

	DIN IEC 63168-1 (VDE 0750-34-1)	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

EntwurfErsatz für
E DIN IEC 63168 (VDE
0750-34-1):2019-05

**Kooperative Mehrfachsysteme in vernetzten Wohnumfeldern –
AAL Anforderungen an funktionale Sicherheit von elektronischen
sicherheitsbezogenen Systemen –
Teil 1: Allgemeine Anforderungen an Design und Entwicklung
(IEC SyCAAL/207/CDV:2021);
Text Deutsch und Englisch**

Cooperative multiple systems in connected home environments –
AAL functional safety requirements of electronic safety-related systems –
Part 1: General requirements for design and development
(IEC SyCAAL/207/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 107 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.....	15
5 Gesamtsicherheitsmanagement.....	15
5.1 Ziele.....	15
5.2 Allgemeines.....	17
5.2.1 Einführung in das Konzept des Sicherheitslebenszyklus.....	17
5.2.2 H-SIL-Konzept.....	17
5.2.3 Externe Maßnahmen zur funktionalen Sicherheit.....	18
5.2.4 Allgemeine Anforderungen für die Anwendung von IEC 63168 (alle Teile).....	18
5.3 Erforderliche Informationen für das Gesamtsicherheitsmanagement.....	18
5.4 Anforderungen und Empfehlungen.....	18
5.4.1 Funktionale Sicherheitskultur.....	18
5.4.2 Kontinuierliche Verbesserung.....	18
5.4.3 Schulung und Qualifizierung.....	19
5.4.4 Sicherheitsmanagement während der Entwicklung.....	19
5.4.5 Zuweisung von Sicherheitsverantwortlichkeiten.....	19
5.4.6 Aufgabenzuordnung.....	19
5.4.7 Planung aller Aktivitäten des Sicherheitsmanagements während der Entwicklung.....	19
5.5 Arbeitsergebnis.....	22
6 Sicherheitsmanagement während der Konzeptphase und der Produktentwicklung.....	22
6.1 Ziele.....	22
6.2 Informationen, die für das Sicherheitsmanagement während der Konzeptphase und der Produktentwicklung erforderlich sind.....	22
6.3 Anforderungen.....	22
6.3.1 Einheit und Umgebungsbedingungen.....	22
6.3.2 Grenzen der Einheit und ihre Schnittstellen zu anderen Einheiten.....	23
6.3.3 Beanspruchungsquellen.....	23
6.3.4 Zusätzliche Festlegungen.....	23
6.4 Arbeitsergebnisse.....	23
7 Aktivitäten des Sicherheitsmanagements nach Produktionsbeginn.....	23
7.1 Ziele.....	23
7.2 Voraussetzung für Aktivitäten des Sicherheitsmanagements nach Produktionsbeginn.....	24

7.3	Anforderungen.....	24
7.3.1	Management der Produkte und Modifikationsverfahren.....	24
7.3.2	Aufgaben zur Vorbereitung und Durchführung von Produktions- und Endkontrolle.....	24
7.3.3	Aufgaben für den sicheren Betrieb und die Außerbetriebnahme von Einheiten.....	24
7.4	Arbeitsergebnisse.....	24
8	Herstellung und Installation von sicherheitsbezogenen Systemen.....	24
8.1	Ziele.....	24
8.2	Allgemeines.....	25
8.3	Für die Herstellung und Installation von sicherheitsbezogenen Systemen erforderliche Informationen.....	25
8.4	Anforderungen.....	25
8.4.1	Produktionsplan.....	25
8.4.2	Prüfplan.....	25
8.4.3	Herstellung und Prüfung.....	25
8.4.4	Prozessfähigkeit.....	25
8.4.5	Prüfberichte.....	25
8.4.6	Nichteinhaltung.....	26
8.4.7	Rückverfolgbarkeit.....	26
8.4.8	Lager- und Transportbedingungen.....	26
8.4.9	Modifikation.....	26
8.5	Arbeitsergebnisse.....	26
Anhang A (informativ) Beispiele für Systemanalysen der Sicherheit anhand eines Anwendungsfalls – Verwendung der AAL-Anwendungsfallvorlage.....		27
A.1	Ziele.....	27
A.2	Auf dem Anwendungsfall basierende Aktivitäten zur Systemanalyse für die Sicherheit.....	27
A.2.1	Ziele.....	27
A.2.2	Vorbereitung vor dem Schreiben des Anwendungsfalls mit der AAL-Anwendungsfallvorlage.....	27
A.2.3	Schreiben mit AAL-Anwendungsfallvorlage.....	29
A.2.4	Durchführung von Sicherheitsaktivitäten einschließlich Diskussionen unter Anwendung des AAL-Anwendungsfalls.....	30
A.3	Beispiel für einen Anwendungsfall: Intelligente Beleuchtungskörper.....	30
A.3.1	Allgemeines.....	30
A.3.2	Vorbereitung vor dem Schreiben des Anwendungsfalls mit der AAL-Anwendungsfallvorlage.....	30
A.3.3	Erstellung eines Anwendungsfalls durch Ausfüllen einer AAL-Anwendungsfallvorlage für dieses Beispiel.....	33
A.3.4	AAL-Anwendungsfall dieses Beispiels.....	34
A.4	Beispiel für einen Anwendungsfall: Anzeigesystem für die Bewegungsführung in Innenräumen und automatischer Roboterreiniger.....	42
A.4.1	Allgemeines.....	42
A.4.2	Vorbereitung vor dem Schreiben des Anwendungsfalls mit der AAL-Anwendungsfallvorlage.....	43
A.4.3	Erstellung eines Anwendungsfalls durch Ausfüllen einer AAL-Anwendungsfallvorlage für dieses Beispiel.....	43

A.4.4	AAL-Anwendungsfall dieses Beispiels.....	46
	Anhang B (informativ) Liste der Veröffentlichungen zur funktionalen Sicherheit kooperativer Systeme in vernetzten Wohnumfeldern.....	53
B.1	Ziele.....	53
B.2	Liste der internationalen Normen.....	53
	Anhang C (informativ) Checkliste für technische Unterlagen.....	56
	Literaturhinweise	58
Bilder		
	Bild 1 – Kooperative Mehrfachsysteme.....	6
	Bild 2 – Sicherheitslebenszyklus.....	7
	Bild 3 – Iterativer Prozess für den Entwurf sicherheitsbezogener Komponenten von Steuerungssystemen.	16
	Bild 4 – Sicherheitslebenszyklus (Wiederholung).....	17
	Bild A.1 – Systemdiagramm des Beispiels.....	31
	Bild A.2 – Systemdiagramm des Beispiels.....	43
	Bild A.3 – Anwendungsfalldiagramm des Beispiels.....	46
Tabellen		
	Tabelle 1 – Struktur von IEC 63168 (alle Teile)/betreffende Leser jedes Teils.....	8
	Tabelle 2 – Verifizierungsmaßnahmen – Sicherheitsaudit, Sicherheits-Review und Sicherheitsbewertung... ..	21
	Tabelle B.1 – Liste der Veröffentlichungen zur funktionalen Sicherheit kooperativer Systeme in vernetzten Wohnumfeldern.....	53
	Tabelle C.1 – Checkliste für technische Unterlagen.....	56

Nationales Vorwort

Das internationale Dokument IEC SyCAAL/207/CDV:2021-01 „Cooperative multiple systems in connected home environments – AAL functional safety requirements of electronic safety-related systems – Part 1: General requirements for design and development“ (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 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) stellt einen Rahmen für Lebenszyklusprozesse mit Aktivitäten und Aufgaben bereit, die für die Sicherheitskonzeption und Instandhaltung von kooperativen Mehrfachsystemen in vernetzten Wohnumfeldern erforderlich sind.

In vernetzten Wohnumfeldern werden Mehrfachsysteme über ein Netzwerk verbunden. Zwischen den jeweiligen Systemen werden verschiedene Informationen einschließlich Betriebsanweisungen ausgetauscht. Jedes System bestimmt anhand der erfassten Informationen seinen Betriebsinhalt und führt ihn aus. Bild 1 zeigt die Beziehung zwischen jedem System und kooperativen Mehrfachsystemen in vernetzten Wohnumfeldern. Bei der Sicherheitskonzeption jedes Systems ist es notwendig, die Funktionsweise aller Systeme im vernetzten Wohnumfeld zu verstehen und das Auftreten von Risiken auf ein sozial verträgliches Maß zu reduzieren.

ANMERKUNG 1 Die Umschreibung „sozial verträgliches Maß“ bezeichnet das Maß des Risikos, das in einem bestimmten Zusammenhang nach den gültigen Wertvorstellungen der Gesellschaft akzeptiert wird.

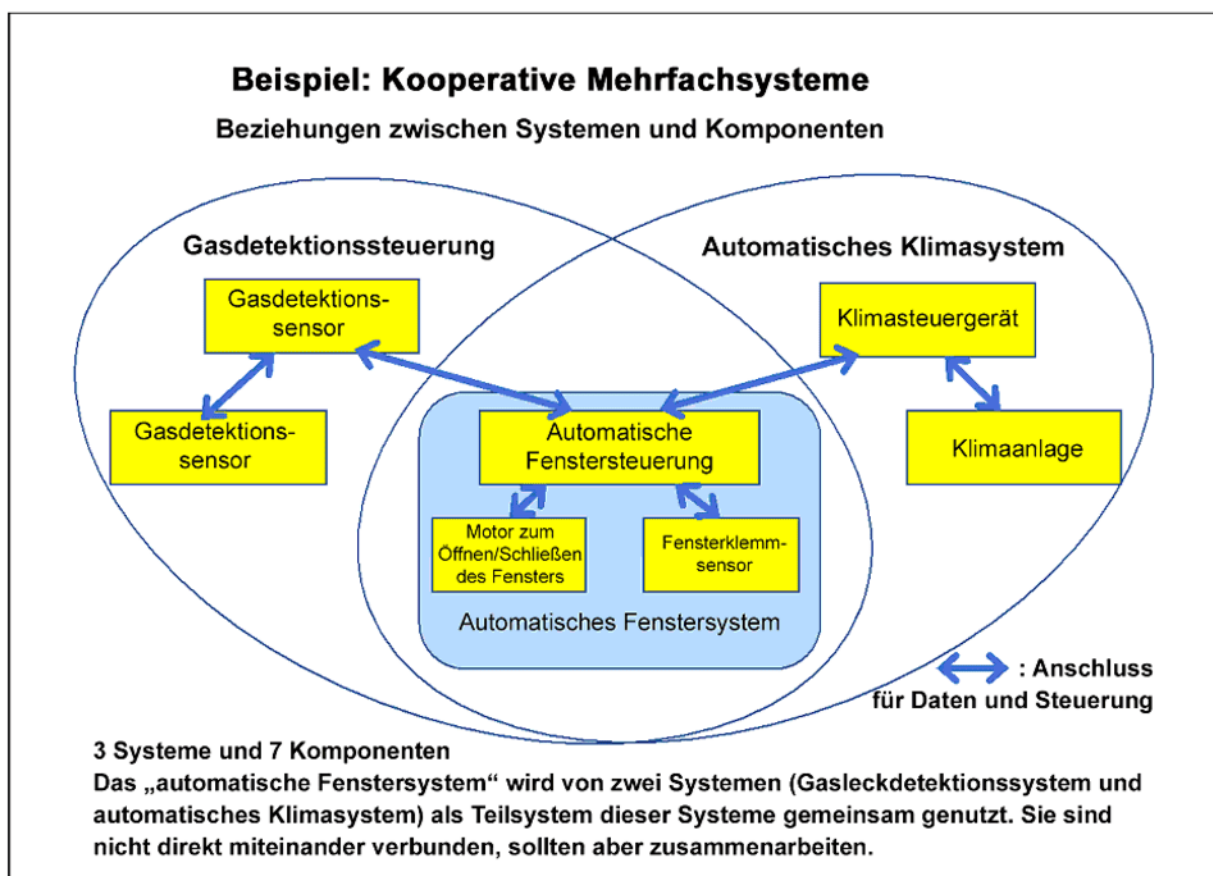


Bild 1 – Kooperative Mehrfachsysteme

Nutzer in vernetzten Wohnumfeldern, einschließlich Bewohner, Besucher und Helfer, betätigen das System direkt und/oder indirekt und sind von den Aktionen, die das System ausführt, betroffen. Bei der Sicherheitskonzeption zur Realisierung des sicheren Betriebs der Systeme ist zu berücksichtigen, dass als Nutzer auch Personen einbezogen werden, die im Leben Hilfe von anderen benötigen, wie Kleinkinder und ältere Menschen.

