

DIN IEC 63168
(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 2019-06-19

Entwurf

**Kooperative Mehrfachsysteme in vernetzten Wohnumfeldern –
Funktionale Sicherheit von elektrischen/elektronischen
sicherheitsbezogenen Systemen –
AAL-Aspekte
(IEC SyCAAL/130/CD:2018);
Text Deutsch und Englisch**

Cooperative multiple systems in connected home environments –
Functional safety of electrical/electronic safety-related systems –
AAL aspects
(IEC SyCAAL/130/CD:2018);
Text in German and English

Anwendungswarnvermerk

Dieser Norm-Entwurf mit Erscheinungsdatum 2019-04-19 wird der Öffentlichkeit zur Prüfung und Stellungnahme vorgelegt.

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

Stellungnahmen werden erbeten

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

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

Gesamtumfang 97 Seiten

DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE

Anwendungsbeginn

Anwendungsbeginn dieser Norm ist

Inhalt

Seite

Einleitung	7
1 Anwendungsbereich	9
2 Normative Verweisungen	9
3 Begriffe	9
4 Abkürzungen	13
5 Gesamtsicherheitslebenszyklus	14
5.1 Ziele	14
5.2 Allgemeines	16
5.2.1 Einführung in das Sicherheitslebenszyklus-Konzept	16
5.2.2 H-SIL-Konzept	16
5.2.3 Externe Maßnahmen zur funktionalen Sicherheit	16
5.3 Vorgaben für diesen Abschnitt	16
5.4 Anforderungen und Empfehlungen	17
5.4.1 Funktionale Sicherheitskultur	17
5.4.2 Kontinuierliche Verbesserung	17
5.4.3 Schulung und Qualifizierung	17
5.4.4 Sicherheitsmanagement während der Entwicklung	17
5.4.5 Zuweisung von Sicherheitsverantwortlichkeiten	17
5.4.6 Aufgabenzuordnung	17
5.4.7 Planung aller Aktivitäten des Sicherheitsmanagements während der Entwicklung	18
5.5 Arbeitsergebnis	20
6 Sicherheitsmanagement während der Konzeptphase und der Produktentwicklung	20
6.1 Ziele	20
6.2 Beiträge zu diesem Abschnitt	20
6.3 Anforderungen	21
6.3.1 Produkt und Umgebungsbedingungen	21
6.3.2 Grenzen des Produktes und seine Schnittstellen zu anderen Produkten	21
6.3.3 Belastungen	21
6.3.4 Zusätzliche Festlegungen	21
6.4 Arbeitsergebnis	22
7 Sicherheitsmanagement nach Produktionsbeginn	22
7.1 Ziele	22
7.2 Beiträge zu diesem Abschnitt	22
7.3 Anforderungen	22
7.3.1 Management der Produktion und Änderungsverfahren	22

7.3.2	Aufgaben zur Vorbereitung und Durchführung von Produktions- und Endkontrolle.....	22
7.3.3	Aufgaben für den sicheren Betrieb und die Außerbetriebnahme von Produkten	22
7.4	Arbeitsergebnis	23
8	Herstellung und Installation von sicherheitsbezogenen Systemen.....	23
8.1	Ziele.....	23
8.2	Allgemeines.....	23
8.3	Voraussetzungen und Empfehlungen	23
8.4	Anforderungen.....	23
8.4.1	Produktionsplan	23
8.4.2	Prüfplan	23
8.4.3	Herstellung und Prüfung	23
8.4.4	Prozessfähigkeit.....	24
8.4.5	Dokumentation	24
8.4.6	Nichteinhaltung	24
8.4.7	Rückverfolgbarkeit	24
8.4.8	Lager- und Transportbedingungen	24
8.4.9	Modifikation	24
8.5	Arbeitsergebnis	24
Anhang A (informativ)	Beispiele für Systemanalysen zur Sicherheit anhand des Anwendungsfalles – Verwendung der AAL-Anwendungsfallvorlage	25
A.1	Ziele.....	25
A.2	Auf dem Anwendungsfall basierende Aktivitäten zur Systemanalyse für die Sicherheit.....	25
A.2.1	Ziele.....	25
A.2.2	Vorbereitung vor dem Schreiben des Anwendungsfalles mit der AAL- Anwendungsfallvorlage	25
A.2.2.1	Allgemeines.....	25
A.2.2.2	Erläuterung der Zielsysteme	26
A.2.2.3	Berücksichtigung der Situationen, in denen Probleme auftreten.....	26
A.2.2.4	Beschreibung des erzählerischen Szenarios.....	26
A.2.3	Schreiben mit AAL-Anwendungsfallvorlage.....	27
A.2.3.1	Allgemeines.....	27
A.2.3.2	Erstellung der Liste aller Akteure des Anwendungsfalles.....	27
A.2.3.3	Beschreibung des Anwendungsfall-Szenarios mit Zeichnungen oder Diagrammen, die den Anwendungsfall darstellen	27
A.2.3.4	Analyse des Anwendungsfalles zum Ausfüllen der Felder der AAL- Anwendungsfallvorlage	27
A.2.4	Durchführung von Sicherheitsaktivitäten einschließlich Diskussionen, Anwendung des AAL- Anwendungsfalles	28
A.3	Anwendungsfall-Beispiel: Intelligente Beleuchtungskörper	28
A.3.1	Allgemeines.....	28
A.3.2	Vorbereitung vor dem Schreiben des Anwendungsfalles mit der AAL-	

Anwendungsfallvorlage	28
A.3.2.1 Erklärung der Zielsysteme in diesem Beispiel	28
A.3.2.2 Betrachtung der Situationen in diesem Beispiel, in denen Probleme auftreten	29
A.3.2.3 Beschreibung des erzählerischen Szenarios dieses Beispiels	29
A.3.3 Erstellung eines Anwendungsfalles durch Ausfüllen einer AAL-Anwendungsfallvorlage für dieses Beispiel	30
A.3.3.1 Erstellung der Liste aller im Anwendungsfall enthaltenen Akteure	30
A.3.3.2 Beschreibung des Anwendungsfall-Szenarios mit Zeichnungen oder Diagrammen, die den Anwendungsfall darstellen	31
A.3.3.3 Analyse des Anwendungsfalles zum Ausfüllen der Felder der AAL-Anwendungsfallvorlage	31
A.3.4 AAL-Anwendungsfall dieses Beispiels	31
A.4 Anwendungsfallbeispiel: Anzeigevorrichtung für die Bewegungsführung im Innenbereich und automatischer Roboterreiniger	39
A.4.1 Allgemeines	39
A.4.2 Vorbereitung vor dem Schreiben des Anwendungsfalles mit der AAL-Anwendungsfallvorlage	39
A.4.2.1 Erklärung der Zielsysteme in diesem Beispiel	39
A.4.2.2 Betrachtung der Situationen in dieses Beispiel, in denen Probleme auftreten	40
A.4.2.3 Beschreibung des erzählerischen Szenarios dieses Beispiels	41
A.4.3 Erstellung eines Anwendungsfalles durch Ausfüllen einer AAL-Anwendungsfallvorlage für dieses Beispiel	42
A.4.3.1 Erstellung der Liste aller im Anwendungsfall enthaltenen Akteure	42
A.4.3.2 Beschreibung des Anwendungsfall-Szenarios mit Zeichnungen oder Diagrammen, die den Anwendungsfall darstellen	42
A.4.3.3 Analyse des Anwendungsfalles zum Ausfüllen der Felder der AAL-Anwendungsfallvorlage	43
A.4.4 AAL-Anwendungsfall dieses Beispiels	43
Anhang B (informativ) Liste der Veröffentlichungen zur funktionalen Sicherheit kooperativer Systeme im vernetzten Wohnumfeld	50
B.1 Ziele	50
B.2 Liste der internationalen Normen	50
Literaturhinweise	53
Bilder	
Bild 1 – Kooperative Mehrfachsysteme	8
Bild 2 – Iterativer Prozess zur Auslegung sicherheitsbezogener Komponenten von Steuerungen	15
Bild 3 – Sicherheitslebenszyklus	16
Bild A.1 – Systemdiagramm des Beispiels	29
Bild A.2 – Systemdiagramm des Beispiels	40
Bild A.3 – Anwendungsfall-Diagramm des Beispiels	43
Tabellen	
Tabelle 1 – Kontrollmaßnahmen – Sicherheitsaudit, Sicherheitsüberprüfung und Sicherheitsbewertung	20

Tabelle B.1 – Liste der Veröffentlichungen zur funktionalen Sicherheit zusammenwirkender Systeme im vernetzten Wohnumfeld	51
--	----

Nationales Vorwort

Das internationale Dokument IEC SyCAAL/130/CD:2018 „Cooperative multiple systems in connected home environments – Functional safety of electrical/electronic safety-related systems – AAL aspects“ (CD, en: Committee Draft) ist unverändert in diesen Norm-Entwurf übernommen worden. Dieser Norm-Entwurf enthält eine noch nicht autorisierte deutsche Übersetzung.

