessen werden kann. Die Klassifizierungen A0, A1, A2 und A3 stehen für „vermeidbar/steuerbar“, „leicht vermeidbar/steuerbar“, „möglich vermeidbar/steuerbar“ und „unmöglich/schwer vermeidbar/steuerbar“ (siehe [Tabelle 4](#)).

[Tabelle 4](#) zeigt außerdem ein Beispiel für die Klassifizierung der Vermeidbarkeit von Schäden.

Tabelle 4 – Klassifizierung der Vermeidbarkeit von Schäden

Klasse der Vermeidbarkeit	A0	A1	A2	A3
Grad der Vermeidbarkeit	vermeidbar/steuerbar	leicht vermeidbar/steuerbar	möglich vermeidbar/steuerbar	unmöglich/schwer vermeidbar/steuerbar
Beispiele	Erwartungsgemäß für jeden selbstständig oder mit Hilfe zu vermeiden Erwartungsgemäß für jeden sofort zu vermeiden Erwartungsgemäß für jeden zu vermeiden	Erwartungsgemäß für fast jeden selbstständig oder mit Hilfe zu vermeiden Erwartungsgemäß für fast jeden sofort zu vermeiden Erwartungsgemäß für fast jeden zu vermeiden (90 %)	Erwartungsgemäß für viele selbstständig oder mit Hilfe zu vermeiden Erwartungsgemäß für viele in angemessener Zeit zu vermeiden Erwartungsgemäß für 70 % zu vermeiden	Erwartungsgemäß für viele selbstständig oder mit Hilfe nicht zu vermeiden Erwartungsgemäß für viele in angemessener Zeit nicht zu vermeiden Erwartungsgemäß für weniger als 50 % zu vermeiden

In einem Fall, der schwache Personen wie Behinderte oder ältere Menschen einschließt, wird eine erneute Schätzung der Vermeidbarkeit in Bezug auf die Situationen dringend empfohlen.

6.4.2 Beziehung zwischen Vermeidbarkeit und AAL-Benutzerdomäne

Es wird empfohlen, die Vermeidbarkeit basierend auf der AAL-Benutzerdomäne zu überprüfen, um die körperlich Schwachen hinsichtlich der AAL-Aspekte zu berücksichtigen. Beispielsweise wird die Vermeidbarkeit für den Nutzer in Stufe 2 in der AAL-Benutzerdomäne um einen Rang höher eingeschätzt als in Stufe 0 oder 1. Auf die gleiche Weise wird die Vermeidbarkeit für den Nutzer in Stufe 3 in der AAL-Benutzerdomäne um zwei Ränge höher eingeschätzt als in Stufe 0 oder 1 (siehe [Tabelle 5](#)).

Tabelle 5 – Einstufung der AAL-Benutzerdomänen für die Schätzung der Vermeidbarkeit

AAL-Benutzerdomäne	Stufe 0 Unabhängig	Stufe 1 Etwas Unterstützung	Stufe 2 Unterstützung der IADLs	Stufe 3 Unterstützung der ADLs
AAL-Systembetrieb	AAL-System läuft, um den unabhängigen AAL-Nutzer zu unterstützen	AAL-System läuft unter der Aufsicht des AAL-Nutzers	AAL-System läuft automatisch, erfordert aber Reaktionen vom AAL-Nutzer	AAL-System läuft automatisch ohne Aufsicht des AAL-Nutzers
Gesundheitsmanagement	Selbstüberwachung	Etwas externe Überwachung erforderlich	IADL-Überwachung erforderlich	IADL-Management erforderlich
Umfang der Unterstützung	Unabhängig	Soziale Unterstützung oder Nothilfe	Soziale und/oder gesundheitliche Unterstützung	Soziale und gesundheitliche Unterstützung

AAL-Benutzerdomäne	Stufe 0 Unabhängig	Stufe 1 Etwas Unterstützung	Stufe 2 Unterstützung der IADLs	Stufe 3 Unterstützung der ADLs
Zeitungsfang	Unabhängig	Teilzeit	Teilzeit und/oder Vollzeit	Vollzeit
Aktive Unterstützung	Unabhängig	Nur bei zusätzlichen Alltagsaktivitäten	Benötigt für instrumentelle Alltagsaktivitäten	Benötigt für Alltagsaktivitäten oder medizinische Unterstützung
Unterstützung des sozialen Lebens	Unabhängig	Nur bei zusätzlichen Alltagsaktivitäten	Benötigt bei Alltagsaktivitäten	Benötigt bei Alltagsaktivitäten
Anpassung der Vermeidbarkeit	Keine Anpassung	Keine Anpassung	+1	+2

Die AAL-Benutzerdomäne wird im System berücksichtigt, weil das System den AAL-Nutzer als Nutzer des Systems annimmt. Unter der Annahme, dass der AAL-Nutzer der Systemnutzer ist, muss das Systemdesign mit ausreichender Sicherheit ausgelegt werden. Wenn als Systemnutzer ein Nutzer mit der AAL-Benutzerdomäne der Stufe 2 oder der Stufe 3 angenommen wird, ist es nicht möglich, einen systematischen Ausfall zu verursachen, so dass es notwendig ist, den Grad der Vermeidbarkeit genau zu erfassen, was sich im H-SIL eines Elements widerspiegelt.

Damit wird sichergestellt, dass es umso schwieriger ist, den Schaden zu vermeiden, je höher die Stufe der AAL-Benutzerdomäne ist.

Im System, in dem als Systemnutzer nur Nutzer der AAL-Benutzerdomäne der Stufe 0 angenommen werden, ist es nicht notwendig, bei der Bewertung der Vermeidbarkeit die Stufe der AAL-Benutzerdomäne zu berücksichtigen, aber es ist wünschenswert anzugeben, dass nur diejenigen mit der Stufe 0 der AAL-Benutzerdomäne als Systemnutzer angenommen werden.

6.5 Bestimmung des H-SIL

Wie in [Tabelle 6](#) angegeben, wird der erforderliche H-SIL durch die Kombination des Schweregrads des Schadens der festgestellten Gefährdungen, der Wahrscheinlichkeit der Exposition in Betriebssituationen und der Vermeidbarkeit des Schadens bestimmt.

Die geforderten H-SIL-Werte werden von H-SIL A bis H-SIL D bezeichnet. H-SIL A stellt die niedrigsten und H-SIL D die höchsten Anforderungen an das System. Mit anderen Worten stellt H-SIL D die strengsten Sicherheitsanforderungen. Zusätzlich zu diesen Stufen gibt es eine Bezeichnung des Qualitätsmanagements QM, deren stillschweigende Anforderung es ist, die Systementwicklung in Übereinstimmung mit Normen wie ISO 9001 durchzuführen. Eine Funktion, die als QM eingestuft ist, darf nicht als eine sicherheitsbezogene Funktion betrachtet werden.

Tabelle 6 – Bestimmung des H-SIL

S (Schweregrad)	E (Exposition)	A (Vermeidbarkeit)			
		A0	A1	A2	A3
S0	E0	QM	QM	QM	QM
	E1	QM	QM	QM	QM
	E2	QM	QM	QM	QM
	E3	QM	QM	QM	QM