IEC 63168 (alle Teile) legt AAL-spezifische, sicherheitsbezogene Anforderungen an kooperative Mehrfachsysteme fest, die gemeinsam in einem vernetzten Wohnumfeld betrieben werden. IEC 63168 (alle Teile) darf auch für nicht kooperative Systeme im vernetzten Wohnumfeld angewendet werden, die bezüglich der Sicherheitskonzeption nicht zum Anwendungsbereich anderer Normen, Vorschriften oder Gesetze gehören.

IEC 63168 (alle Teile) enthält die Festlegungen:

- für den Sicherheitslebenszyklus kooperierender Systeme in vernetzten Wohnumfeldern (siehe Bild 2);
- für die Aktivitäten und Aufgaben, die in jeder Phase des Sicherheitslebenszyklus erforderlich sind;
- für den Sicherheits-Integritätslevel für vernetzte Wohnumfelder, der die Eigenschaften der Nutzer berücksichtigt, insbesondere die Notwendigkeit der Unterstützung durch andere; und
- für die Risikominderungsprozesse des kooperativen Systems unter Verwendung der Sicherheits-Integritätslevel für vernetzte Wohnumfelder.

ANMERKUNG 2 In jeder Phase sind Überlegungen zur Harmonisierung der einschlägigen Normen erforderlich.

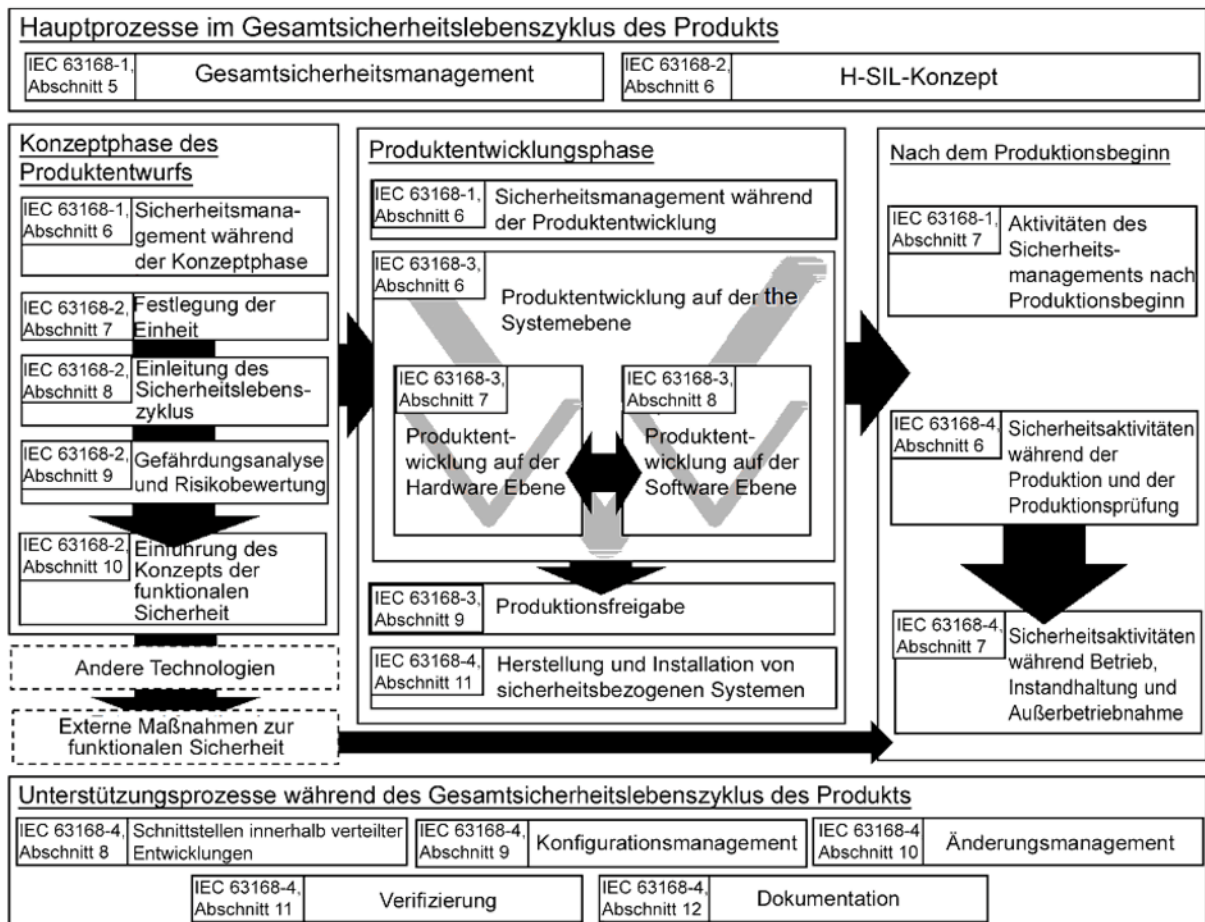


Bild 2 – Sicherheitslebenszyklus

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 Entwurf und Entwicklung	Alle mit Sicherheitsfragen in einem vernetzten Wohnumfeld Beschäftigten
2	Konzeptphase des Produktentwurfs	Planer 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, Planer von kooperativen Systemen in einem vernetzten Wohnumfeld

ANMERKUNG 3 Zu Instandhaltungsdienstleistern gehören auch Organisationen von Instandhaltungsdienstleistern.

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, Richtlinien, Gesetze usw. geregelt werden. Die Elemente ohne Anbindung an kooperative Mehrfachsysteme gehören nicht zum Anwendungsbereich dieses Dokuments.

Es ist bekannt, dass einschlägige Normen, Gesetze und Vorschriften bei einigen Produkten besondere Anforderungen an die funktionale Sicherheit der betreffenden Produkte stellen können, die die Anforderungen der Norm IEC 63168 (alle Teile) einschließen oder ergänzen. Es wird ein sich gegenseitig ergänzender und harmonisierter Ansatz empfohlen, um IEC 63168 (alle Teile) ohne Widersprüche zu diesen Normen, Gesetzen und Vorschriften anzuwenden.

ANMERKUNG 4 Hinsichtlich der Sicherheit einzelner Produkte oder Systeme in kooperativen Mehrfachsystemen werden die einschlägigen internationalen Normen (z. B. IEC 60335 (alle Teile) für Haushaltsgeräte), Gesetze und Vorschriften herangezogen.

ANMERKUNG 5 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.

ANMERKUNG 6 Siehe [Anhang B](#) zu internationalen Sicherheitsnormen.

Kooperative Mehrfachsysteme in vernetzten Wohnumfeldern – AAL Anforderungen an funktionale Sicherheit von elektronischen sicherheitsbezogenen Systemen – Teil 1: Allgemeine Anforderungen an Design und Entwicklung

1 Anwendungsbereich

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.

Die AAL-spezifischen Anforderungen an die funktionale Sicherheit sind:

- AAL-spezifische Festlegungen des Sicherheits-Integritätslevels (SIL), die verschiedene Eigenschaften von AAL-Nutzern berücksichtigen; und
- ein Gefährdungsanalyse- und Risikobewertungsverfahren unter Verwendung des AAL-spezifischen SIL.

Diese kooperativen Mehrfachsysteme können von AAL-Nutzern betrieben werden, die unter Umständen nicht vollständig ausgebildet sind.

Die 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.

Dieses Dokument legt allgemeine Anforderungen an die AAL-spezifische funktionale Sicherheit für Entwurf und Entwicklung von elektrischen/elektronischen (E/E) sicherheitsbezogenen Systemen für kooperative Mehrfachsysteme fest, die gemeinsam in einem vernetzten Wohnumfeld betrieben werden.

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 – Part 1: Vocabulary*

IEC 60050-871:2018, *International electrotechnical vocabulary – Part 871: Active assisted living (AAL)*

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 63168-2:20XX, *Cooperative multiple systems in connected home environments – AAL functional safety requirements of electrical/electronic safety related systems – Part 2: Concept phase of product design*

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 folgenden Begriffe.

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

AAL-Komponente

Gegenstand, der einzeln oder in Kombination mit Zubehörteilen oder Software zu einem einwandfreien Funktionieren der vom Hersteller bestimmten Anwendung eines AAL-Systems zum technikunterstützten Ausgleich für Menschen mit Gesundheitsproblemen beiträgt

[QUELLE: IEC 60050-871:2018, 871-04-02, modifiziert – Anmerkung 1 zum Begriff wurde gestrichen.]

3.2

AAL-Nutzer

Person, die AAL-Geräte, -Systeme oder -Dienstleistungen anwendet und/oder aus ihnen Nutzen zieht

[QUELLE: IEC 60050-871:2018, 871-02-05]

3.3

Audit

Prüfung eines implementierten Prozesses in Bezug auf die Prozessziele

[QUELLE: ISO 26262-1:2018, 3.5]

3.4

vernetztes Wohnumfeld

Wohnumfeld, das ein Heimnetzwerk bereitstellt (IEV 732-10-01), um sicherzustellen, dass Geräte innerhalb des Hauses miteinander und mit Geräten außerhalb des Hauses kommunizieren können

3.5

kooperative Mehrfachsysteme

Systeme, die mit einer möglichen wechselseitigen Beeinflussung funktionieren

3.6

elektrisches und/oder elektronisches System

E/E-System

System, das aus elektrischen oder elektronischen Elementen besteht, einschließlich programmierbarer elektronischer Elemente

Anmerkung 1 zum Begriff: Ein Element eines E/E-Systems kann auch ein anderes E/E-System sein.

BEISPIEL Stromversorgung; Sensor oder andere Eingabevorrichtung; Kommunikationsweg; Stellglied oder andere Ausgabevorrichtung.

[QUELLE: ISO 26262-1:2018, 3.40]

3.7

Element

System, Komponenten (Hardware oder Software), Hardware-Teile oder Software-Einheiten

Anmerkung 1 zum Begriff: Wird „Software-Element“ oder „Hardware-Element“ verwendet, bezeichnet dieser Ausdruck nur ein Element der Software bzw. nur ein Element der Hardware.

[QUELLE: ISO 26262-1:2018, 3.41, modifiziert – Anmerkung 2 zum Begriff wurde gestrichen.]

3.8

Exposition

Dauer und Häufigkeit, in der sich eine Person in einer Situation befindet, in der die potentielle Gefährdung besteht

[QUELLE: ISO 25119-1:2018, 3.14]

3.9

Ausfall

Beendigung eines beabsichtigten Verhaltens eines Elements oder einer Einheit aufgrund der Offenbarung eines Fehlzustands

Anmerkung 1 zum Begriff: Die Beendigung kann dauerhaft oder vorübergehend sein.

[QUELLE: ISO 26262-1:2018, 3.50]

3.10

Fehlzustand

Störbedingung, die dazu führen kann, dass ein Element oder eine Einheit versagt

[QUELLE: ISO 26262-1:2018, 3.54, modifiziert – Alle Anmerkungen zum Begriff wurden gestrichen.]

3.11

funktionale Sicherheit

System, das in einer Weise funktioniert, die kein unangemessenes Verletzungsrisiko für Bewohner, Besucher oder umstehende Personen darstellt

[QUELLE: ISO 25119-1:2018, 3.19, modifiziert – „Bediener oder Umstehenden“ wurde ersetzt durch „Bewohner, Besucher oder umstehende Personen“.]

3.12

Anforderung an die funktionale Sicherheit

Anforderung an eine sicherheitsbezogene Funktion des E/E-Systems

[QUELLE: ISO 25119-1:2018, 3.21, modifiziert – „E/E/PES“ wurde ersetzt durch „E/E“.]

3.13

Schaden

physische Verletzung oder Schädigung der Gesundheit von Personen

[QUELLE: ISO 25119-1:2018, 3.23]

3.14

Gefährdung

potentielle Schadensquelle

[QUELLE: ISO 25119-1:2018, 3.24]

3.15

Gefährdungsanalyse und Risikobewertung

Verfahren zur Identifizierung und Kategorisierung von Gefährdungsereignissen von Einheiten und zur Festlegung von Sicherheitszielen und H-SILs im Zusammenhang mit der Vermeidung oder Minderung der damit verbundenen Gefährdungen, um unangemessene Risiken zu vermeiden

[QUELLE: ISO 26262-1:2018, 3.76, modifiziert – „ASILs“ wurde ersetzt durch „H-SILs“]

3.16

Gefährdungsereignis

Kombination aus einer Gefährdung und einer Betriebssituation

[QUELLE: ISO 26262-1:2018, 3.77]

3.17

Wohnumfeld

Umgebung in einer Wohnung einschließlich der Gesamtheit aller Geräte (zum Beispiel Haushaltstechnik, Heimnetzwerk, Mobiliar)

[QUELLE: IEC 60050-871:2018, 871-03-02, modifiziert – „z. B.“ wurde ersetzt durch „zum Beispiel“.]