Um Zweifelsfälle in der Übersetzung auszuschließen, ist die englische Originalfassung des CD entsprechend der diesbezüglich durch die IEC erteilten Erlaubnis beigelegt. Die Nutzungsbedingungen für den deutschen Text des Norm-Entwurfes gelten gleichermaßen auch für den englischen IEC-Text.

Das internationale Dokument wurde vom SyC AAL „Active Assisted Living“ der Internationalen Elektrotechnischen Kommission (IEC) erarbeitet und den nationalen Komitees zur Stellungnahme vorgelegt.

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

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

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

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

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

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

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

Kooperative Mehrfachsysteme in vernetzten Wohnumfeldern – Funktionale Sicherheit von elektrischen/elektronischen sicherheitsbezogenen Systemen – AAL-Aspekte

Einleitung

Dieses Dokument stellt einen Rahmen für Lebenszyklusprozesse mit Aktivitäten und Aufgaben bereit, die für die sichere Gestaltung und Wartung von kooperativen Mehrfachsystemen in vernetzten Wohnumfeldern erforderlich sind.

In einem vernetzten Wohnumfeld werden mehrere Systeme 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 im vernetzten Wohnumfeld. Bei der Sicherheitskonzeption jedes Systems ist es notwendig, die Gesamtheit mehrerer Systeme in einem vernetzten Wohnumfeld zu erfassen und das Risiko von unsicheren Zuständen durch die Verbindung auf ein sozial akzeptables Maß zu reduzieren.

Benutzer in vernetzten Wohnumfeldern, einschließlich Bewohner, Besucher und Helfer, betreiben das System direkt und/oder indirekt und sind von den Aktionen des Systems 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 Säuglinge und ältere Menschen.

Dieses Dokument bietet einen umfassenden Ansatz für die Realisierung eines Systems aus Elementen zur Ausführung von Sicherheitsfunktionen (sicherheitsbezogenes System), das für jedes kooperative System erforderlich ist. Wenn das nicht kooperierende System in einem vernetzten Wohnumfeld hinsichtlich des Sicherheitskonzeptes keinen Bezug zu anderen internationalen Normen hat, steht dies der Anwendung dieses Ansatzes nicht entgegen.

Dieses Dokument stellt die Vorgaben zur Verfügung:

- über den Sicherheitslebenszyklus kooperierender Systeme in einem vernetzten Wohnumfeld;
- für die Tätigkeiten und Aufgaben, die in jeder Phase des Sicherheitslebenszyklus erforderlich sind;
- auf dem Sicherheits-Integritätslevel für ein vernetztes Wohnumfeld, das die Eigenschaften der Benutzer berücksichtigt, insbesondere die Notwendigkeit der Unterstützung durch andere; und
- über die Risikominderungsprozesse des kooperativen Systems unter Verwendung der Sicherheits-Integritätslevel für ein vernetztes Wohnumfeld.

Es wird angenommen, dass der Leser dieses Dokuments ist:

- Entwickler von kooperativen Systemen im vernetzten Wohnumfeld;
- Entwickler von Systemkomponenten in einem vernetzten Wohnumfeld;
- Installateur von kooperativen Systemen in einem vernetzten Wohnumfeld.

Dieses Dokument besteht aus den folgenden Teilen, unter dem allgemeinen Titel Kooperative Mehrfachsysteme in vernetzten Wohnumfeldern – Funktionale Sicherheit von sicherheitsbezogenen elektrischen/elektronischen Systemen – AAL-Aspekte -:

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

Es wird anerkannt, dass einige produktspezifische Normen besondere, anwendbare Anforderungen an die funktionale Sicherheit der betreffenden Produkte haben können, die die Anforderungen der Normenreihe IEC 63168 einbeziehen oder ergänzen.

ANMERKUNG 1 Bei der Sicherheit einzelner Produkte in kooperativen Mehrfachsystemen sollten die einschlägigen internationalen Normen (z. B. Normenreihe IEC 60335 für Haushaltsgeräte) beachtet werden.

ANMERKUNG 2 Siehe [Anhang B](#) über die zu berücksichtigenden internationalen Sicherheitsnormen.

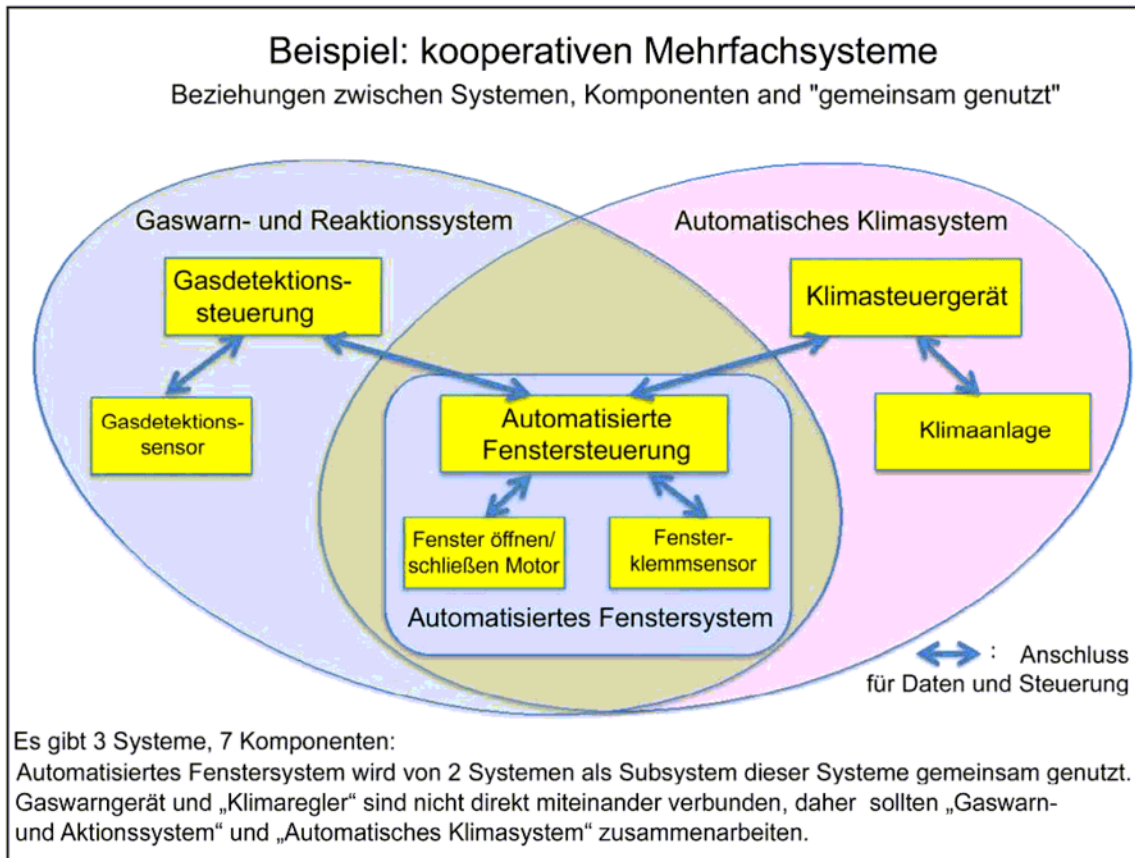


Bild 1 – Kooperative Mehrfachsysteme

1 Anwendungsbereich

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

Die AAL-spezifischen Anforderungen an die funktionale Sicherheit sind:

- AAL-spezifische Begriffe des Sicherheits-Integritätslevel (SIL), die verschiedene Arten von AAL-Benutzern berücksichtigen; und
- ein Risikobewertungsverfahren unter Verwendung des AAL-spezifischen SIL.

Diese kooperativen Mehrfachsysteme können von AAL-Anwendern installiert und betrieben werden, einschließlich Bedienern, die nicht vollständig ausgebildet sind.

Die Anforderungen werden in Übereinstimmung mit den Prinzipien der Grundnorm für funktionale Sicherheit, IEC 61508 (Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme) und den anderen zugehörigen Normen, einschließlich ISO/IEC 14762 (Informationstechnik – Anforderungen an die funktionale Sicherheit für Heim-Elektronik-Systeme (HES)) und IEC 63044-Reihe (Allgemeine Anforderungen an die Elektrische Systemtechnik für Heim und Gebäude (ESHG) und an Systeme der Gebäudeautomation (GA)), festgelegt.

