

	DIN IEC 63168-4 (VDE 0750-34-4)	DIN
	Diese Norm ist zugleich eine VDE-Bestimmung im Sinne von VDE 0022. Sie ist nach Durchführung des vom VDE-Präsidium beschlossenen Genehmigungsverfahrens unter der oben angeführten Nummer in das VDE-Vorschriftenwerk aufgenommen und in der „etz Elektrotechnik + Automation“ bekannt gegeben worden.	VDE

ICS 11.180.01; 97.120

Einsprüche bis 2022-04-18

Entwurf

**Kooperative Mehrfachsysteme in vernetzten Wohnumfeldern –
AAL Anforderungen an funktionale Sicherheit von elektronischen
sicherheitsbezogenen Systemen –
Teil 4: Produktion, Betrieb, Modifikation und Unterstützungsprozess
(IEC SyCAAL/210/CDV:2021);
Text Deutsch und Englisch**

Cooperative multiple systems in connected home environments –
AAL functional safety requirements of electronic safety-related systems –
Part 4: Production, operation, modification and supporting process
(IEC SyCAAL/210/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 46 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.....	8
2 Normative Verweisungen.....	8
3 Begriffe.....	8
4 Abkürzungen.....	9
5 Überblick.....	9
5.1 Überblick über die Sicherheitsaktivitäten nach der Produktionsfreigabe.....	9
5.2 Unterstützungsprozesse in der gesamten Norm IEC 63168 (alle Teile).....	10
6 Sicherheitsaktivitäten während der Produktion und der Produktionsprüfung.....	10
6.1 Zweck der Beschreibung der Sicherheitsaktivitäten während der Produktion und der Produktionsprüfung.....	10
6.2 Allgemeines.....	10
6.3 Für Sicherheitsaktivitäten während der Produktion und der Produktionsprüfung erforderliche Informationen.....	10
6.4 Anforderungen und Empfehlungen.....	11
6.4.1 Produktionsplan.....	11
6.4.2 Produktionsprüfplan.....	11
6.4.3 Personal.....	11
6.4.4 Prozessfähigkeit.....	11
6.4.5 Dokumentation.....	11
6.4.6 Nichterfüllung.....	11
6.4.7 Lager- und Transportbedingungen.....	11
6.5 Arbeitsergebnisse.....	11
7 Sicherheitsaktivitäten während Betrieb, Instandhaltung und Außerbetriebnahme.....	12
7.1 Zweck der Beschreibung der Sicherheitsaktivitäten während Betrieb, Instandhaltung und Außerbetriebnahme.....	12
7.2 Allgemeines.....	12
7.3 Für die Sicherheitsaktivitäten während Betrieb, Instandhaltung und Außerbetriebnahme erforderliche Informationen.....	12
7.4 Anforderungen und Empfehlungen.....	12
7.4.1 Instandhaltungsplanung.....	12
7.4.2 Reparaturanweisungen.....	12
7.4.3 Technische Instandhaltungsanweisungen.....	13
7.4.4 Benutzerinformationen.....	13
7.4.5 Felduntersuchungen.....	13
7.4.6 Außerbetriebnahme und Demontage.....	13

7.5	Arbeitsergebnisse.....	13
8	Schnittstellen innerhalb verteilter Entwicklungen.....	13
8.1	Zweck.....	13
8.2	Allgemeines.....	13
8.3	Für Schnittstellen innerhalb verteilter Entwicklungen erforderliche Informationen.....	14
8.4	Anforderungen und Empfehlungen.....	14
8.4.1	Anwendung der Anforderungen.....	14
8.4.2	Lieferantenauswahlkriterien.....	14
8.4.3	Einleitung und Planung einer verteilten Entwicklung.....	14
8.4.4	Durchführung einer verteilten Entwicklung.....	15
8.4.5	Bewertung der funktionalen Sicherheit am Standort des Lieferanten.....	15
8.4.6	Nach der Produktionsfreigabe.....	15
8.5	Arbeitsergebnisse.....	15
9	Konfigurationsmanagement.....	15
9.1	Zweck.....	15
9.2	Allgemeines.....	16
9.3	Für das Konfigurationsmanagement erforderliche Informationen.....	16
9.4	Anforderungen und Empfehlungen.....	16
9.5	Arbeitsergebnisse.....	16
10	Änderungsmanagement.....	16
10.1	Zweck.....	16
10.2	Allgemeines.....	16
10.3	Für das Änderungsmanagement erforderliche Informationen.....	16
10.4	Anforderungen und Empfehlungen.....	17
10.4.1	Planung und Einleitung des Änderungsmanagements.....	17
10.4.2	Änderungsanforderung.....	17
10.4.3	Analyse von Änderungsanforderungen.....	17
10.4.4	Beurteilung der Änderungsanforderung.....	17
10.4.5	Durchführung und Dokumentation der Änderung.....	18
10.5	Arbeitsergebnisse.....	18
11	Verifizierung.....	18
11.1	Zweck.....	18
11.2	Allgemeines.....	18
11.3	Für die Verifizierung der Arbeitsergebnisse erforderliche Informationen.....	18
11.4	Anforderungen und Empfehlungen.....	19
11.4.1	Planung der Verifizierung.....	19
11.4.2	Verifizierungsspezifikation.....	19
11.4.3	Durchführung und Beurteilung der Verifizierung.....	20
11.5	Arbeitsergebnisse.....	20
12	Dokumentation.....	