3.18

H-SIL-Aufteilung

Aufteilung von redundanten Sicherheitsanforderungen auf hinreichend unabhängige Elemente, die demselben Sicherheitszweck dienen, mit dem Ziel, den H-SIL der redundanten Sicherheitsanforderungen zu reduzieren, die den entsprechenden Elementen zugeordnet sind

[QUELLE: ISO 26262-1:2018, 3.3, modifiziert – „ASIL“ wurde ersetzt durch „H-SIL“ und alle Anmerkungen zum Begriff wurden gestrichen.]

3.19

Einheit

System oder Kombination von Systemen, für das/die IEC 63168 (alle Teile) gilt und das/die eine Funktion oder einen Teil einer Funktion auf der Ebene des vernetzten Wohnumfelds realisiert

[QUELLE: ISO 26262-1:2018, 3.84, modifiziert – „ISO 26262“ wurde ersetzt durch „IEC 63168 (alle Teile)“, „des Fahrzeugs“ wurde ersetzt durch „des vernetzten Wohnumfelds“ und Anmerkung 1 zum Begriff wurde gestrichen.]

3.20

Lebenszyklus

Gesamtheit der Phasen vom Konzept bis zur Außerbetriebnahme der Einheit

[QUELLE: ISO 26262-1:2018, 3.86]

3.21

Modifikation

Schaffung einer neuen Einheit aus einer bestehenden Einheit

Anmerkung 1 zum Begriff: Modifikation wird in der Normenreihe IEC 63168 (alle Teile) in Bezug auf die Wiederverwendung für die Anpassung des Lebenszyklus verwendet. Eine Änderung wird während des Lebenszyklus einer Einheit angewendet, während eine Modifikation angewendet wird, um eine neue Einheit aus einer bestehenden zu erschaffen.

[QUELLE: ISO 26262-1:2018, 3.91, modifiziert – „Normenreihe ISO 26262“ wurde ersetzt durch „Normenreihe IEC 63168 (alle Teile)“.]

3.22

Betriebssituation

Szenario, das während des Lebenszyklus eines vernetzten Wohnumfelds auftreten kann

[QUELLE: ISO 26262-1:2018, 3.104, modifiziert – „Lebenszyklus eines Fahrzeugs“ wurde ersetzt durch „Lebenszyklus eines vernetzten Wohnumfelds“ und das BEISPIEL wurde gestrichen.]

3.23

Review

Untersuchung eines Arbeitsergebnisses hinsichtlich des Erreichens seines Ziels entsprechend dem Zweck des Reviews

Anmerkung 1 zum Begriff: Aus Sicht der Entwicklungsphase eine Verifizierungsprüfung und eine Bestätigungsprüfung.

[QUELLE: ISO 26262-1:2018, 3.127]

3.24

Risiko

Kombination aus der Eintrittswahrscheinlichkeit des Schadens und der Schwere des Schadens

[QUELLE: ISO 26262-1:2018, 3.128]

3.25

Sicherheitsaktivität

Aktivität, die in einer oder mehreren Unterphasen des Sicherheitslebenszyklus durchgeführt wird

[QUELLE: ISO 26262-1:2018, 3.133]

3.26

Sicherheitskultur

dauerhafte Werte, Haltungen, Motivationen und Kenntnisse einer Organisation, in der bei Entscheidungen und Verhalten die Sicherheit Vorrang vor konkurrierenden Zielen hat

[QUELLE: ISO 26262-1:2018, 3.137, modifiziert – Anmerkung 1 zum Begriff wurde gestrichen.]

3.27

Sicherheitsziel

Beschreibung, wie eine bestimmte Gefährdung zu vermeiden ist

Anmerkung 1 zum Begriff: Das Sicherheitsziel ist die oberste Zielvorgabe als ein Ergebnis der Gefährdungsanalyse und Risikobewertung, aus der sicherheitsbezogene Funktionen abgeleitet werden.

Anmerkung 2 zum Begriff: Ein Sicherheitsziel kann sich auf mehrere Gefährdungen beziehen und mehrere Sicherheitsziele können sich auf eine einzelne Gefährdung beziehen.

[QUELLE: ISO 26262-1:2018, 3.44, modifiziert – Das BEISPIEL wurde gestrichen.]

3.28

Sicherheits-Integritätslevel für ein vernetztes Wohnumfeld

H-SIL

eine von vier Stufen, um die notwendigen Anforderungen der IEC 63168 (alle Teile) an die Einheit oder das Element und die anzuwendenden Sicherheitsmaßnahmen zur Vermeidung eines unangemessenen Restrisikos festzulegen, wobei A die niedrigste Stufe und D die höchste Stufe darstellt

3.29

Sicherheitslebenszyklus

notwendige Tätigkeiten im Rahmen der Realisierung von sicherheitsbezogenen Systemen während einer Dauer, die mit der Konzeptphase des Produktentwurfs beginnt und endet, wenn alle sicherheitsbezogenen E/E-Systeme und andere risikomindernde Maßnahmen nicht mehr für die Verwendung verfügbar sind

[QUELLE: IEC 61508-4:2010, 3.7.1]

3.30

Sicherheitsmanager

Person oder Organisation, die für die Überwachung und Sicherstellung der Ausführung von Aktivitäten verantwortlich ist, die zur Erreichung der funktionalen Sicherheit erforderlich sind

Anmerkung 1 zum Begriff: Auf verschiedenen Entwicklungsstufen der Einheit kann jedes beteiligte Unternehmen eine oder mehrere unterschiedliche Personen einsetzen, indem die Aufgaben entsprechend der internen Matrixorganisation aufgeteilt werden.

[QUELLE: ISO 26262-1:2018, 3.140]

3.31

Sicherheitsplan

Plan zur Verwaltung und Lenkung der Ausführung der Sicherheitsaktivitäten eines Projekts, einschließlich Daten, Meilensteine, Aufgaben, Ergebnisse, Verantwortlichkeiten und Ressourcen

[QUELLE: ISO 26262-1:2018, 3.143]

3.32

sicherheitsbezogene Funktion

Funktion, die potentiell zur Verletzung oder Erreichung eines Sicherheitsziels beitragen kann

[QUELLE: ISO 26262-1:2018, 3.145]

3.33

Schweregrad

Ausmaß eines möglichen Schadens für eine gefährdete Person unter der Annahme, dass ein Schaden aufgetreten ist

[QUELLE: ISO 25119-1:2018, 3.47]

3.34

Unterphase

Unterteilung einer Phase im Sicherheitslebenszyklus, die in einem Abschnitt von IEC 63168 (alle Teile) festgelegt ist

BEISPIEL Die Gefährdungsanalyse und Risikobewertung ist eine Unterphase des Sicherheitslebenszyklus, die in IEC 63168-2, Abschnitt 9, festgelegt ist.

[QUELLE: ISO 26262-1:2018, 3.161, modifiziert – „ISO 26262“ wurde ersetzt durch „IEC 63168 (alle Teile)“, „ISO 26262-3:2018, Abschnitt 6“ wurde ersetzt durch „IEC 63168-2, Abschnitt 9“.]

3.35

System

Gruppe von Komponenten oder Teilsystemen, die mindestens einen Sensor, eine Steuerung und ein Stellglied miteinander verbindet

Anmerkung 1 zum Begriff: Der zugehörige Sensor oder das Stellglied kann in das System eingebunden oder extern sein.

[QUELLE: ISO 26262-1:2018, 3.163]

3.36

Arbeitsergebnis

Ergebnis einer Entwurfs- oder Entwicklungsaktivität

[QUELLE: ISO 25119-1:2018, 3.57]

4 Abkürzungen

Für die Anwendung dieses Dokuments gelten die folgenden Begriffe.

SOP	Produktionsbeginn (en: start of production)
SRS	sicherheitsbezogenes System (en: safety related system)

5 Gesamtsicherheitsmanagement

5.1 Ziele

Für die Entwicklung eines sicheren E/E-Systemprodukts in vernetzten Wohnumfeldern müssen Entwickler die Auswirkungen auf die Sicherheit der kooperativen Mehrfachsysteme während des Produktlebenszyklus berücksichtigen. Zu den zu berücksichtigenden Inhalten gehören die Gefährdungsanalyse und die Risikobewertung der kooperativen Mehrfachsysteme. Da zu den Nutzern von E/E-Systemprodukten junge und ältere Menschen gehören und der Einflussbereich der kooperativen Mehrfachsysteme Besucher und Nachbarn umfasst, dürfen Entwickler gegebenenfalls eine Systemanalyse zur Sicherheit auf der Grundlage eines Anwendungsfalls durchführen.

ANMERKUNG 1 Siehe IEC 63168-2, um die Beispiele für Gefährdungsanalyse und Risikobewertung zu verstehen.

ANMERKUNG 2 Siehe [Anhang A](#), um die Beispiele der Systemanalyse für die Sicherheit auf der Grundlage eines Anwendungsfalls zu verstehen.

ANMERKUNG 3 Bei der Erstellung der Beschreibungen von Anwendungsfällen ist es wünschenswert, die in IEC TS 63134 festgelegte Vorlage für AAL-Anwendungsfälle zu verwenden, um den AAL-Aspekt zu berücksichtigen.

Das Hauptziel dieses Abschnitts besteht darin, die Verantwortlichkeiten der Personen, Abteilungen und Organisationen zu definieren, die für jede Phase während des gesamten Sicherheitslebenszyklus oder für Aktivitäten innerhalb der verschiedenen Phasen verantwortlich sind. Dies bezieht sich sowohl auf die Aktivitäten, die erforderlich sind, um das notwendige Maß an funktionaler Sicherheit für die Einheit sicherzustellen, als auch auf die Bestätigungsmaßnahmen, die dieses Maß an funktionaler Sicherheit bestätigen. Ein weiteres Ziel ist es, Managementaktivitäten während des gesamten Sicherheitslebenszyklus zu definieren.

Das E/E-System muss so konzipiert und aufgebaut sein, dass die Grundsätze der Gefährdungsanalyse und Risikobewertung und eines iterativen Prozesses zur Gestaltung sicherheitsbezogener Komponenten von Steuerungssystemen vollständig berücksichtigt werden (siehe [Bild 3](#)).