Dieser Teil von IEC 63168 legt allgemeine Anforderungen an den Entwurf und die Entwicklung von kooperativen Mehrfachsystemen in einem vernetzten Wohnumfeld fest.

2 Normative Verweisungen

Die folgenden Dokumente werden im Text in solcher Weise in Bezug genommen, dass einige Teile davon oder ihr gesamter Inhalt Anforderungen des vorliegenden Dokuments darstellen. Bei datierten Verweisungen gilt nur die in Bezug genommene Ausgabe. Bei undatierten Verweisungen gilt die letzte Ausgabe des in Bezug genommenen Dokuments (einschließlich aller Änderungen).

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

ISO 25119-1:2010, *Tractors and machinery for agriculture and forestry – Safety-related parts of control systems – Part 1: General principles for design and development*

ISO 26262-1:2011, *Road vehicles – Functional safety – Part 1: Vocabulary*

IEC 61508-4:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 4: Definitions and abbreviations*

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-Plattform: verfügbar unter <http://www.iso.org/obp>

3.1

Audit

Prüfung eines implementierten Prozesses

[QUELLE: ISO 26262-1:2011, 1.5]

3.2

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

3.3

kooperative Mehrfachsysteme

Systeme, die bei wechselseitiger Beeinflussung funktionieren

3.4

elektrisches und/oder elektronisches System

E/E-System

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

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

[QUELLE: ISO 26262-1:2011, 1.31]

3.5

Element

System oder Teil eines Systems, das Komponenten, Hardware, Software, Hardwareteile und Softwareeinheiten einschließt

[QUELLE: ISO 26262-1:2011, 1.32]

3.6

Exposition

Dauer und Häufigkeit, in der sich eine Person in einer Situation befindet, in der die potenzielle Gefahr besteht

[QUELLE: ISO 25119-1:2010, 1.34]

3.7

Ausfall

Beendigung der Fähigkeit einer Einheit, eine erforderliche Funktion zu erfüllen

[QUELLE: ISO 25119-1:2010, 1.35]

3.8

Fehler

Zustand einer Einheit, gekennzeichnet durch die Unfähigkeit, eine erforderliche Funktion zu erfüllen, wobei die durch Instandhaltung oder andere geplante Handlungen bzw. durch das Fehlen äußerer Mittel verursachte Funktionsunfähigkeit ausgeschlossen ist

[QUELLE: ISO 25119-1:2010, 3.16]

3.9

funktionale Sicherheit

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

3.10

Anforderung an die funktionale Sicherheit

Anforderung an eine sicherheitsbezogene Funktion des E/E-Systems

3.11

Schaden

Körperverschädigung

[QUELLE: ISO 25119-1:2010, 3.24]

3.12

Gefahr

potenzielle Schadensquelle

[QUELLE: ISO 25119-1:2010, 3.25]

3.13

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 Gefahren, um unangemessene Risiken zu vermeiden

3.14

Gefährdungseignis

Kombination aus einer Gefahr und einer Gefährdungssituation

3.15

Gefährdungssituation

Umstand, unter dem eine Person einer oder mehreren Gefahren ausgesetzt ist, die unmittelbare oder langfristige Auswirkungen haben können.

[QUELLE: ISO 25119-1:2010, 3.26]

3.16

Wohnumfeld

Umgebung innerhalb eines Hauses, einschließlich der Gesamtheit der Geräte [z. B. Haustechnik, Heimnetzwerk, Einrichtung]

[QUELLE: IEC 60050-871:2018, 871-03-02]

3.17

H-SIL-Aufteilung

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

3.18

Einheit

System oder Anordnung von Systemen zur Implementierung einer Funktion auf der Ebene des angeschlossenen Wohnumfelds, auf das IEC 63168 angewendet wird

3.19

Lebenszyklus

Gesamtheit der Phasen vom Konzept bis zur Außerbetriebnahme der Einheit

[QUELLE: ISO 26262-1:2011, 1.72]

3.20

Modifikation

autorisierte Änderung einer Einheit

[QUELLE: ISO 26262-1:2011, 1.75]

3.21

Betriebsart

erkennbarer Funktionszustand eines Objekts oder Elements

[QUELLE: ISO 26262-1:2011, 1.81]

3.22

Überprüfung

Prüfung eines Arbeitsergebnisses, hinsichtlich der Erreichung des beabsichtigten Arbeitsergebnisses, entsprechend dem Zweck der Überprüfung

Anmerkung 1 zum Begriff: Überprüfungen können durch Checklisten unterstützt werden.

[QUELLE: ISO 26262-1:2011, 1.98]

3.23

Risiko

Kombination aus der Eintrittswahrscheinlichkeit des Schadens und der Schwere des Schadens

[QUELLE: ISO 26262-1:2011, 1.99]

3.24

Risikoanalyse

Kombination aus der Festlegung der Grenzen der Maschine, der Identifizierung der Gefährdungen und der Risikoabschätzung

[QUELLE: ISO 25119-1:2010, 3.40]

3.25

Risikobeurteilung

Gesamtprozess aus Risikoanalyse und Risikobewertung

[QUELLE: ISO 25119-1:2010, 3.41]

3.26

Risikobewertung

Beurteilung auf der Grundlage einer Risikoanalyse, ob ein bestimmtes Risiko tolerierbar ist

[QUELLE: ISO 25119-1:2010, 3.42]

3.27

Sicherheitsaktivitäten

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

3.28

Sicherheitskultur

Richtlinie und Strategie, die innerhalb eines Unternehmens zur Unterstützung der Entwicklung, Herstellung und des Betriebs von sicherheitsbezogenen Systemen verwendet werden

[QUELLE: ISO 26262-1:2011, 1.107]

3.29

Sicherheitsziel

Beschreibung, wie eine bestimmte Gefährdung zu vermeiden ist

Anmerkung 1 zum Begriff: Es ist die oberste Sicherheitsanforderung, die sich aus der Gefahrenanalyse und der Risikobewertung ergibt.

Anmerkung 2 zum Begriff: Das Vorhandensein mehrerer Sicherheitsziele für eine Einheit ist möglich.

[QUELLE: ISO 25119-1:2010, 3.44]

3.30

Sicherheits-Integritätslevel für ein vernetztes Wohnumfeld

H-SIL

eine von vier Stufen, um die notwendigen Anforderungen der IEC 63168 an den Gegenstand oder das Element und die Sicherheitsmaßnahmen zur Vermeidung eines unangemessenen Restrisikos festzulegen, wobei ein Alphabet von A die niedrigste Stufe bis D die höchste Stufe darstellt

3.31

Sicherheitslebenszyklus

notwendige Tätigkeiten im Rahmen der Realisierung von sicherheitsbezogenen Systemen während einer Dauer, die mit der Konzeptphase des Produktdesigns 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]

3.32

Sicherheitsmanager

Rolle, die der Verantwortliche des Managements für funktionale Sicherheit während der Artikelentwicklung ausfüllt

[QUELLE: ISO 26262-1:2011, 1.109]

3.33

Sicherheitsplan

Plan zur Verwaltung und Steuerung der Ausführung der Sicherheitsaktivitäten (1.104) eines Projekts, einschließlich Daten, Meilensteine, Aufgaben, Ergebnisse, Verantwortlichkeiten und Ressourcen

[QUELLE: ISO 26262-1:2011, 1.112]

3.34

Schweregrad

Maß für den wahrscheinlichsten Grad der Schädigung einer gefährdeten Person

[QUELLE: ISO 25119-1:2010, 3.47]

3.35

Unterphasen

Unterteilung einer Stufe im Sicherheitslebenszyklus, die in einem gesonderten Abschnitt festgelegt ist

3.36

System

Gruppe von Elementen, die mindestens einen Sensor, eine Steuerung und ein Stellglied miteinander verbinden

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

Anmerkung 2 zum Begriff: Ein Element eines Systems kann auch ein anderes System sein.

[QUELLE: ISO 26262-1:2011, 1.129]

3.37

Arbeitsergebnis

Ergebnis einer Design- oder Entwicklungsaktivität

[QUELLE: ISO 25119-1:2010, 3.57]

4 Abkürzungen

Für die Anwendung dieses Dokuments gelten die folgenden Begriffe.

SOP Produktionsstart

SRS sicherheitsbezogenes System

5 Gesamtsicherheitslebenszyklus

5.1 Ziele

Für die Entwicklung eines sicheren E/E-Systemprodukts in einem vernetzten Wohnumfeld sollten Entwickler die Auswirkungen auf die Sicherheit der kooperativen Mehrfachsysteme während des zu entwickelnden Produktlebenszyklus berücksichtigen. Zu den zu berücksichtigenden Inhalten gehören die Gefährdungsanalyse und die Risikobewertung der kooperativen Mehrfachsysteme. Da zu den Nutzern von E/E-Systemprodukten auch Jugendliche und ältere Menschen gehören und der Einflussbereich der kooperativen Mehrfachsysteme Besucher und Nachbarn umfasst, können Entwickler bei Bedarf eine Systemanalyse zur Sicherheit auf der Grundlage eines Anwendungsfalls durchführen.

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

ANMERKUNG 2 Siehe [Anhang A](#), um die Beispiele der Systemanalyse für die Sicherheit anhand des Anwendungsfalles zu verstehen.

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 betrifft sowohl die Tätigkeiten, die erforderlich sind, um das notwendige Maß an funktionaler Sicherheit für den Artikel zu gewährleisten, als auch 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 sollte so konzipiert und aufgebaut sein, dass die Grundsätze der Risikoanalyse, der Risikobewertung und eines iterativen Prozesses zur Gestaltung sicherheitsbezogener Komponenten von Steuerungssystemen vollständig berücksichtigt werden (siehe [Bild 2](#)).

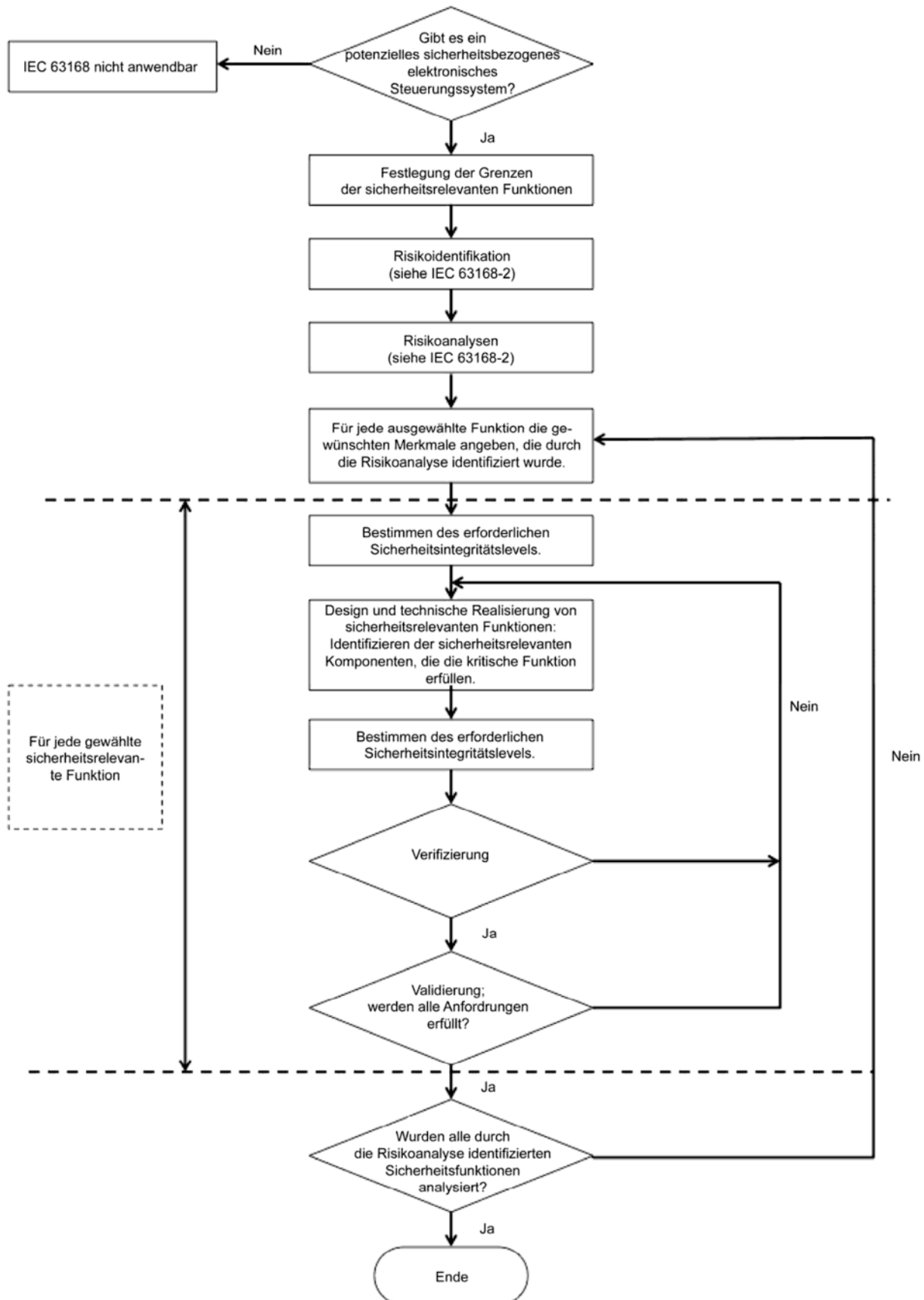


Bild 2 – Iterativer Prozess zur Auslegung sicherheitsbezogener Komponenten von Steuerungen

5.2 Allgemeines

5.2.1 Einführung in das Sicherheitslebenszyklus-Konzept

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

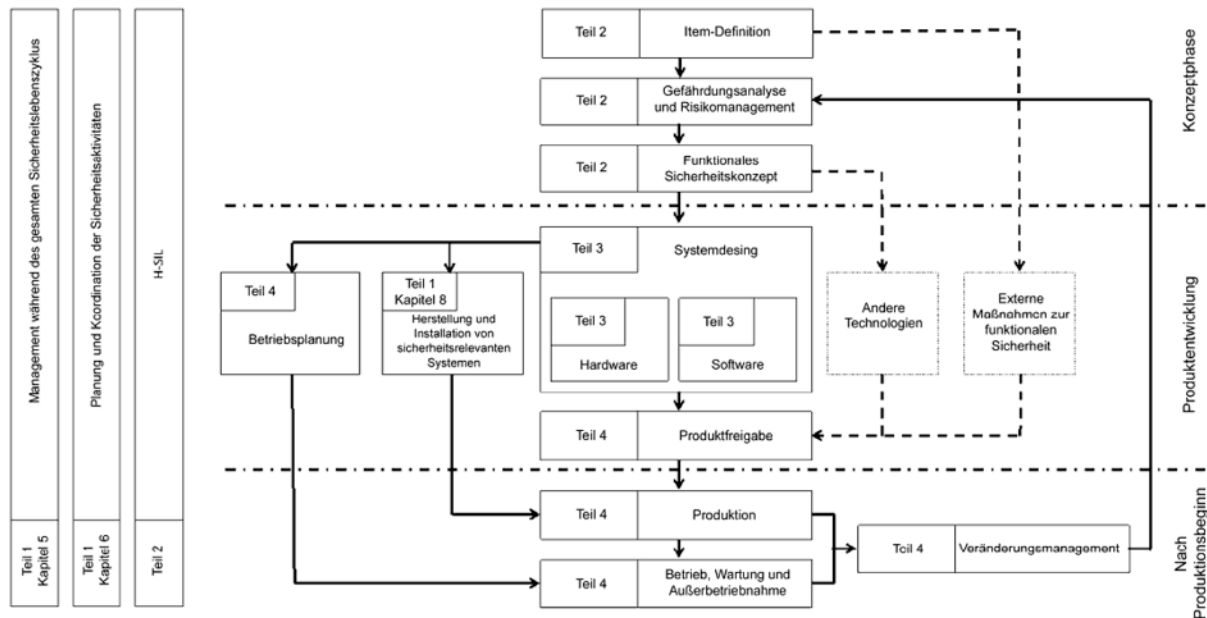


Bild 3 – Sicherheitslebenszyklus

5.2.2 H-SIL-Konzept

Das Konzept des H-SIL ist in alle Sicherheitsaktivitäten im gesamten Sicherheitslebenszyklus des Systems eingebunden. Im Gefährdungsanalyse- und Risikobewertungsverfahren für einzelne Systeme, einschließlich Einheiten und Elementen, wird die H-SIL-Aufteilung für alle Elemente unter Berücksichtigung von Exposition, Schweregrad und AAL-Benutzerdomäne durchgeführt. Eine detaillierte Beschreibung der H-SIL ist in IEC 63168-2 enthalten.

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

Wurde die H-SIL-Aufteilung in einem früheren Entwicklungsstadium nach IEC 63168-2 durchgeführt, ist die aus der Aufteilung resultierende H-SIL einzuhalten.