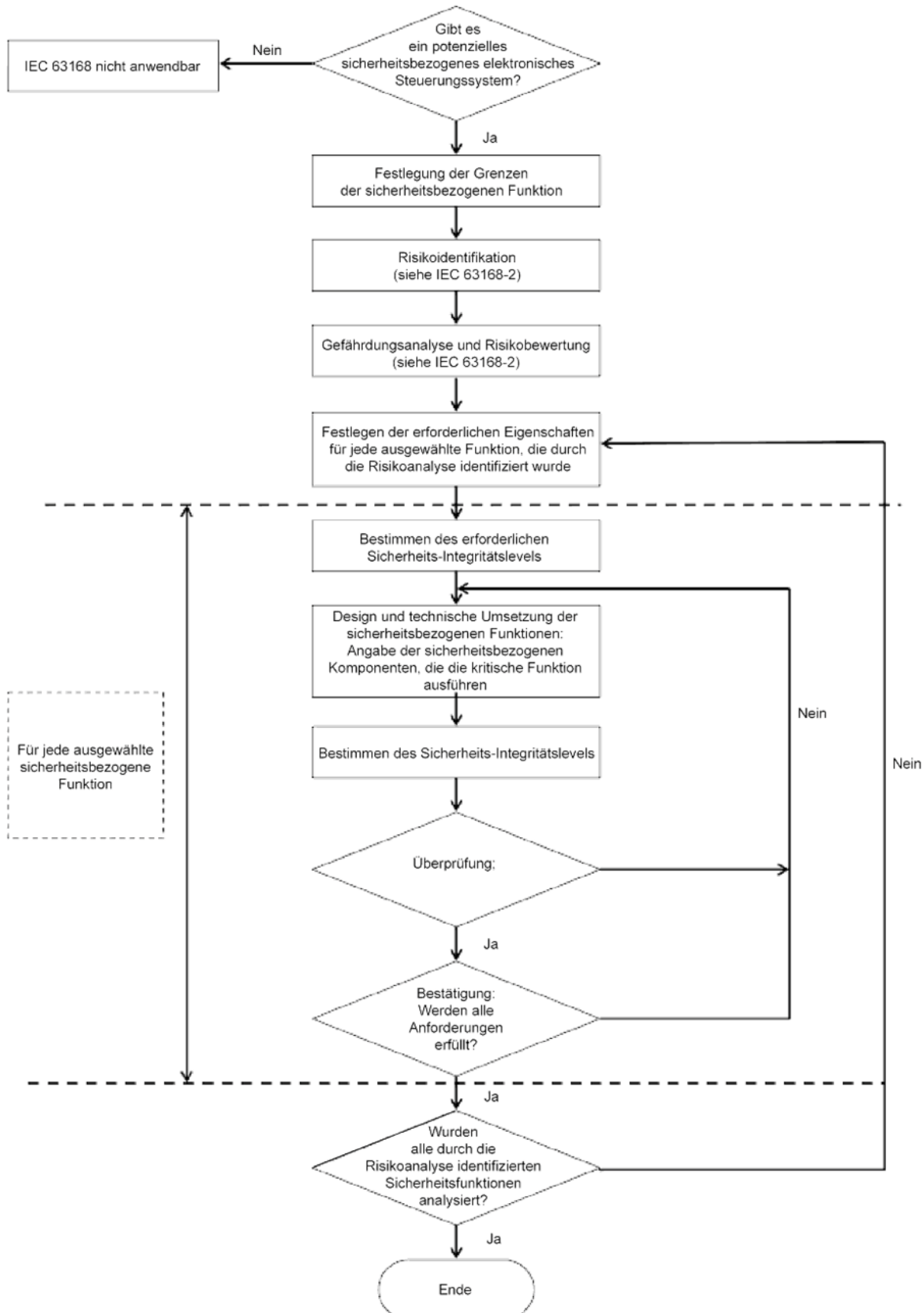
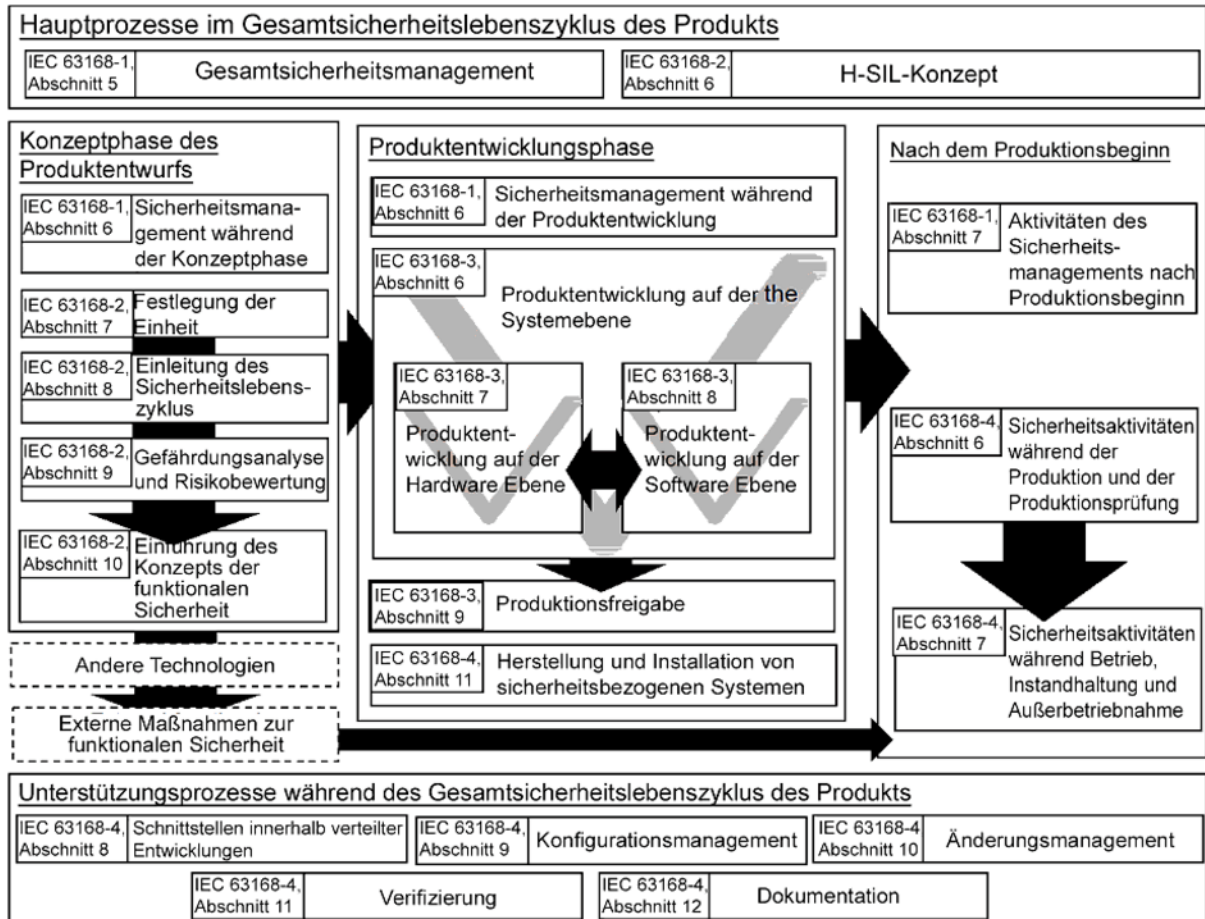


Bild 3 – Iterativer Prozess für den Entwurf sicherheitsbezogener Komponenten von Steuerungssystemen

5.2 Allgemeines

5.2.1 Einführung in das Konzept des Sicherheitslebenszyklus

Der Sicherheitslebenszyklus (siehe Bild 4) besteht aus den Sicherheitsaktivitäten in der Konzeptphase, in der Serienentwicklung und nach dem Produktionsbeginn. Diese Aktivitäten sind in IEC 63168-2, IEC 63168-3 und IEC 63168-4 ausführlich beschrieben. Die Planung, Koordinierung und Verifizierung dieser Aktivitäten über alle Phasen des Lebenszyklus hinweg sind eine zentrale Managementaufgabe.



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

Bild 4 – Sicherheitslebenszyklus (Wiederholung)

5.2.2 H-SIL-Konzept

Das Konzept des H-SIL ist in alle Sicherheitsaktivitäten im Gesamtsicherheitslebenszyklus des Systems eingebunden. Im Verfahren der Gefährdungsanalyse und Risikobewertung für einzelne Systeme, einschließlich Einheiten und Elemente, erfolgt die H-SIL-Aufteilung für alle Elemente unter Berücksichtigung von Exposition, Schweregrad und Vermeidbarkeit (einschließlich Eigenschaften des AAL-Nutzers). Eine genaue Beschreibung des H-SIL ist in IEC 63168-2 angegeben.

ANMERKUNG Die Vermeidbarkeit ist der Indikator zur Angabe des Ausmaßes, in dem ein Schaden für eine anwesende Person vermieden werden kann. Siehe IEC 63168-2, Abschnitt 6, für eine genauere Beschreibung.

Die Anforderungen oder Empfehlungen der einzelnen Unterabschnitte müssen für H-SIL A, B, C und D erfüllt werden, sofern nicht anders angegeben. Diese Anforderungen und Empfehlungen beziehen sich auf das H-SIL des Sicherheitsziels.

Wurde die H-SIL-Aufteilung in einem früheren Entwicklungsstadium nach IEC 63168-2 durchgeführt, muss das aus der Aufteilung resultierende H-SIL eingehalten werden.

5.2.3 Externe Maßnahmen zur funktionalen Sicherheit

Diese Maßnahmen können durch die in der Systemdefinition beschriebene Einheit nicht beeinflusst werden. Die externe funktionale Sicherheit umfasst die Eigenschaften der beteiligten Personen (physisch, sprachlich usw.) oder der Umwelt. Sie ist in der Systemdefinition beschrieben. Bei der Gefährdungsanalyse und Risikobewertung kann die externe funktionale Sicherheit berücksichtigt werden.

ANMERKUNG Die Vermeidbarkeit ist der Indikator zur Angabe des Ausmaßes, in dem ein Schaden für eine anwesende Person vermieden werden kann. Siehe IEC 63168-2, Abschnitt 6, für eine genauere Beschreibung.

5.2.4 Allgemeine Anforderungen für die Anwendung von IEC 63168 (alle Teile)

Wenn die Einhaltung mit IEC 63168 (alle Teile) beansprucht wird, muss jede Anforderung erfüllt werden, sofern nicht einer der folgenden Punkte zutrifft:

- a) eine Anpassung der Sicherheitsaktivitäten nach diesem Dokument wurde geplant und zeigt, dass die Anforderung nicht zutrifft, oder
- b) es liegt eine Begründung vor, dass die Nichteinhaltung zulässig ist, und die Begründung wurde nach diesem Dokument bewertet.

Die Ergebnisse der Sicherheitsaktivitäten werden als Arbeitsergebnisse angegeben.

ANMERKUNG 1 Informationen, die als „ANMERKUNG“ oder „BEISPIEL“ gekennzeichnet sind, dienen nur als Anleitung zum Verständnis oder zur Verdeutlichung der zugehörigen Anforderung. Sie werden nicht als Anforderung selbst oder als vollständig oder erschöpfend interpretiert.

ANMERKUNG 2 Siehe IEC 63168-4, Anhang A, für die Dokumente, die erforderlich sind, um die Übereinstimmung mit IEC 63168 (alle Teile) zu beanspruchen.

5.3 Erforderliche Informationen für das Gesamtsicherheitsmanagement

Die notwendigen Informationen sind ein bewährter Qualitätssicherungsplan (z. B. ISO 9001 oder vergleichbar) und ein Gesamtprojektplan.

5.4 Anforderungen und Empfehlungen

5.4.1 Funktionale Sicherheitskultur

Je nach den unterschiedlichen Wohnumfeldern, Produkten und Arten von Bewohnern in den verschiedenen Ländern sind viele Dinge zu beachten. Eine Aufgabe des Managements und aller Mitarbeiter ist es, eine Kultur zu schaffen, in der der funktionalen Sicherheit die gebührende Aufmerksamkeit geschenkt wird. Dies kann z. B. erfolgen:

- durch Formulierung der Ziele der funktionalen Sicherheit und deren Kommunikation innerhalb des Unternehmens und
- durch Überprüfung des Status von Prozessen, um die funktionale Sicherheit zu erreichen.

ANMERKUNG Zu den Mitarbeitern können Entwickler von Herstellern, Systemintegratoren und Dienstleistern gehören.

5.4.2 Kontinuierliche Verbesserung

Das Management muss die Prozesse zur kontinuierlichen Verbesserung erleichtern. Mittel dazu sind:

- die Schaffung von unternehmensspezifischen Verfahren zur Erfüllung der Anforderungen von IEC 63168 (alle Teile);
- die Bereitstellung von Werkzeugen, Vorlagen, Datenbanken und anderen Ressourcen, die die Durchführung von Sicherheitsaktivitäten unterstützen; und
- die Einholung von Rückmeldungen aus Erkenntnissen über sicherheitsbezogene Komponenten aus Projekten und Transfer dieser Erkenntnisse an die Mitglieder neuer Projektteams.

5.4.3 Schulung und Qualifizierung

Die Durchführung der Aufgaben im Sicherheitslebenszyklus erfordert entsprechend qualifiziertes Personal. Ziel muss die Aufrechterhaltung eines ausgewogenen Maßes an Kompetenz in folgenden Bereichen sein:

- technische Sicherheitskonzepte,
- Methodik und
- Kenntnisse über den Prozess der funktionalen Sicherheit und Informationen zu den Anforderungen.

5.4.4 Sicherheitsmanagement während der Entwicklung

Ziel muss es sein, alle sicherheitsbezogenen Aspekte während der Entwicklung zwischen allen beteiligten Personen, Abteilungen und/oder Lieferanten zu koordinieren.

5.4.5 Zuweisung von Sicherheitsverantwortlichkeiten

Die Planung und Durchführung von Aktivitäten, die die funktionale Sicherheit in Projekte im Anwendungsbereich von IEC 63168 (alle Teile) einbeziehen, stellt eine zentrale Managementaufgabe für die für die Einheit verantwortliche Person oder Organisation dar.

Die Verantwortung für die Einbeziehung der funktionalen Sicherheit liegt zunächst beim Projektleiter. Die sich daraus ergebenden Aufgaben können delegiert werden. Die Kommunikations- und Entscheidungswege in Bezug auf den Sicherheitsplan und die Behebung sicherheitsbezogener Mängel müssen klar definiert sein.

Dabei muss sichergestellt werden, dass Personen über ausreichende, dokumentierte Qualifikationen und Kompetenzen für ihre Aufgaben verfügen. Die erforderliche Ausbildung und Erfahrung können vom H-SIL und der Komplexität der Einheit abhängen. Entsprechend qualifizierte Personen erfüllen auch mehrere Aufgaben. Insbesondere ist es möglich, dass Aufgaben von entsprechend qualifizierten Entwicklern ausgeführt werden.

5.4.6 Aufgabenzuordnung

Das Folgende ist eine Übersicht der wesentlichen Aufgaben der funktionalen Sicherheit.

Die Aufgaben des Managements der funktionalen Sicherheit liegen in der Verantwortung eines Produktsicherheitsmanagers oder des Leiters eines vom Projektleiter benannten Sicherheitsteams.

Für die Durchführung von Sicherheitsmanagementmaßnahmen ist ein Qualitätsmanagementsystem unerlässlich. Zu den Aufgaben des Managements der funktionalen Sicherheit gehört die zeitnahe und korrekte Bereitstellung der Ergebnisse der Sicherheitsaktivitäten in allen Phasen des Entwicklungsprozesses. Die Durchführung einzelner Aufgaben kann delegiert werden.

5.4.7 Planung aller Aktivitäten des Sicherheitsmanagements während der Entwicklung

5.4.7.1 Allgemeines

Alle Sicherheitsaktivitäten während der Entwicklungsphasen des Sicherheitslebenszyklus müssen geplant werden, einschließlich mindestens der folgenden:

- Verfahren und Strategie zur Erreichung der funktionalen Sicherheit;
- Sicherstellung einer ausreichenden Qualifikation von Personen und Organisationseinheiten bei der Zuweisung und Übertragung von Sicherheitsmaßnahmen;
- Festlegung der Sicherheitsverantwortlichkeiten zwischen den Entwicklungspartnern;
- Vorkehrungen für die Einrichtung von Unterstützungsprozessen innerhalb des Projekts;
- Durchführung einer Gefährdungsanalyse und Risikobewertung nach IEC63168-2;
- Umsetzung der Sicherheitsanforderungen im Rahmen der Entwicklungsaktivitäten nach IEC 63168-2 und IEC 63168-3;
- Bestätigung durch Entwicklungspartner, dass sie die Sicherheitsanforderungen durch Bewertungen, Reviews und Audits erfüllt haben;
- Planung der Verifizierung und Bestätigung der Sicherheit in Bezug auf die Sicherheitsanforderungen nach IEC 63168-4;
- Festlegung der Aktivitäten zur Bestätigung der funktionalen Sicherheit (Audit, Review, Bewertung); und
- Einbeziehung der gesamten Projektsicherheitsaktivitäten in das projektspezifische Sicherheitsmanagement.

5.4.7.2 Erstellen von sicherheitsbezogenen Arbeitsergebnissen

Die sicherheitsbezogenen Arbeitsergebnisse müssen so verfasst werden, dass andere den angewendeten Prozess verstehen können. Arbeitsergebnisse müssen in Übereinstimmung mit den Richtlinien zur Archivierung von Unternehmensdokumenten aufbewahrt werden.

5.4.7.3 Sicherheitsplan

5.4.7.3.1 Ziele

Der Sicherheitsplan dient der systematischen Planung und Bereitstellung von Ressourcen, die für Sicherheitsaktivitäten benötigt werden. Der Betrachtungsumfang ist in der Systemdefinition unter Berücksichtigung des gesamten Lebenszyklus beschrieben.

Der Sicherheitsplan muss an das Projekt angepasst werden. Einige Aktivitäten könnten für ein bestimmtes Projekt unnötig sein oder zusätzliche Aktivitäten müssen aufgenommen werden.

Der Sicherheitsplan wird vom Produktsicherheitsmanager erstellt und vom Projektleiter umgesetzt.

Sicherheitsaktivitäten werden in die Gesamtprojektplanung einbezogen und mit den erforderlichen Ressourcen ausgestattet.

5.4.7.3.2 Inhalt des Sicherheitsplans

Der Sicherheitsplan muss alle Aktivitäten enthalten, die im Lebenszyklus festgelegt sind, d. h. unterstützende Aktivitäten, Bewertung und Managementaktivitäten. Bei Bedarf kann eine detailliertere Unterteilung vorgenommen werden.

Sicherheitsaktivitäten sind im Sicherheitsplan beschrieben. Dabei lohnt es sich, die folgenden Merkmale einer Aktivität zu beschreiben:

- Ziel(e);
- Voraussetzungen – Ergebnisse, die aus anderen Aktivitäten benötigt werden, Dokumente der geforderten Informationen;
- Verantwortliche(r);
- notwendige Ressourcen;

- Dauer, Frist; und
- Aufzeichnung der Ergebnisse.

5.4.7.3.3 Format des Sicherheitsplans

Der Sicherheitsplan kann ein eigenständiges Dokument sein oder in einen allgemeinen Projektplan integriert werden; in letzterem Fall müssen Sicherheitsaktivitäten als solche gekennzeichnet werden.

Der Sicherheitsplan kann Verweisungen auf andere Pläne enthalten. Im Allgemeinen sind Verweisungen parallelen Beschreibungen von Aktivitäten in mehreren Dokumenten vorzuziehen.

Der Sicherheitsplan muss dem Versions- und Änderungsmanagement unterzogen werden.

5.4.7.3.4 Anpassung der Aktivitäten innerhalb von Prozessen (nach H-SIL)

Die Charakteristik aller Aktivitäten ist immer abhängig vom H-SIL und dem funktionalen Sicherheitsplan für jedes Projekt.

Darüber hinaus können Aktivitäten und ganze Phasen des Lebenszyklus, die für bestimmte Projekte nicht gelten, mit entsprechender Begründung entfallen.

Bei der Erstellung des Sicherheitsplans muss darauf geachtet werden, dass die spezifischen Merkmale aller Aktivitäten an den H-SIL und die Umstände des Projekts angepasst werden.

Wenn einzelne Aktivitäten entfallen oder in reduzierter Form durchgeführt werden, muss eine klare Begründung angegeben werden.

5.4.7.3.5 Verifizierung der funktionalen Sicherheit

Die Aktivitäten zur Sicherstellung der funktionalen Sicherheit müssen das Sicherheitsaudit, das Sicherheits-Review und die Sicherheitsbewertung nach [Tabelle 2](#) umfassen.

**Tabelle 2 – Verifizierungsmaßnahmen – Sicherheitsaudit,
Sicherheits-Review und Sicherheitsbewertung**

Verifizierungsmaß- nahme	Audit	Review	Bewertung
Gegenstand	Implementierung der für die funktionale Sicherheit erforderlichen Prozesse	Ergebnis einer bestimmten sicherheitsbezogenen Aktivität	Gesamte Einheit, die in der Phase der „Systemdefinition“ beschrieben wird
Umfang und Tiefe	Vom Auditor festgelegt	Geplant vor der Durchführung des Reviews	Umfang ist die vollständige Verifizierung aller Prozesse und technischen Maßnahmen, die für die funktionale Sicherheit erforderlich sind Die Tiefe wird vom Prüfer bestimmt
Im Lebenszyklus durchzuführen	Während der Implementierung der erforderlichen Prozesse und vor Abschluss jeder Aktivität	Nach Abschluss jeder sicherheitsbezogenen Aktivität	Parallel zur Entwicklung oder in einem Block Fertigstellung vor der Serienfreigabe

Verifizierungsmaßnahme	Audit	Review	Bewertung
Verantwortlichkeit	Zur ausreichenden Verifizierung der Prozesse	Für eine ordnungsgemäße Durchführung des Reviews	Gemeinsame Verantwortlichkeit für die funktionale Sicherheit
Ergebnis	Audit-Bericht (kann Teil einer Bewertung sein)	Review-Protokoll (kann Teil einer Bewertung sein)	Erklärung zur funktionalen Sicherheit der Einheit

5.5 Arbeitsergebnis

Die Arbeitsergebnisse des Managements während des gesamten Sicherheitszyklus sind die folgenden:

- Verifizierungsmaßnahmen – Prozessanweisung zur Auditierung der Prozesse während der Serienentwicklung; und
- Sicherheitsplan.

6 Sicherheitsmanagement während der Konzeptphase und der Produktentwicklung

6.1 Ziele

Ziel dieser Phase ist es, ein angemessenes Verständnis der Einheit zu entwickeln, um alle im Sicherheitslebenszyklus definierten Aufgaben zufriedenstellend zu erfüllen. Auf der Grundlage des gewählten Sicherheitskonzepts sollte ein geeignetes Verfahren zur Bestimmung des erforderlichen Leistungsniveaus verwendet werden. Geeignete Verfahren sind die Gefährdungsanalyse und Risikobewertung (siehe unten), andere Normen, gesetzliche Anforderungen und die Expertise der Prüfstelle.

6.2 Informationen, die für das Sicherheitsmanagement während der Konzeptphase und der Produktentwicklung erforderlich sind

Die notwendigen Informationen sind eine Beschreibung der Einheit, ihrer Schnittstellen, bereits bekannte Sicherheits- und Zuverlässigkeitsanforderungen und der Anwendungsbereich.

6.3 Anforderungen

6.3.1 Einheit und Umgebungsbedingungen

Ein sicherheitsbezogenes Konzept muss Folgendes umfassen:

- a) Anwendungsbereich, Kontext und Zweck der Einheit;
- b) funktionale Anforderungen an die Einheit;
- c) andere Anforderungen an die Einheit und die Umgebungsbedingungen, einschließlich
 - technische oder physische Anforderungen, z. B. Betriebs-, Umwelt- und Umgebungsbedingungen und -beschränkungen; und
 - gesetzliche Anforderungen, insbesondere sicherheitsgezogene Gesetze, Vorschriften und Normen (national und international); und
- d) historische Sicherheits- und Zuverlässigkeitsanforderungen sowie das für ähnliche oder verwandte Einheiten erreichte Sicherheits- und Zuverlässigkeitsniveau.

6.3.2 Grenzen der Einheit und ihre Schnittstellen zu anderen Einheiten

Die folgenden Informationen müssen berücksichtigt werden, um ein Verständnis für die Funktionsweise der Einheit in ihrer Umgebung zu gewinnen:

- die Grenzen der Einheit;
- ihre Schnittstellen und Interaktionen mit anderen Einheiten und Komponenten;
- Anforderungen an andere Einheiten; und
- Zuordnung und Verteilung entsprechender Funktionen auf die eingebundenen Einheiten.

6.3.3 Beanspruchungsquellen

Die Beanspruchungsquellen, die die Sicherheit und Zuverlässigkeit der Einheit möglicherweise beeinträchtigen können, müssen bestimmt werden, einschließlich der folgenden:

- das Zusammenspiel verschiedener Einheiten;
- Gefährdungen physikalischer oder chemischer Art (Energiegehalt, Toxizität, Explosivität, Korrosivität, Reaktivität, Brennbarkeit usw.);
- andere externe Ereignisse (Temperatur, Luftfeuchte, Schock, elektromagnetische Verträglichkeit (EMV) usw.);
- vernünftigerweise vorhersehbare menschliche Bedienungsfehler;
- Gefährdungen, die von der Einheit ausgehen, und Ereignisse, die einen Ausfall auslösen (z. B. während der Montage oder Instandhaltung).

6.3.4 Zusätzliche Festlegungen

Zusätzlich zu den in 5.4.2 beschriebenen Aktivitäten müssen die folgenden Festlegungen oder Maßnahmen durchgeführt werden:

- Festlegung, ob für die Einheit im Falle einer Modifikation eine Auswirkungsanalyse durchzuführen ist, um den Sicherheitslebenszyklus entsprechend anzupassen;
- Erstellung eines Plans und einer Spezifikation zum Bestätigen der Anforderungen an die in 5.4.1 definierte Einheit;
- Festlegung des Projektmanagements für die entsprechenden Phasen des Lebenszyklus;
- ausreichende Eingangsdaten für die Zuverlässigkeitsbewertung;
- angemessene Verfahren und Anwendung von Werkzeugen und Technologien; und
- Einsatz von qualifiziertem Personal.

6.4 Arbeitsergebnisse

Die Arbeitsergebnisse des Konzepts/der Festlegung der Einheit sind:

- a) die Einheit und die Umgebungsbedingungen,
- e) Grenzen der Einheit und ihre Schnittstellen zu anderen Einheiten,
- f) Beanspruchungsquellen und
- g) zusätzliche Bestimmungen.

7 Aktivitäten des Sicherheitsmanagements nach Produktionsbeginn

7.1 Ziele

Ziel dieser Phase ist es, die Verantwortlichkeiten der für die funktionale Sicherheit nach dem Produktionsbeginn (SOP) verantwortlichen Personen, Abteilungen und Organisationen zu definieren. Dies gilt für allgemeine

Aktivitäten, die erforderlich sind, um das notwendige Maß an funktionaler Sicherheit für die Einheit sicherzustellen, sowie für die Bestätigungsmaßnahmen, die dieses Maß an funktionaler Sicherheit bestätigen.

7.2 Voraussetzung für Aktivitäten des Sicherheitsmanagements nach Produktionsbeginn

Der Hersteller sollte ein Qualitätsmanagementsystem einführen.

ANMERKUNG Das hier erwähnte Qualitätsmanagementsystem ist das gleiche, wie in 5.3 beschrieben.