5.2.3 Externe Maßnahmen zur funktionalen Sicherheit

Diese Maßnahmen können durch die in der Systemdefinition beschriebene Punkte 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 Risikoanalyse kann die externe funktionale Sicherheit berücksichtigt werden.

5.3 Vorgaben für diesen Abschnitt

Die notwendigen Vorgaben sind ein bewährter Qualitätssicherungsplan (z. B. ISO/TS 16949 oder vergleichbar) und ein Gesamtprojektplan.

5.4 Anforderungen und Empfehlungen

5.4.1 Funktionale Sicherheitskultur

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
- Überprüfung des Status von Prozessen, um die funktionale Sicherheit zu erreichen.

5.4.2 Kontinuierliche Verbesserung

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

- die Schaffung von unternehmensspezifischen Verfahren zur Erfüllung der Anforderungen in IEC 63168,
- die Bestimmung von Werkzeugen, Vorlagen, Datenbanken und anderen Ressourcen, die bei der Durchführung sicherheitsbezogener Tätigkeiten helfen, und
- Einholung von Rückmeldungen aus Erkenntnissen über sicherheitsbezogener 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 sollte es sein, ein ausgewogenes Maß an Kompetenz in folgenden Bereichen aufrechtzuerhalten

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

5.4.4 Sicherheitsmanagement während der Entwicklung

Ziel sollte 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 Sinne von IEC 63168 einbeziehen, stellt eine zentrale Managementaufgabe für die, für den Bereich 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 ist sicherzustellen, dass Personen über ausreichende, dokumentierte Qualifikationen und Kompetenzen für ihre Aufgaben verfügen. Die erforderliche Ausbildung und Erfahrung kann vom H-SIL und der Komplexität des Themas 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 für die funktionale 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 sicherheitsbezogener Aktivitäten 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 sind zu planen, 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 Risikoanalyse nach IEC 63168-2;
- Umsetzung der Sicherheitsanforderungen im Rahmen der Entwicklungsaktivitäten nach IEC63168-2 und IEC 63168-3;
- Bestätigung durch Entwicklungspartner, dass sie die Sicherheitsanforderungen durch Bewertungen, Überprüfungen und Audits erfüllt haben;
- Planung der Überprüfung und Bestätigung der Sicherheitsanforderungen nach IEC 63168-4;
- Festlegung der Tätigkeiten zur Bestätigung der funktionalen Sicherheit (Audit, Überprüfung, Bewertung);
- Einbeziehung der gesamten Projektsicherheitsaktivitäten in das projektspezifische Sicherheitsmanagement.

5.4.7.2 Erstellung der Sicherheitsdokumentation

Die Sicherheitsdokumentation ist so zu verfassen, dass andere den abgelaufenen Prozess verstehen können. Die Dokumentation muss in Übereinstimmung mit den Richtlinien zur Aufbewahrung 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 sicherheitsbezogene Tätigkeiten 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.

Sicherheitsbezogene Aktivitäten sollten in die Gesamtprojektplanung einbezogen und mit den erforderlichen Ressourcen ausgestattet werden.

5.4.7.3.2 Inhalt des Sicherheitsplans

Der Sicherheitsplan sollte alle Aktivitäten umfassen, die im Lebenszyklus festgelegt sind, unterstützende Aktivitäten, Bewertung und Managementaktivitäten. Bei Bedarf kann eine detailliertere Unterteilung vorgenommen werden.

Sicherheitsbezogene Aktivitäten 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, Quelldokumente;
- Verantwortliche(r);
- notwendige Ressourcen;
- Dauer, Frist;
- Dokumentation 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 sicherheitsbezogene Tätigkeiten als solche gekennzeichnet werden.

Der Sicherheitsplan kann Verweise auf andere Pläne enthalten. Im Allgemeinen ist es besser, Referenzen als parallele Beschreibungen von Aktivitäten in mehreren Dokumenten zu haben.

Der Sicherheitsplan unterliegt dem Versions- und Änderungsmanagement.

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 weggelassen werden.

Bei der Erstellung des Sicherheitsplans ist darauf zu achten, dass die spezifischen Merkmale aller Tätigkeiten an den H-SIL und die Umstände des Projekts angepasst werden.

Eine klare Begründung ist immer dann anzugeben, wenn einzelne Aktivitäten weggelassen oder in reduzierter Form durchgeführt werden.

5.4.7.3.5 Nachweis der funktionalen Sicherheit

Die Tätigkeiten zur Sicherstellung der funktionalen Sicherheit umfassen das Sicherheitsaudit, die Sicherheitsüberprüfung und die Sicherheitsbewertung nach [Table 1](#).

Tabelle 1 – Kontrollmaßnahmen – Sicherheitsaudit, Sicherheitsüberprüfung und Sicherheitsbewertung

Überprüfungs- maßnahme	Audit	Überprüfung	Bewertung
Betreff	Implementierung der für die funktionale Sicherheit erforderlichen Prozesse	Ergebnis einer bestimmten sicherheitsbezogenen Tätigkeit	Der gesamte Punkt ist in der Phase „Systemdefinition“ beschrieben.
Umfang und Tiefe	Vom Auditor festgelegt	Geplant vor der Durchführung der Überprüfung	Umfang ist die vollständige Überprüfung aller Prozesse und technischen Maßnahmen, die für die funktionale Sicherheit erforderlich sind Die Tiefe wird vom Prüfer bestimmt
Wird im Lebenszyklus durchgeführt	Während der Implementierung der erforderlichen Prozesse und vor Abschluss jeder Aktivität	Nach Abschluss jeder sicherheitsbezogenen Tätigkeit	Parallel zur Entwicklung oder in einem Block Fertigstellung vor der Serienfreigabe
Verantwortung	Zur ausreichenden Verifizierung der Prozesse	Für eine ordnungsgemäße Durchführung der Überprüfung	Übernimmt die gemeinsame Verantwortung für die funktionale Sicherheit
Ergebnis	Prüfbericht (kann Teil einer Bewertung sein)	Überprüfungsprotokoll (kann Teil einer Bewertung sein)	Erklärung zur funktionalen Sicherheit des Objekts

5.5 Arbeitsergebnis

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

- Kontrollmaßnahmen – Prozessanweisung zur Prüfung der Prozesse während der Serienentwicklung;
- 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 Methoden sind die Risikoanalyse (siehe unten), andere Normen, gesetzliche Anforderungen und die Expertise der Prüfstelle.

6.2 Beiträge zu diesem Abschnitt

Die notwendigen Beiträge sind eine Beschreibung des Produktes, seiner Schnittstellen, bereits bekannte Sicherheits- und Zuverlässigkeitsanforderungen und der Anwendungsbereich.

6.3 Anforderungen

6.3.1 Produkt und Umgebungsbedingungen

Ein sicherheitsbezogenes Konzept muss Folgendes umfassen:

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

6.3.2 Grenzen des Produktes und seine Schnittstellen zu anderen Produkten

Die folgenden Informationen sind zu berücksichtigen, um ein Verständnis für die Funktionsweise des Produktes in seiner Umgebung zu gewinnen:

- die Grenzen des Produktes;
- seine Schnittstellen und Interaktionen mit anderen Produkten und Komponenten;
- Anforderungen an andere Produkte;
- Zuordnung und Verteilung relevanter Funktionen auf die eingebundenen Produkte.

6.3.3 Belastungen

Die Belastungen, die die Sicherheit und Zuverlässigkeit des Produktes beeinträchtigen könnten, müssen bestimmt werden, einschließlich der folgenden:

- das Zusammenspiel verschiedener Produkte;
- Gefahren physikalischer oder chemischer Art (Energiegehalt, Toxizität, Explosivität, Korrosivität, Reaktivität, Brennbarkeit usw.);
- andere externe Ereignisse (Temperatur, Schock, elektromagnetische Verträglichkeit (EMV), usw.);
- vernünftigerweise vorhersehbare menschliche Bedienungsfehler;
- Gefahren, die vom Produkt ausgehen, und Ereignisse, die einen Ausfall auslösen (z. B. während der Montage oder Wartung).

6.3.4 Zusätzliche Festlegungen

Zusätzlich zu den in 5.3.2 beschriebenen Tätigkeiten müssen die folgenden Festlegungen oder Maßnahmen durchgeführt werden:

- Festlegung, ob für das Produkt, im Falle einer Änderung, eine Auswirkungsanalyse durchzuführen ist, um den Sicherheitslebenszyklus entsprechend anzupassen;
- Erstellung eines Plans und einer Spezifikation zum Bestätigen der Anforderungen an das in 5.3.1 definierte Produkt;
- Festlegung des Projektmanagements für die entsprechenden Phasen des Lebenszyklus;
- ausreichende Eingangsdaten für die Zuverlässigkeitsbewertung;
- angemessene Verfahren und Anwendung von Werkzeugen und Technologien;
- Einsatz von qualifiziertem Personal.