7.3 Anforderungen

7.3.1 Management der Produkte und Modifikationsverfahren

In den Lebenszyklusphasen nach dem SOP müssen organisatorische Maßnahmen eingeleitet werden, um die funktionale Sicherheit aller produzierten Einheiten zu erreichen und während der gesamten Lebensdauer des Systems zu erhalten. Die technischen Anforderungen für das Erreichen und die Aufrechterhaltung der funktionalen Sicherheit in allen produzierten Einheiten während der Lebensdauer des Systems werden in der Regel bei der Entwicklung der Einheit festgelegt und können nach einem Modifikationsprozess geändert werden.

7.3.2 Aufgaben zur Vorbereitung und Durchführung von Produktions- und Endkontrolle

Die Umsetzung der Anforderungen an die Produktion/Installation/Anpassung und Schulung des Betriebspersonals muss verzeichnet und überwacht werden. Darüber hinaus muss die Serienkonformität in Bezug auf Sicherheitsanforderungen und Arbeitsergebnisse überprüft werden.

7.3.3 Aufgaben für den sicheren Betrieb und die Außerbetriebnahme von Einheiten

Die folgenden Aufgaben müssen ausgeführt werden:

- Ausarbeitung und Aufnahme besonderer Inhalte und Warnhinweise in die Betriebsanleitung;
- Aufführung der Anforderungen an das Instandhaltungs- und Herstellerwartungspersonal und Überwachung der Umsetzung;
- Rückmeldung der beobachteten Fehlzustände;
- Aufstellung der Sicherheitsanforderungen für die Außerbetriebnahme (siehe IEC 63168-4);
- Erwägen, im Qualitätsmanagementsystem dem V-Modell Meilensteine hinzuzufügen (siehe IEC 63168-3);
- für jede Phase des V-Modells muss eine Verifizierungsmaßnahme vorhanden sein; und
- Erwägen, das bestehende V-Modell im Laufe des Projekts zu verfeinern.

ANMERKUNG Das V-Modell ist die typische Methodik für die Entwicklung von E/E-Systemen. Die Erläuterung des Ausdrucks, der sich auf die funktionale Sicherheit bezieht, kann IEC 61508-3, 7.1.2.4, entnommen werden. Siehe IEC 63168-3 für weitere Einzelheiten.

7.4 Arbeitsergebnisse

Die Arbeitsergebnisse aus den Aktivitäten des Sicherheitsmanagements nach dem SOP sind spezielle Inhalte und Warnhinweise für Betriebsanleitungen.

8 Herstellung und Installation von sicherheitsbezogenen Systemen

8.1 Ziele

Die Ziele in dieser Phase sind die Entwicklung eines Produktions- und Installationsplans für ein sicherheitsbezogenes System (SRS). Ein weiteres Ziel ist die Aufrechterhaltung der geforderten funktionalen

Sicherheit während des Produktionsprozesses durch den jeweiligen Produkthersteller oder die für den Prozess verantwortliche Person/Organisation (Hersteller der Einheit, Lieferant, Unterlieferant usw.).

8.2 Allgemeines

Durch die Einbeziehung sicherheitsbezogener Merkmale in die Produktionsplanung und -kontrolle definiert diese Phase die Schritte, die erforderlich sind, um die funktionale Sicherheit auch während des Produktionsprozesses aufrechtzuerhalten.

8.3 Für die Herstellung und Installation von sicherheitsbezogenen Systemen erforderliche Informationen

Die folgenden Informationen müssen bereitgestellt werden:

- Montagehinweise – die Angabe der von der Montage betroffenen Komponenten oder Funktionen;
- Prüfhinweise und -kriterien – Informationen, die sich auf Prüfverfahren und die zu prüfenden Kriterien für die sicherheitsbezogenen Funktionen beziehen;
- Produktfreigabe – die Freigabeinformation für Produktion, Prüfung und Installation; und
- Produktüberwachung – erforderlich für sicherheitsbezogene Merkmale und die Sicherstellung, dass die sicherheitsbezogenen Eigenschaften von Komponenten im Produktionsprozess des Herstellers der Einheit nach dessen Vorgaben eingehalten werden.

8.4 Anforderungen

8.4.1 Produktionsplan

Es ist ein Produktionsplan unter Berücksichtigung der Montageanleitung zu erstellen, der Folgendes enthält:

- Identifizierung von sicherheitsbezogenen Komponenten und Merkmalen;
- Reihenfolge und Verfahren der Produktionsschritte; und
- Ausrüstung/Werkzeuge.

8.4.2 Prüfplan

Ein Prüfplan, der die Anweisungen für die Prüfung berücksichtigt, muss erstellt werden und Folgendes enthalten:

- Identifizierung von sicherheitsbezogenen Komponenten und Merkmalen – Reihenfolge und Verfahren der Prüfschritte; und
- Prüfung von Geräten/Werkzeugen, Prüfkriterien.

8.4.3 Herstellung und Prüfung

Die Herstellung und Prüfung muss von qualifiziertem Personal nach den Produktions- und Prüfplänen durchgeführt werden.

8.4.4 Prozessfähigkeit

Die Prozessfähigkeit muss durch branchenübliche Anforderungen sichergestellt werden. Die Prozessfähigkeit von Geräten/Werkzeugen und Prüfmitteln muss auch durch branchenübliche Praktiken sichergestellt werden. Die Prüfmittel müssen einem geeigneten Prozess der Prüfmittelprüfung unterzogen werden.

8.4.5 Prüfberichte

Die Durchführung der Prüfung nach dem Prüfplan muss dokumentiert werden. Die Prüfberichte müssen mindestens die folgenden Informationen enthalten:

- Datum der Prüfung;
- Prüfer;
- eindeutige Identifikation der Teile und Prüfergebnisse; und
- Einbeziehung aller Abweichungen des beobachteten vom erwarteten Verhalten.

8.4.6 Nichteinhaltung

Ein Verfahren im Fall der Nichteinhaltung eines Prüfkriteriums muss verfügbar sein. Eine Nachbearbeitung ist nur bei Nachweis der Prozesskontrolle zulässig.

8.4.7 Rückverfolgbarkeit

Die Rückverfolgbarkeit einer bestimmten Konfiguration von sicherheitsbezogenen Komponenten in einem Produkt muss während der gesamten Produktion sichergestellt sein.

8.4.8 Lager- und Transportbedingungen

Bei der Festlegung der Bedingungen für die Lagerung und Vorbereitung des Produkts für den Transport sind sicherheitsbezogene Kriterien zu berücksichtigen (siehe IEC 63168-4).

8.4.9 Modifikation

Für produktionsbedingte Modifikationen der Produkte muss eine Einflussanalyse verwendet werden, um den Schritt des Lebenszyklus zu bestimmen, zu dem zurückzukehren ist, und die Schritte, die zu wiederholen sind (IEC 63168-4).

8.5 Arbeitsergebnisse

Die Arbeitsergebnisse aus der Herstellung und Installation von sicherheitsbezogenen Systemen sind:

- Angabe der sicherheitsbezogenen Produktionsschritte (Produktionsplan);
- Prüf- und Einstellkriterien (sicherheitsbezogen);
- Angaben über Nichteinhaltung; und
- Rückverfolgbarkeit der Produkte nach sicherheitsbezogenen Kriterien.

Anhang A (informativ)

Beispiele für Systemanalysen der Sicherheit anhand eines Anwendungsfalls – Verwendung der AAL-Anwendungsfallvorlage

A.1 Ziele

Die Betrachtung der Anwendungsfälle bei der Analyse des Systems hilft, die Eigenschaften des Systems aus verschiedenen Blickwinkeln zu analysieren. Obwohl letztendlich ein oder mehrere Anwendungsfälle für das System vorgestellt werden, werden verschiedene Faktoren und deren Möglichkeiten bei der Präsentation von Anwendungsfällen berücksichtigt. Bei der Analyse des Sicherheitsaspekts des Systems muss die Sicherheit immer aus verschiedenen Blickwinkeln betrachtet werden und dies wird durch die Betrachtung des Anwendungsfalls erreicht.

In diesem Anhang werden die durchzuführenden Aktivitäten der Systemanalyse für die Sicherheit auf der Grundlage des Anwendungsfalls erläutert. Im Folgenden werden zwei Beispiele für die Systemanalyse für die Sicherheit anhand des Anwendungsfalls gezeigt. Bei der Durchführung von Gefährdungsanalysen und Risikobewertungen der kooperativen Mehrfachsysteme in einem vernetzten Wohnumfeld können Probleme durch eine Sicherheitsanalyse anhand von Anwendungsfällen geklärt werden. Die Ausführenden der Systemanalyse werden durch das Lesen des Inhalts eine Vorstellung vom Analyseverfahren des Zielsystems bekommen.

A.2 Auf dem Anwendungsfall basierende Aktivitäten zur Systemanalyse für die Sicherheit

A.2.1 Ziele

Das Ziel dieses Unterabschnitts ist es, das Verständnis der Ausführenden der Systemanalyse zu fördern, indem die Aktivitäten, die bei der Systemanalyse für die Sicherheit auf der Grundlage von Anwendungsfällen durchgeführt werden sollten, nacheinander vorgestellt werden. Der Zweck der Einführung mehrerer Systeme in ein vernetztes Wohnumfeld ist es, das Leben der Nutzer in einer Weise aktiv zu unterstützen, in der verschiedene Nutzungen denkbar sind. Die Verwendung der AAL-Anwendungsvorlage ist in der Analyse nicht vorgeschrieben, aber unter Berücksichtigung der genannten Faktoren ist die AAL-Anwendungsfallvorlage ein sehr attraktives und leistungsfähiges Werkzeug in der Systemanalyse für die Sicherheit kooperativer Mehrfachsysteme im vernetzten Wohnumfeld.

ANMERKUNG 1 Der Modellierungsrahmen des Anwendungsfalls, der so angepasst wurde, dass die menschlichen Aspekte von AAL in IEC TS 63134 berücksichtigt werden, wird wie in [IEC 62559-2](#) beschrieben benötigt.

ANMERKUNG 2 Siehe IEC TS 63134, um die Inhalte der Vorlage und der Terminologie des AAL-Anwendungsfalls zu verstehen.

A.2.2 Vorbereitung vor dem Schreiben des Anwendungsfalls mit der AAL-Anwendungsfallvorlage

A.2.2.1 Allgemeines

In [A.2.2.2](#), [A.2.2.3](#) und [A.2.2.4](#) sind drei wichtige Aktivitäten unter den Arbeiten aufgeführt, die als Vorbereitungsphase vor der Beschreibung des Anwendungsfalls mit der AAL-Anwendungsvorlage durchzuführen sind. Da diese Aktivitäten ergänzende Aspekte haben, ist es nicht notwendig, die Reihenfolge der Arbeiten einzuhalten. Es handelt sich um eine vorübergehende Reihenfolge zur Förderung einer effizienten Analyse. So kann der Ausführende beispielsweise einen fehlenden Teil der Aktivitäten zur Erläuterung des Zielsystems offenlegen, indem er die Situation, in der Probleme auftreten, betrachtet oder das Szenario

erzählerisch beschreibt. Wenn sich der Ausführende auf die Punkte der effizienten Analyse und Beschreibung von Anwendungsfällen konzentriert, kann er auch parallel Aktivitäten durchführen, die in [A.2.2.2](#), [A.2.2.3](#) und [A.2.2.4](#) beschrieben werden (z. B. Erstellung der Liste aller am Anwendungsfall beteiligten Akteure, Untersuchung zugehöriger Gesetze und internationaler Normen usw.).

A.2.2.2 Erläuterung der Zielsysteme

Bei der Erläuterung des Zielsystems ist es wünschenswert, ein Systemdiagramm zu erstellen, um die Aktivität zu erleichtern. Für die Feinheit der Teile des Systemdiagramms ist es nicht notwendig, alle Systeme bis auf die Einheitenebene zu unterteilen. Es genügt, den minimalen Systemaufbau im Zielteil zu beschreiben, anstatt das gesamte System im Systemdiagramm zu beschreiben. Bei Bedarf sollten Materialien erstellt werden, die die Beziehung zwischen dem System und den Nutzern, die Regeln für den Systembetrieb und die Zeitpläne zeigen sollten. Wie bereits erwähnt, kann bei der Arbeit der Ausführenden an den folgenden beiden Aktivitäten der Teil, der in der Aktivität „Erläuterung der Zielsysteme“ fehlte, offensichtlich werden. Es ist wünschenswert, klar erkennbare Arbeiten in der Reihenfolge auszuführen.