6.4 Arbeitsergebnis

Die Arbeitsergebnisse des Konzepts/der Festlegung des Produktes sind

- e) das Produkt und die Umgebungsbedingungen,
- f) Grenzen des Produktes und seine Schnittstellen zu anderen Produkten
- g) Stressquellen und
- h) zusätzliche Bestimmungen.

7 Sicherheitsmanagement nach Produktionsbeginn

7.1 Ziele

Ziel dieser Phase ist es, die Verantwortlichkeiten der für die funktionale Sicherheit nach der SOP verantwortlichen Personen, Abteilungen und Organisationen zu definieren. Dies betrifft sowohl die Tätigkeiten, die erforderlich sind, um das notwendige Maß an funktionaler Sicherheit für das Produkt zu gewährleisten, als auch die Rückmeldemaßnahmen, die dieses Maß an funktionaler Sicherheit bestätigen.

7.2 Beiträge zu diesem Abschnitt

Der Hersteller sollte ein Qualitätsmanagementsystem einführen.

7.3 Anforderungen

7.3.1 Management der Produktion und Änderungsverfahren

In den Lebenszyklusphasen nach der 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 an die Erreichung und Aufrechterhaltung der funktionalen Sicherheit in allen produzierten Einheiten während der Lebensdauer des Systems werden in der Regel bei der Entwicklung des Objekts festgelegt und können nach einem Änderungsprozess 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 aufgelistet und überwacht werden. Darüber hinaus muss die Serienkonformität in Bezug auf Sicherheitsanforderungen und Dokumentation überprüft werden.

7.3.3 Aufgaben für den sicheren Betrieb und die Außerbetriebnahme von Produkten

Die folgenden Aufgaben müssen ausgeführt werden.

- Ausarbeitung und Aufnahme besonderer Inhalte und Warnhinweise in die Betriebsanleitung.
- Auflistung der Anforderungen an das Instandhaltungs- und Herstellerwartungspersonal und Überwachung der Umsetzung.
- Rückmeldung der beobachteten Fehler.
- Auflistung 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 Überprüfungsmaßnahme vorhanden sein.
- Erwägen, das bestehende V-Modell im Laufe des Projekts zu verfeinern.

7.4 Arbeitsergebnis

Die Arbeitsergebnisse aus den Aktivitäten des Sicherheitsmanagements nach der SOP sind spezielle Inhalte und Hinweise 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 SRS. Ein weiteres Ziel ist es, sicherzustellen, dass die erforderliche funktionale Sicherheit während des Produktionsprozesses durch den jeweiligen Produkthersteller oder die für den Prozess verantwortliche Person/Organisation (Artikelhersteller, Lieferant, Unterlieferant, usw.) gewährleistet ist.

8.2 Allgemeines

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

8.3 Voraussetzungen und Empfehlungen

Die folgenden Informationen sollten verfügbar sein:

- Montagehinweise – die Dokumentation der von der Montage betroffenen Komponenten oder Funktionen;
- Prüfhinweise und -kriterien – Dokumente, die sich auf Prüfverfahren und die zu prüfenden Kriterien für die sicherheitsbezogenen Funktionen beziehen;
- Produktfreigabe – die Freigabedokumente für Produktion, Prüfung und Installation;
- Produktüberwachung – erforderlich für sicherheitsbezogene Merkmale und die Sicherstellung, dass die sicherheitsbezogenen Eigenschaften von Komponenten im Produktionsprozess des Artikelherstellers 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;
- 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;
- 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 ist auch durch branchenübliche Praktiken sicherzustellen. Die Prüfmittel müssen einem geeigneten Prozess der Prüfmittelprüfung unterzogen werden.

8.4.5 Dokumentation

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

- Datum der Prüfung,
- Tester,
- eindeutige Teileidentifikation und Prüfergebnisse und
- aller Abweichungen des beobachteten vom erwarteten Verhalten einschließen.

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 Änderungen an den Produkten muss eine Auswirkungsanalyse verwendet werden, um den Lebenszyklus-Schritt zu bestimmen, zu dem zurückzukehren ist, und die Schritte, die zu wiederholen sind (IEC 63168-4).

8.5 Arbeitsergebnis

Die Arbeitsergebnisse aus der Herstellung und Installation von sicherheitsbezogenen Systemen sind

- Dokumentation der sicherheitsbezogenen Produktionsschritte (Produktionsplan),
- Prüf- und Einstellkriterien (sicherheitstechnisch),
- Dokumentation der Nichteinhaltung und
- Rückverfolgbarkeit der Produkte nach sicherheitsbezogenen Kriterien.

Anhang A (informativ)

Beispiele für Systemanalysen zur Sicherheit anhand des Anwendungsfalles – 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, sollten im Allgemeinen verschiedene Faktoren und deren Möglichkeiten bei der Präsentation von Anwendungsfällen berücksichtigt werden. Bei der Analyse des Sicherheitsaspekts des Systems ist der Akt der Betrachtung der Sicherheit aus verschiedenen Blickwinkeln immer eine Frage der Anforderung, und der Akt der Betrachtung des Anwendungsfalles wird ihn erreichen.

In diesem Anhang werden die durchzuführenden Aktivitäten zur Systemanalyse für die Sicherheit auf der Grundlage des Anwendungsfalles erläutert. Im Folgenden werden zwei Beispiele für die Systemanalyse zur Sicherheit anhand des Anwendungsfalles 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. Diejenigen, die die Systemanalyse ausführen, werden in der Lage sein, eine Vorstellung von der Methode der Analyse des Zielsystems zu bekommen, indem sie den Inhalt lesen.

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

A.2.1 Ziele

Das Ziel dieses Unterabschnitts ist es, die Ausführenden der Systemanalyse anzuregen, die Aktivitäten, die bei der Systemanalyse für die Sicherheit auf der Grundlage von Anwendungsfällen durchgeführt werden sollten, nacheinander zu präsentieren. Der Zweck der Einführung mehrerer Systeme in einem vernetzten Wohnumfeld ist es, das Leben der Benutzer 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 oben genannten Faktoren ist die AAL-Anwendungsfallvorlage ein sehr attraktives und leistungsfähiges Werkzeug in der Systemanalyse zur Sicherheit mehrerer kooperierender Systeme im vernetzten Wohnumfeld.

ANMERKUNG Siehe IEC TS 63134, um die Inhalte der AAL-Anwendungsfallvorlage zu verstehen.

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

A.2.2.1 Allgemeines

In den folgenden Unterabschnitten sind drei wichtige Aktivitäten unter den Arbeiten aufgeführt, die als Vorbereitungsphase vor der Beschreibung des Anwendungsfalles 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 einen vorübergehenden Vorgang zur Unterstützung einer effizienten Analyse. So kann der Ausführende beispielsweise einen fehlenden Teil der Aktivitäten zur Erläuterung des Zielsystems offen legen, indem er die Situation, in der Probleme auftreten, berücksichtigt 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 den folgenden Unterabschnitten beschrieben werden (z. B. Erstellung der Liste aller in den Anwendungsfall einbezogenen Akteure, Untersuchung verwandter 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. In der Granularität der Teile des Systemdiagramms ist es nicht notwendig, alle Systeme bis auf die Positionsebene 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 Benutzern, die Regeln für den Systembetrieb und die Zeitpläne zeigen sollten. Wie bereits erwähnt, kann der Teil klar werden, der in der Aktivität „Erläuterung der Zielsysteme“ fehlte, wenn die Ausführenden an den folgenden beiden Aktivitäten arbeiten. Es ist wünschenswert, klar erkennbare Arbeiten in Auftrag zu geben.

A.2.2.3 Berücksichtigung der Situationen, in denen Probleme auftreten

Da das Wohnumfeld (einschließlich des vernetzten Wohnumfeldes) verschiedene Aspekte aufweist, ist es die schwierigste und wichtigste Tätigkeit, über Situationen nachzudenken, in denen Probleme auftreten. Es ist notwendig, das Umfeld und das Klima des Ortes, an dem das Haus gebaut wird, sowie die Gewohnheit und den Geschmack des Benutzers zu berücksichtigen (ob man im Raum Schuhe trägt oder nicht und ob man auf dem Boden sitzt). Es ist auch notwendig, über verschiedene Aspekte der Charakteristika des Benutzers nachzudenken. Die Vertiefung der Analyse bei dieser Tätigkeit 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 Benutzers 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 Benutzers: Baby, Kleinkind, Kind, Erwachsener, Alter
- Behinderung des Nutzers: keine Behinderung, vorübergehende Behinderung (durch Unfall oder Krankheit), dauerhafte Behinderung
- Aufenthaltsdauer des Benutzers: ansässig, einmaliger Besucher (z. B. Freund, Nachbar), regelmäßiger Besucher (z. B. Betreuer, Haushälterin, Tagesmutter)

Wenn die Situation, in der Probleme auftreten, nicht in Betracht gezogen werden kann, wird das Zielsystem als ausreichend sicher angenommen. Es gibt jedoch Möglichkeiten der Kontrolle durch die Ausführenden, wobei ein sorgfältiges Urteilsvermögen erforderlich ist, um die gesamten Aktivitäten der Systemanalyse für die Sicherheit anhand des Anwendungsfall abzuschließen. Selbst wenn eine ausreichende Sicherheit an den Zielsystemen realisiert wird, sollten die Tätigkeiten der Systemanalyse zur Sicherheit auf der Grundlage des Anwendungsfall in dem Sinne fortgesetzt werden, dass der Prozess des Sicherheitsdenkens auf dem Zielsystem als Anwendungsfall belassen wird.

A.2.2.4 Beschreibung des erzählerischen Szenarios

Der Vorteil der Beschreibung des erzählerischen Szenarios liegt darin, dass ein gemeinsames Verständnis auf leicht verständliche Weise aufgebaut wird. Ziel ist es nicht, Unstimmigkeiten im Verständnis der Anwendungsfälle zwischen den Ausführenden von Sicherheitsaktivitäten und den Lesern von Anwendungsfällen zu beseitigen. Bei der Beschreibung von erzählerischen Szenarien ist darauf zu achten, dass sie vollständig, lückenlos, einfach, kurz und leicht verständlich sind. Die Erklärung sollte im erzählerischen Szenario abgeschlossen werden. Es ist wichtig, das gesamte System, die Umgebung und die Situation zu erklären, einschließlich der menschlichen Faktoren, eben alles. 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 gestalten. Schließlich ist es notwendig zu prüfen, ob es sich um eine für andere Leser lesbare Beschreibung handelt. Manchmal vergessen die Ausführenden, die einen Anwendungsfall in Betracht ziehen, den Grad des Verständnisses anderer Leser, indem sie zu viel

über einen Anwendungsfall nachdenken. Die Ausführenden sollten Gegenmaßnahmen in Betracht ziehen, wie z. B. 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 oben beschriebenen Aktivitäten wurde die Konstruktion der Basisteile für den eigentlichen aussagekräftigen Anwendungsfall abgeschlossen. In den folgenden Aktivitäten analysieren die Ausführenden die Teile weiter und füllen die Felder des Platzhalters in der AAL-Anwendungsvorlage aus. Mit dem Abschluss dieser Aktivitäten ist die Erstellung des AAL-Anwendungsfalles abgeschlossen und der Aufbau des Hauptteils der Systemanalyse für Sicherheit auf Basis des Anwendungsfalles nahezu abgeschlossen.

Bei der Beschreibung des Anwendungsfalles durch die Verwendung der AAL-Anwendungsfallvorlage in der Praxis sollten die Ausführenden darauf achten, dass sie nach sorgfältigem 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 und die Analyseinstrumente für AAL (wie AAL-Struktur, AAL-Akteure-Liste usw.), die von SyC AAL bereitgestellt werden, so weit wie möglich zu verwenden.

Es wird empfohlen, dass die Ausführenden zunächst in die erzählerischen Szenarien einsteigen sollten, und zwar in die „vollständigen Beschreibung“ des „1.8 Erzählung der Anwendungsfalles“ der AAL-Anwendungsfallvorlage.

A.2.3.2 Erstellung der Liste aller Akteure des Anwendungsfalles

In dieser Aktivität erfassen die Ausführenden zunächst alle Personen, Elemente, 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. In der 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“ verwendet: Personen, Komponenten, Systeme, Integrierte Systeme, Anwendungen und Organisationen“ der AAL-Anwendungsfallvorlage.

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

In dieser Aktivität füllen die Ausführenden „2 Zeichnungen oder Diagramme, die den Anwendungsfall darstellen“ der AAL-Anwendungsfallvorlage detailliert aus. Es ist ratsam, den Systemplan der Zielsysteme auszufüllen, falls vorhanden. Nach Ausfüllen der Spezifikationen der Zielsysteme erstellen und beschreiben die Ausführenden das Anwendungsfall-Szenario entsprechend dem erzählerischen Szenario. Es gibt keine Rezepte für die Art des Ausfüllens der Szenarien des Anwendungsfalles, so dass verschiedene Inhalte, wie die Verwendung des Systemdiagramms, die Verwendung des Zeitdiagramms usw. berücksichtigt werden, aber für den Leser einfach und leicht verständlich gehalten werden sollten. Die Ausführenden können Niemanden beschreiben, der nicht in der Liste aller Akteure erscheint. Auch wenn jemand nur „2 Zeichnungen oder Diagramme, die den Anwendungsfall darstellen“ liest, sollten die Ausführenden versuchen so zu beschreiben, dass die Leser den Inhalt zweifelsfrei verstehen können.

A.2.3.4 Analyse des Anwendungsfalles zum Ausfüllen der Felder der AAL-Anwendungsfallvorlage

Die für die Sicherheitsdiskussion notwendigen Elemente (Exposition, H-SIL, usw.) sind in „1.13 Allgemeine Hinweise“ beschrieben. Die Ausführenden fassen das Ziel des Anwendungsfalles zusammen und beschreiben es in „1.7 Umfang und Ziele des Anwendungsfalles“. Für die anderen Anwendungsfälle (einschließlich AAL-Anwendungsfälle), die sich auf den Anwendungsfall beziehen, wenn vorhanden, beschreiben es die Ausführenden in „1.12 Beziehung zu anderen bekannten Anwendungsfällen“. Zu Rechtsvorschriften und internationalen Normen im Zusammenhang mit dem Inhalt des Anwendungsfalles füllen die Ausführenden „1.10 Aspekte: Rechtsgültige Verträge, gesetzliche Vorschriften, Beschränkungen und andere (einschließlich regionaler Vorschriften)“ und „1.11 In Bezug genommene Normen und/oder Normungskomitees“ in

angemessener Weise aus. Für die anderen Felder 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, Anwendung des AAL-Anwendungsfalles

Die Analyse der Sicherheit des Zielsystems anhand des Anwendungsfalles wird 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 Reduzierung von Sicherheitsrisiken durchzuführen. Die Ausführenden sollten nicht vergessen, dass die Analyse der Sicherheit des Zielsystems anhand des Anwendungsfalles eine Vorbereitung eines Teils der Gefahrenanalyse und Risikobewertung für das System ist.

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

A.3 Anwendungsfall-Beispiel: Intelligente Beleuchtungskörper

A.3.1 Allgemeines

Dieses Beispiel zeigt ein Szenario, das in Bezug auf die Sicherheit durch intelligente Beleuchtung als unvollständiges System angenommen werden kann. Das Zielsystem besteht aus einem intelligenten Beleuchtungskörper, einem Netzschalter, einer intelligenten Lichtsteuerung und einer Anwendungssoftware auf dem Smartphone.

Als Voraussetzung für das Szenario gibt es Probleme bei der Konstruktion und Fehler im Betrieb, aber im Normalbetrieb gibt es keine Probleme mit dem ursprünglichen Benutzer. In diesem Beispiel verursachen die Designprobleme und der Betriebsausfall einen schweren Schaden, wenn der Besucher, dessen AAL-Benutzerdomäne sich vom ursprünglichen Benutzer unterscheidet, das System als temporärer Benutzer betreibt.

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

A.3.2.1 Erklärung der Zielsysteme in diesem Beispiel

Das System dieses Beispiels sieht wie folgt aus (siehe Bild B.1):

- Ziel dieses Systems ist die automatisierte Lichtsteuerung unter Verwendung von Personensensoren und Zeitdaten.
- Wenn die Bewegung einer Person um den Ort herum wahrgenommen wird, an dem der Beleuchtungskörper aufgestellt ist, wird der Beleuchtungskörper eingeschaltet, wenn es sich um eine andere Zeitzone als den Tag handelt (weil es hell ist, auch wenn er tagsüber nicht leuchtet).
- Für jeden Beleuchtungskörper gibt es eine intelligente Lichtsteuerung.
- Eine intelligente Lichtsteuerung ist mit einem oder mehreren Personensensoren und einer Uhr zur Zeitdatenerfassung verbunden.
- Die Stromversorgung der Fassung eines Beleuchtungskörpers erfolgt über einen normalen EIN/AUS-Schalter, und ein intelligenter Beleuchtungskörper dient dazu, von der intelligenten Lichtsteuerung eine Anweisung zum Ein- und Ausschalten des Lichts zu erhalten.
- Anwendungssoftware, die auf einem Smartphone läuft, wird als Schnittstelle für den Benutzer verwendet, um das Ein- und Ausschalten direkt zu unterstützen.
- Der Ein/Aus-Befehl der Anwendung auf dem Smartphone hat Vorrang vor allen anderen.
- Mit Hilfe der Anwendungssoftware auf dem Smartphone kann der Benutzer den EIN/AUS-Zustand aller Beleuchtungskörper und die Fehler aller Sensoren bestätigen.