A.2.2.3 Berücksichtigung der Situationen, in denen Probleme auftreten

In Anbetracht der Tatsache, dass das Wohnumfeld (einschließlich des vernetzten Wohnumfelds) verschiedene Aspekte aufweist, ist es die schwierigste und wichtigste Aktivität, über Situationen nachzudenken, in denen Probleme auftreten. Es ist notwendig, das Umfeld und das Klima des Ortes, an dem das Haus gebaut ist, sowie die Gewohnheit und den Geschmack des Nutzers zu berücksichtigen (ob im Raum Schuhe getragen werden oder nicht und ob auf dem Boden gesessen wird). Es ist auch notwendig, über verschiedene Aspekte der Eigenschaften von Nutzern nachzudenken. Die Vertiefung der Analyse bei dieser Aktivität wird dazu beitragen, den Inhalt des Anwendungsfalls zu bereichern. Die wichtigsten zu berücksichtigenden Punkte sind nachfolgend aufgeführt:

- Anzahl der Stockwerke im Haus: ob es eine Treppe im Haus gibt oder nicht;
- Eigentümer des Hauses: ob im Besitz des Nutzers oder nicht;
- Wohnform: ob Mehrfamilienhaus oder Einfamilienhaus;
- Lage im Haus: Küche, Flur, Bad usw.;
- Zeitzone: Morgen, Nachmittag, Abend, Nacht, späte Nacht usw.;
- Jahreszeiten und Klima: feuchter Sommer, trockener Sommer, kalter Frühling usw.;
- Alter des Nutzers: Baby, Kind, Erwachsener oder ältere Person;

ANMERKUNG Diese Benennungen (Baby, Kind, Erwachsener oder ältere Person) sind in ISO/IEC Guide 50 und ISO/IEC 10779 definiert.

- Behinderung des Nutzers: keine Behinderung, vorübergehende Behinderung (durch Unfall oder Krankheit), dauerhafte Behinderung; und
- Aufenthaltsdauer des Nutzers: Bewohner, einmaliger Besucher (z. B. Freund, Nachbar), regelmäßiger Besucher (z. B. Betreuer, Haushälterin, Tagesmutter).

Wenn keine Situation, in der Probleme auftreten, betrachtet werden kann, wird das Zielsystem als ausreichend sicher angenommen. Es besteht jedoch die Möglichkeit, dass der Ausführende etwas übersieht, so dass ein gutes Urteilsvermögen erforderlich ist, um die gesamten Aktivitäten der Systemanalyse für die Sicherheit anhand des Anwendungsfalls abzuschließen. Selbst wenn eine ausreichende Sicherheit bei den Zielsystemen wahrgenommen wird, sollten die Aktivitäten der Systemanalyse für die Sicherheit auf der Grundlage des Anwendungsfalls in dem Sinne fortgesetzt werden, dass das Sicherheitsdenken für das Zielsystem als Anwendungsfall aufgegeben wird.

A.2.2.4 Beschreibung eines erzählerischen Szenarios

Der Vorteil der Beschreibung eines erzählerischen Szenarios liegt darin, dass ein gemeinsames Verständnis auf leicht verständliche Weise aufgebaut wird. Das Ziel ist es, keine Unstimmigkeiten im Verständnis der Anwendungsfälle zwischen den Ausführenden von Sicherheitsaktivitäten und den Lesern von Anwendungsfällen zu erzeugen. Bei der Beschreibung eines erzählerischen Szenarios ist darauf zu

achten, dass sie vollständig ist, keine benötigten Informationen fehlen, dass sie einfach und kurz ist und leicht verständlich. Die Erklärung sollte auf das erzählerische Szenario begrenzt sein. Das wichtigste ist die Erklärung des Gesamtsystems, der Umgebung und der Situation, einschließlich der menschlichen Faktoren. Bei Handlungen von Personen innerhalb des erzählerischen Szenarios sollten die Ausführenden dieser Aktivität keine Handlungen zulassen, die gegen den gesunden Menschenverstand verstoßen. Obwohl die Satzmenge im erzählerischen Szenario zwangsläufig zunehmen könnte, ist es notwendig, nicht benötigte Elemente und Beschreibungen so weit wie möglich zu zerlegen und Beschreibungen einfach und kurz zu halten. Schließlich ist es notwendig zu prüfen, ob es sich um eine für andere Leser lesbare Beschreibung handelt. Manchmal vergessen die Ausführenden, die einen Anwendungsfall betrachten, den Grad des Verständnisses anderer Leser, indem sie zu viel über einen Anwendungsfall nachdenken. Die Ausführenden sollten Gegenmaßnahmen in Betracht ziehen, wie das Lesen des bei dieser Aktivität erstellten erzählerischen Szenarios durch andere Personen.

A.2.3 Schreiben mit AAL-Anwendungsfallvorlage

A.2.3.1 Allgemeines

Mit den beschriebenen Aktivitäten ist der Aufbau der Basisteile für den eigentlichen beschreibenden Anwendungsfall abgeschlossen. Mit den folgenden Aktivitäten analysieren die Ausführenden die Teile weiter und füllen die Leerfelder in der AAL-Anwendungsfallvorlage aus. Mit diesen Aktivitäten wird der AAL-Anwendungsfall erstellt und der Aufbau des Hauptteils der Systemanalyse für die Sicherheit auf der Grundlage des Anwendungsfalls ist nahezu abgeschlossen.

Bei der Beschreibung des Anwendungsfalls anhand der AAL-Anwendungsfallvorlage in der Praxis sollten die Ausführenden darauf achten, dass sie nach genauem Lesen der Anhänge in der AAL-Anwendungsfallvorlage nicht vom Konzept der Vorlage abweichen. Die Ausführenden sollten versuchen, die Begriffe, die in den von SyC AAL herausgegebenen internationalen Normen für den Wortschatz definiert werden, und die Analyseinstrumente für AAL (wie AAL-Struktur, Liste der AAL-Akteure usw.), die von SyC AAL bereitgestellt werden, so weit wie möglich zu verwenden.

Es wird empfohlen, dass die Ausführenden zunächst unter „1.8 Darstellung des Anwendungsfalls“, „vollständige Beschreibung“, der AAL-Anwendungsfallvorlage die erzählerischen Szenarios ausfüllen müssen.

A.2.3.2 Erstellung der Liste aller Akteure des Anwendungsfalls

Bei dieser Aktivität erfassen die Ausführenden zunächst alle Personen, Einheiten, Systeme und externen Organisationen, die im erzählerischen Szenario als AAL-Akteure erscheinen. Als nächstes ist es sinnvoll, die Rollen und Beschreibungen der einzelnen Akteure sowie die Interaktion zwischen den Akteuren zu analysieren. Für die Rolle der Akteure ist es sinnvoll, eine Liste der AAL-Akteure zu erstellen, um das Verständnis zu erleichtern. Nachdem die Liste aller im Anwendungsfall enthaltenen Akteure fertiggestellt ist, wird die Liste zum Ausfüllen von „1.9 Akteure: Personen, Komponenten, Systeme, Integrierte Systeme, Anwendungen und Organisationen“ der AAL-Anwendungsfallvorlage verwendet.

A.2.3.3 Beschreibung des Anwendungsfallszenarios mit Zeichnungen oder Diagrammen, die den Anwendungsfall darstellen

Bei dieser Aktivität erstellen die Ausführenden die Zeichnungen oder Diagramme der Zielsysteme, die den Anwendungsfall durch die AAL-Anwendungsfallvorlage abbilden. Nach dem Ausfüllen der Spezifikationen der Zielsysteme in den Zeichnungen oder Diagrammen erstellen und beschreiben die Ausführenden das Anwendungsfallszenario entsprechend dem erzählerischen Szenario. In diesem Dokument wird kein spezifisches Verfahren für die Beschreibung des Szenarios angegeben. Die Beschreibung des Szenarios kann anhand des Systemdiagramms und des Zeitdiagramms erfolgen. Das Wichtigste ist, die Beschreibung des Szenarios für den Leser möglichst einfach und leicht verständlich zu halten. Die Ausführenden können nur eine Person (Personen) und eine Einheit (Einheiten) in die Liste aller Akteure aufnehmen. Die Zeichnungen und Diagramme des Zielsystems sollten so beschrieben werden, dass die Leser das Szenario zweifelsfrei verstehen können.

A.2.3.4 Analyse des Anwendungsfalls, um die Leerfelder der AAL-Anwendungsfallvorlage auszufüllen

Die für die Sicherheitsdiskussion notwendigen Elemente (Exposition, H-SIL usw.) sind in „1.13 Allgemeine Bemerkungen“ beschrieben. Die Ausführenden fassen das Ziel des Anwendungsfalls zusammen und beschreiben es in „1.7 Umfang und Ziele des Anwendungsfalls“. Für die anderen Anwendungsfälle (einschließlich AAL-Anwendungsfälle), die mit dem Anwendungsfall in Zusammenhang stehen, wenn vorhanden, beschreiben die Ausführenden das Ziel in „1.12 Zusammenhang mit anderen bekannten Anwendungsfällen“. Zu Rechtsvorschriften und internationalen Normen im Zusammenhang mit dem Inhalt des Anwendungsfalls füllen die Ausführenden „1.10 Aspekte: Rechtsgültige Verträge, Gesetzliche Vorschriften, Beschränkungen und Sonstiges (einschließlich regionaler Vorschriften)“ und „1.11 Referenznormen und/oder -normungskomitees“ entsprechend aus. Für die anderen Leerfelder der AAL-Anwendungsfallvorlage analysieren die Ausführenden den Anwendungsfall und füllen sie aus. Teile, die nicht ausgefüllt werden können, können die Ausführenden leer lassen.

A.2.4 Durchführung von Sicherheitsaktivitäten einschließlich Diskussionen unter Anwendung des AAL-Anwendungsfalls

Die Sicherheitsanalyse des Zielsystems anhand des Anwendungsfalls ist durch die bisherigen Aktivitäten nahezu abgeschlossen. Um jedoch den Mangel an Sicherheitsbedenken zu vermeiden, der aus persönlichen Annahmen und Fehleinschätzungen in der Analyse besteht, ist es wünschenswert, auf der Grundlage der erstellten Anwendungsfälle Aktivitäten zur Verringerung von Sicherheitsrisiken durchzuführen. Die Ausführenden sollten nicht vergessen, dass die Sicherheitsanalyse des Zielsystems anhand des Anwendungsfalls eine Vorbereitung eines Teils der Gefährdungsanalyse und Risikobewertung für das System ist.

ANMERKUNG Für ein Beispiel für eine Gefährdungsanalyse und Risikobewertung des Systems siehe IEC 63168-2.

A.3 Beispiel für einen Anwendungsfall: Intelligente Beleuchtungskörper

A.3.1 Allgemeines

Dieses Beispiel stellt ein Szenario dar, das in Bezug auf die Sicherheit durch die Nutzung von intelligenter Beleuchtung als unvollständiges System angesehen werden kann. Das Zielsystem besteht aus einer intelligenten Lichtquelle, einem Netzschalter, einer intelligenten Lichtsteuerung, Personensensoren, einer Uhr und einer Anwendungssoftware auf dem Smartphone.

Als Voraussetzung für das Szenario gibt es Probleme bei der Ausführung und Betriebsfehler, aber bei bestimmungsgemäßem Gebrauch gibt es keine Probleme beim ursprünglichen Nutzer. In diesem Beispiel verursachen die Ausführungsprobleme und der Betriebsausfall einen schweren Schaden, wenn der Besucher, dessen AAL-Benutzerdomäne sich vom ursprünglichen Nutzer unterscheidet, das System als zeitweiliger Nutzer bedient.

A.3.2 Vorbereitung vor dem Schreiben des Anwendungsfalls mit der AAL-Anwendungsfallvorlage

A.3.2.1 Erklärung der Zielsysteme für dieses Beispiel

Das System in diesem Beispiel sieht wie folgt aus (siehe [Bild A.1](#)):

- Ziel dieses Systems ist die intelligente Lichtsteuerung unter Verwendung von Personensensoren und Zeitdaten.
- Wenn die Bewegung einer Person um den Ort herum wahrgenommen wird, an dem die intelligente Lichtquelle aufgestellt ist, wird die intelligente Lichtquelle zu einer anderen Uhrzeit als bei Tag eingeschaltet (weil es bei Tag auch dann hell ist, wenn die Lichtquelle nicht eingeschaltet ist).
- Es gibt intelligente Lichtquellen an verschiedenen Stellen im Haus.

- Für jede intelligente Lichtquelle gibt es eine intelligente Lichtsteuerung.
- Eine intelligente Lichtsteuerung ist mit einem oder mehreren Personensensoren, intelligenten Lichtquellen und einer Uhr zur Zeitdatenerfassung verbunden.
- Außerdem ist jede intelligente Lichtsteuerung mit der Anwendungssoftware auf dem Smartphone verbunden.
- Die Stromversorgung der intelligenten Lichtquelle erfolgt über einen normalen EIN/AUS-Schalter und die intelligente Lichtquelle dient dazu, von der intelligenten Lichtsteuerung einen Steuerbefehl zum Ein- und Ausschalten des Lichts zu erhalten.
- Eine Anwendungssoftware, die auf einem Smartphone läuft, wird als Schnittstelle für den Nutzer verwendet, um das Ein- und Ausschalten direkt zu unterstützen.
- Der EIN/AUS-Steuerbefehl der Beleuchtung von der Anwendung auf dem Smartphone hat Vorrang vor allem anderen.
- Mit Hilfe der Anwendungssoftware auf dem Smartphone kann der Nutzer den EIN/AUS-Zustand aller intelligenten Lichtquellen und die Fehlzustände aller Sensoren bestätigen, die aus den Zustandsdaten der intelligenten Lichtsteuerungen stammen.

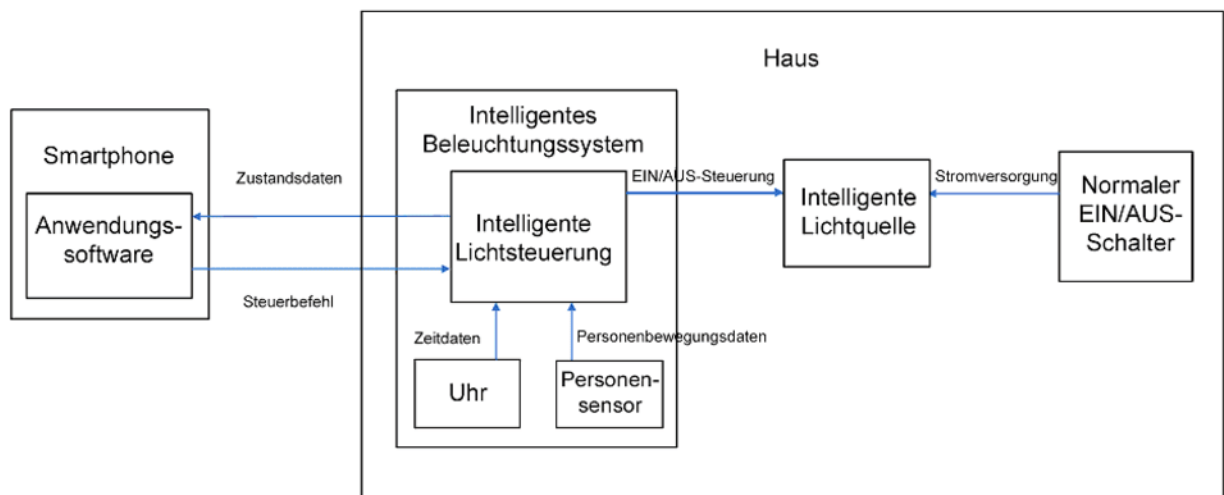


Bild A.1 – Systemdiagramm des Beispiels

Nachstehend werden die Regeln der intelligenten Lichtsteuerung angegeben:

- Der Steuerbefehl von der Smartphone-Anwendungssoftware hat Vorrang vor allem.
- bei Tag (11 Uhr – 16 Uhr): Grundsätzlich ist die Beleuchtung ausgeschaltet, an dunklen Orten (wie Toilette, Flur, Treppenhaus) wird die Beleuchtung durch Nutzung der Personenbewegungsdaten eingeschaltet.
- außerhalb des Tags (16 Uhr – 11 Uhr): Die Beleuchtung wird mit Nutzung der Personenbewegungsdaten ein- und ausgeschaltet.
- Wenn die Personenbewegungsdaten nicht an der Steuerung angekommen sind, ist Beleuchtung von 23 Uhr bis 7 Uhr ausgeschaltet, zu den anderen Zeiten ist die Beleuchtung eingeschaltet.

A.3.2.2 Betrachtung der Situationen in diesem Beispiel, in denen Probleme auftreten

Obwohl wir uns eine Reihe von Problemen mit diesem System vorstellen können, ist es schwierig, diese als ein tatsächliches Problem anzunehmen. Die Tatsache, dass die Benutzerschnittstelle außer als Anwendungssoftware auf dem Smartphone nicht vorhanden ist, ist es kein Problem, wenn alle Nutzer ein Smartphone besitzen. Selbst wenn eine Fehlfunktion durch einen Ausfall des Personensensors auftritt, hängt es von der AAL-Benutzerdomäne des Nutzers ab, ob der Nutzer es als Problem empfindet. Darüber hinaus ist die Bedienung der Beleuchtung mit Hilfe von Anwendungen auf dem Smartphone zulässig und eine Situation mit geringer Sicherheit, die durch den automatischen Betrieb nur mit Zeitdaten aufgrund eines Ausfalls des Personensensors verursacht wird, ist weniger wahrscheinlich. Dadurch besteht sogar die Möglichkeit, dass der Ausfall des Personensensors von normalen Anwendern nicht als Problem des Systems angesehen wird.

Es ist jedoch eindeutig, dass die Steuerung durch den Nutzer auf das Smartphone beschränkt ist, und wenn es ein Problem in der Situation gibt, dass nur Nutzer, die das Smartphone nicht benutzen können, nicht berücksichtigt werden, ist es offensichtlich gefährlich. Nutzer, die das System vorübergehend als Besucher nutzen und deren AAL-Benutzerdomäne eine andere ist, können häufig in einem Wohnumfeld vorkommen. Die nicht ausreichende Beleuchtung, die normalen Nutzern nicht auffällt, ist außerdem für zeitweilige Nutzer mit einem leichten Sehfehler, z. B. im Alter, ein erhebliches Problem. So besteht selbst beim Gehen im Dunkeln für einen zeitweiligen Nutzer mit schwachem Tritt auf einem normalen, ebenen Boden nur eine geringe Sturzgefahr, aber es ist durchaus anzunehmen, dass die Sturzgefahr auf einer Bodenfläche mit Stufen, wie einer Treppe, größer wird.

A.3.2.3 Beschreibung des erzählerischen Szenarios dieses Beispiels

Ein Szenario, in dem das Problem bei dem in diesem Beispiel gezeigten System offensichtlich wird, ist leicht anzunehmen und ist kein spezielles Szenario. In diesem Beispiel erfüllt ein solches Szenario die folgenden Bedingungen:

- Der ursprüngliche Nutzer ist sich der Unregelmäßigkeit des Systems nicht bewusst oder hat es dabei belassen, weil sie für ihn keine Unannehmlichkeiten darstellt, selbst wenn er sie bemerkt.
- Ein zeitweiliger Nutzer, der nicht der ursprüngliche Nutzer ist, bleibt für eine kurze Dauer (mehrere Tage).
- Der zeitweilige Nutzer unterscheidet sich vom ursprünglichen Nutzer in der AAL-Benutzerdomäne, und selbst wenn die Situation für den ursprünglichen Nutzer keine Rolle spielt, kann es zur einer gefährlichen Situation für den zeitweiligen Nutzer führen.
- Der zeitweilige Nutzer ist der Anwendung eines Smartphone nicht geübt.
- Zeitweilige Nutzer werden mit dem ursprünglichen Nutzer, der das Smartphone nicht benutzen kann, allein zu Hause gelassen.

Bei der erzählerischen Beschreibung eines solchen Szenarios kann Folgendes betrachtet werden.

Takuji (68 Jahre alt) hat einige Probleme mit der Sehschärfe an einem dunklen Ort. Takuji besuchte das Haus seines Sohnes Masaru (40 Jahre alt).

Masarus Haus ist ein zweistöckiges Einfamilienhaus und eine intelligente Beleuchtungsanlage ist installiert. Das intelligente Beleuchtungssystem arbeitet nach der Uhrzeit und der Ausgangsinformation der in jedem Raum, Flur und Treppenhaus installierten Personensensoren. Wenn die Person anwesend ist und der Raum dunkel wird, werden die Lichter automatisch eingeschaltet. Bewohner können auch die Smartphone-Anwendungssoftware verwenden, um die Beleuchtung jeder Leuchte ein- und auszuschalten. Ein normaler EIN/AUS-Schalter für die Beleuchtung ist installiert, wird aber als Hilfsmittel verwendet, und Masaru, seine Frau und sein Sohn Shota (8 Jahre alt) sind damit vertraut.

Als Masaru und seine Frau draußen waren und nur Takuji und Shota im Haus waren, begab sich Takuji am frühen Nachmittag in den zweiten Stock. Leider war der Personensensor der Treppe defekt und niemand wusste von diesem Fehler. Der Sensor war in der Lage, eine Person zu erkennen, die sich von der unteren zur oberen Etage bewegt, aber er konnte nicht eine Person erkennen, die sich von der oberen zur unteren Etage bewegt. Nach einer Weile versuchte Takuji, die Treppe hinunterzusteigen, und die Beleuchtung der Treppe leuchtete nicht auf. Takuji betätigte den normalen EIN/AUS-Schalter an der Wand, da die Treppe für Takuji etwas zu dunkel war, um ohne Beleuchtung hinunterzusteigen.

Takuji betätigte den normalen EIN/AUS-Schalter mehrmals, jedes Mal leuchtete das Licht nur wenige Sekunden und schaltet sich dann automatisch aus. Takuji war verwirrt und fragte Shota laut, was los sei. Shota erkannte, dass die intelligente Beleuchtung der Treppe nicht funktioniert hat, aber er hatte kein Smartphone. Shota kontaktierte seinen Vater Masaru und Masaru wusste, dass der Sensor der Treppe ein Problem mit der Verwendung der Smartphone-Anwendungssoftware von Masaru hatte. Masaru nutzt die Anwendungssoftware, um die Treppenbeleuchtung zu betätigen. Takuji konnte sicher nach unten gelangen.

A.3.3 Erstellung eines Anwendungsfalls durch Ausfüllen einer AAL-Anwendungsfallvorlage für dieses Beispiel

A.3.3.1 Erstellung der Liste aller im Anwendungsfall enthaltenen Akteure

Nach dem Ausfüllen der „vollständigen Beschreibung“ von „1.8 Darstellung des Anwendungsfalls“ der AAL-Anwendungsfallvorlage wird mit der Extraktion aller Akteure aus dem erzählerischen Szenario und dem Systemdiagramm begonnen. In diesem erzählerischen Szenario existieren vier Personen. Aber Masarus Frau wirkt nicht mit in diesem Szenario, drei Personen wurden aufgeführt:

- Takuji: 68 Jahre alt;
- Masaru: 40 Jahre alt, Takujis Sohn; und
- Shota: 8 Jahre alt, Masarus Sohn.

Aus dem Systemdiagramm (siehe [Bild A.1](#)) sind drei Einheiten (d. h. Smartphone, intelligentes Beleuchtungssystem, intelligente Lichtquelle) und ein Element (d. h. normaler Ein-/Ausschalter) ersichtlich. Im Smartphone gibt es eine Anwendungssoftware und im intelligenten Beleuchtungssystem gibt es eine Uhr, viele Personensensoren und viele intelligente Lichtsteuerungen. Dazu wurden acht Teilsysteme aufgeführt:

- intelligente Beleuchtungssysteme;
 - eine Uhr;
 - viele Personensensoren;
 - viele intelligente Lichtsteuerungen;
- intelligente Lichtquellen;
- Smartphone;
 - Anwendungssoftware;
- normale EIN/AUS-Schalter.

Nun kann die Liste aller Akteure unter „1.9 Akteure: Personen, Komponenten, Systeme, Integrierte Systeme, Anwendungen und Organisationen“ ausgefüllt werden.

A.3.3.2 Beschreibung des Anwendungsfallsszenarios mit Zeichnungen oder Diagrammen, die den Anwendungsfall darstellen

Um zunächst das geplante Gesamtsystem zu beschreiben, werden das bereits erstellte Systemdiagramm und das anzuschließende System beschrieben. In diesem Beispiel ist eine Betriebsvorschrift der intelligenten Lichtsteuerung erforderlich.

Als nächstes wird die Veränderung des Zustands des Zielsystems als Ganzes in Übereinstimmung mit der Veränderung des Szenarios beschrieben. In diesem Beispiel werden das Auftreten und die Änderung der Informationsübertragung, die entsprechend dem Zustandsübergang des Benutzerszenarios erfolgt, dargestellt, indem die Informationsübertragung im Systemdiagramm entsprechend dem Zustandsübergang aufgeführt wird, um die Zustandsänderung im Gesamtsystem zu veranschaulichen.

A.3.3.3 Analyse des Anwendungsfalls, um die Leerfelder der AAL-Anwendungsfallvorlage auszufüllen

Die Erläuterung des Szenarios in diesem Anwendungsfall ist soweit abgeschlossen. Nun müssen die einschlägigen internationalen Normen, Vorschriften, andere Anwendungsfälle, Schweregrade, Expositionen und verwandte Themen im Zusammenhang mit diesem Inhalt untersucht und die Leerfelder in der Anwendungsfallvorlage ausgefüllt werden.