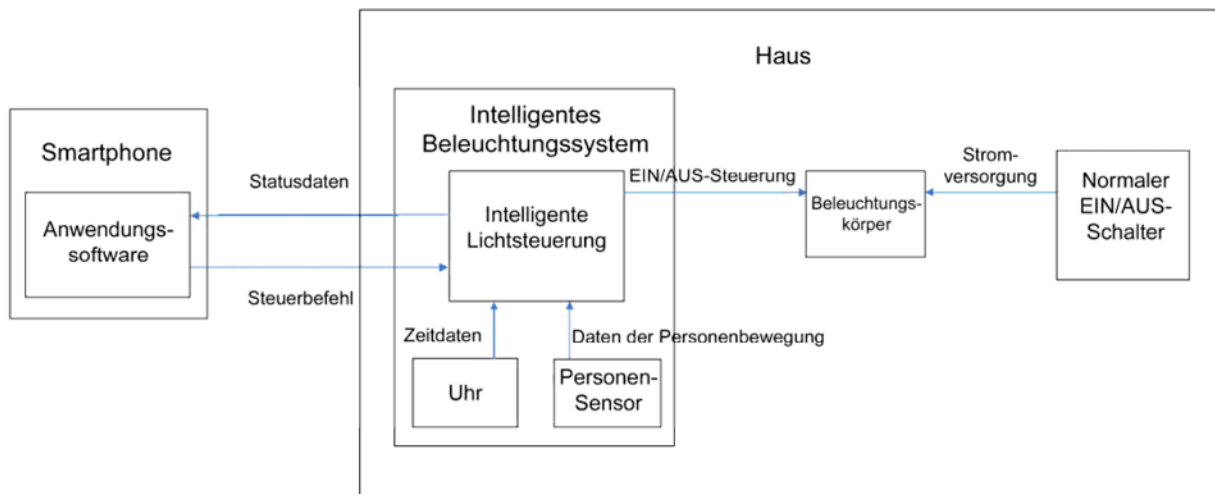


Bild A.1 – Systemdiagramm des Beispiels

Die folgenden Punkte werden als Regeln der intelligenten Lichtsteuerung dargestellt.

- Der Steuerbefehl der Smartphone-Anwendungssoftware hat Vorrang vor allem.
- Tagsüber (AM 11 – PM 4): Grundlegende Beleuchtung AUS, an dunklen Orten (wie Toilette, Flur, Treppenhaus) Beleuchtung EIN mit Personensensordaten
- Außerhalb der Tageszeit (PM 4 – AM 11): Beleuchtung EIN / AUS mit Personensensordaten
- Wenn die Daten des Personensensors nicht an der Steuerung angekommen sind, Beleuchtung AUS bei Tag und Nacht (PM 11 – AM 7), Beleuchtung EIN bei anderen Zeiten als Tag und Nacht

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, es als ein tatsächliches Problem erscheinen zu lassen. Die Tatsache, dass die Benutzerschnittstelle, außer der Anwendungssoftware auf dem Smartphone, nicht existiert, ist kein Problem, wenn alle Benutzer ein Smartphone besitzen. Selbst wenn eine Fehlfunktion durch einen Ausfall des Personensensors auftritt, hängt es von der AAL-Benutzerdomäne des Benutzers ab, ob der Benutzer es als Problem empfindet. Darüber hinaus ist der Betrieb der Beleuchtung mit Hilfe von Anwendungen auf dem Smartphone zulässig, und eine Situation 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 nicht als Problem des Systems für normale Anwender betrachtet wird.

Es ist jedoch klar, dass die Kontrolle des Benutzers auf das Smartphone beschränkt ist und wenn es ein Problem mit der Situation gibt, dass nur Benutzer, die das Smartphone nicht benutzen können, nicht berücksichtigt werden, ist es offensichtlich gefährlich. Benutzer, die das System vorübergehend als Besucher nutzen, deren AAL-Benutzerdomäne eine andere ist, können häufig in einem Wohnumfeld vorkommen. Die nicht ausreichende Beleuchtung, die bei normalen Anwendern nicht auffällt, ist auch für temporäre Anwender mit leichten Augenabweichungen, z. B. durch Alterung, ein wichtiges Problem. So besteht für einen temporären Benutzer beim Gehen mit schlechten Füßen wenig Gefahr, auf einen normalen ebenen Boden zu fallen, aber es ist durchaus anzunehmen, dass die Sturzgefahr auf einer Bodenfläche mit Stufen wie Treppen größer wird.

A.3.2.3 Beschreibung des erzählerischen Szenarios dieses Beispiels

Ein Szenario, in dem das Problem in dem System, das in diesem Beispiel dargestellt ist, offensichtlich wird, wird problemlos angenommen und ist kein spezielles Szenario. In diesem Beispiel entspricht ein solches Szenario einem Szenario, das die folgenden Bedingungen erfüllt:

- Der ursprüngliche Benutzer ist sich der Anomalie des Systems nicht bewusst oder hat es verlassen, weil er keine Unannehmlichkeiten verspürt, selbst wenn er es bemerkt.

- Ein temporärer Benutzer, der nicht der ursprüngliche Benutzer ist, bleibt für einen kurzen Zeitraum (mehrere Tage).
- Der temporäre Benutzer unterscheidet sich vom ursprünglichen Benutzer in der AAL-Benutzerdomäne, und selbst wenn die Situation für den ursprünglichen Benutzer keine Rolle spielt, kann es eine gefährliche Situation für den temporären Benutzer sein.
- Der temporäre Benutzer ist nicht gut darin, ein Smartphone zu benutzen.
- Temporäre Benutzer werden mit dem ursprünglichen Benutzer, der das Smartphone nicht benutzen kann, allein zu Hause gelassen.

Als erzählerische Beschreibung, die einem solchen Szenario entspricht, ist es möglich, Folgendes zu berücksichtigen.

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 Zeit und der Ausgangsinformation, der in jedem Raum, Flur und Treppenhaus installierten menschlichen Sensoren. Insbesondere, wenn die Person anwesend ist und der Raum dunkel wird, werden die Lichter automatisch eingeschaltet. Anwohner 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) verstehen es.

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 fand diesen Fehler. Der Sensor war in der Lage, eine Person zu erkennen, die sich von der unteren Treppe auf die obere Treppe bewegt, aber er konnte keine Person erkennen, die sich von der oberen Treppe auf die untere Treppe bewegt. Nach einer Weile versuchte Takuji die Treppe hinunterzugehen und die Lichter der Treppe leuchteten nicht auf. Takuji betätigte den normalen EIN/AUS-Schalter an der Wand, da die Treppe etwas dunkel war, um ohne Beleuchtung die Treppe hinunterzugehen.

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 lautstark nach Shota, was los sei. Shota verstand, dass die intelligente Beleuchtung der Treppe nicht richtig 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 bedienen. Takuji konnte sicher nach unten gelangen.

A.3.3 Erstellung eines Anwendungsfalles 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“ des „1.8 Beschreibung des Anwendungsfalles“ der AAL-Anwendungsfallvorlage wird mit der Extraktion aller Akteure aus dem Erzählszenario und dem Systemdiagramm begonnen. In diesem erzählerischen Szenario existieren vier Personen. Aber Masarus Frau wirkt nicht mit in diesem Szenario, drei Personen wurden aufgelistet:

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

Aus dem Systemdiagramm sind drei Elemente (z. B. Smartphone, intelligentes Beleuchtungssystem, intelligente Beleuchtungskörper) und ein Element (z. B. normaler Ein-/Ausschalter) ersichtlich. Im Smartphone gibt es Anwendungssoftware und im intelligenten Beleuchtungssystem gibt es eine Uhr, viele Sensoren und viele intelligente Lichtsteuerungen. Dazu wurden acht Systeme aufgelistet:

- Intelligentes Beleuchtungssystem