12.1	Zweck.....	20
12.2	Allgemeines.....	20
12.3	Für die Dokumentation erforderliche Informationen.....	20
12.4	Anforderungen und Empfehlungen.....	21
12.4.1	Dokumentationsprozess.....	21
12.4.2	Formale Elemente.....	21
12.4.3	Eigenschaften von Dokumenten.....	21
12.4.4	Speicherung des Sicherheitsdokuments.....	21
12.5	Arbeitsergebnisse.....	21
Anhang A (informativ) Checkliste für technische Unterlagen.....		22
Literaturhinweise		24
Bilder		
Bild 1 – Kooperative Mehrfachsysteme.....		6
Bild 2 – Sicherheitslebenszyklus.....		7
Tabellen		
Tabelle 1 – Struktur von IEC 63168 (alle Teile)/betreffende Leser jedes Teils.....		7
Tabelle A.1 – Checkliste für technische Unterlagen.....		22

Nationales Vorwort

Das internationale Dokument IEC SyCAAL/210/CDV:2021-01 „Cooperative multiple systems in connected home environments – AAL functional safety requirements of electronic safety-related systems – Part 4: Production, operation, modification and supporting process“ (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) legt AAL-spezifische Anforderungen an die funktionale Sicherheit von elektrischen/elektronischen (E/E) sicherheitsbezogenen Systemen für kooperative Mehrfachsysteme fest, die gemeinsam in einem vernetzten Wohnumfeld betrieben werden, wie in [Bild 1](#) dargestellt.

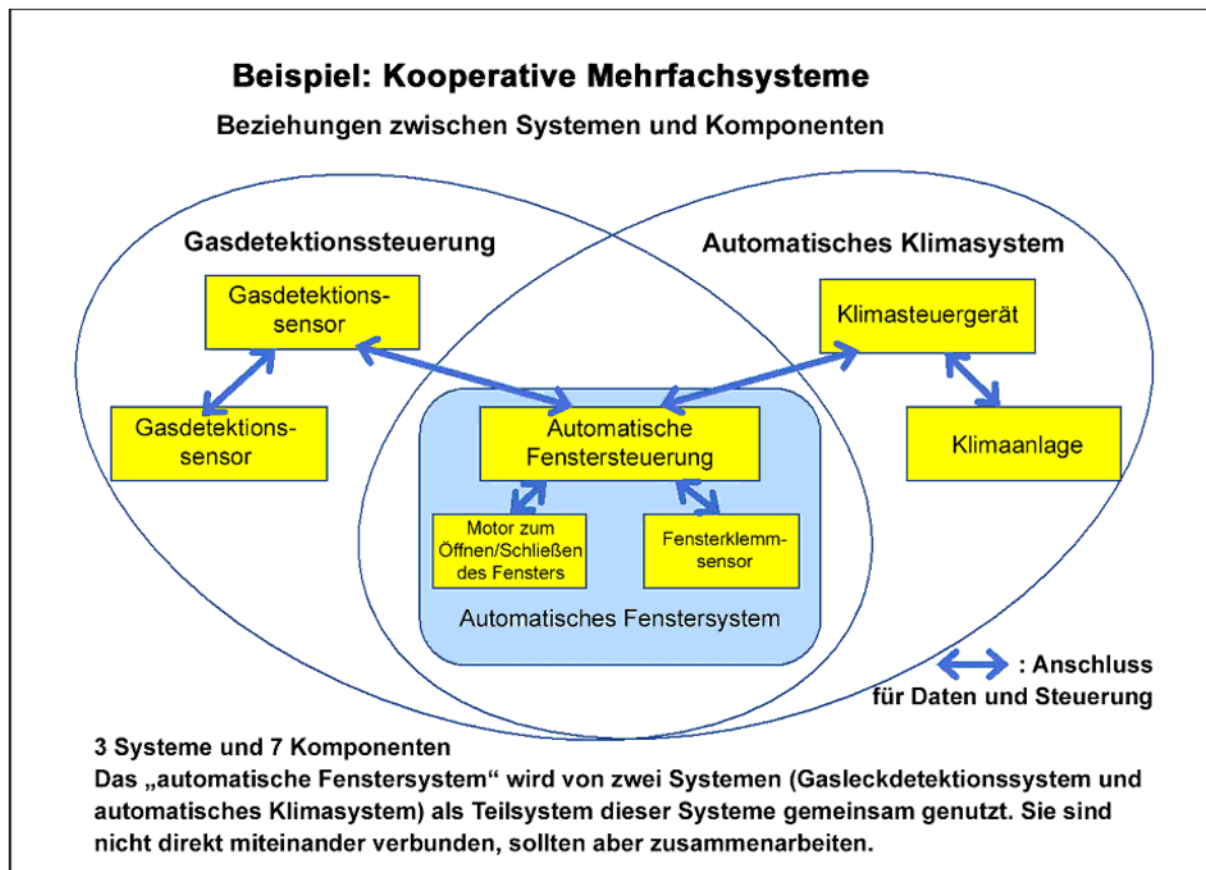


Bild 1 – Kooperative Mehrfachsysteme

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

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

IEC 63168 (alle Teile) besteht aus vier Teilen:

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

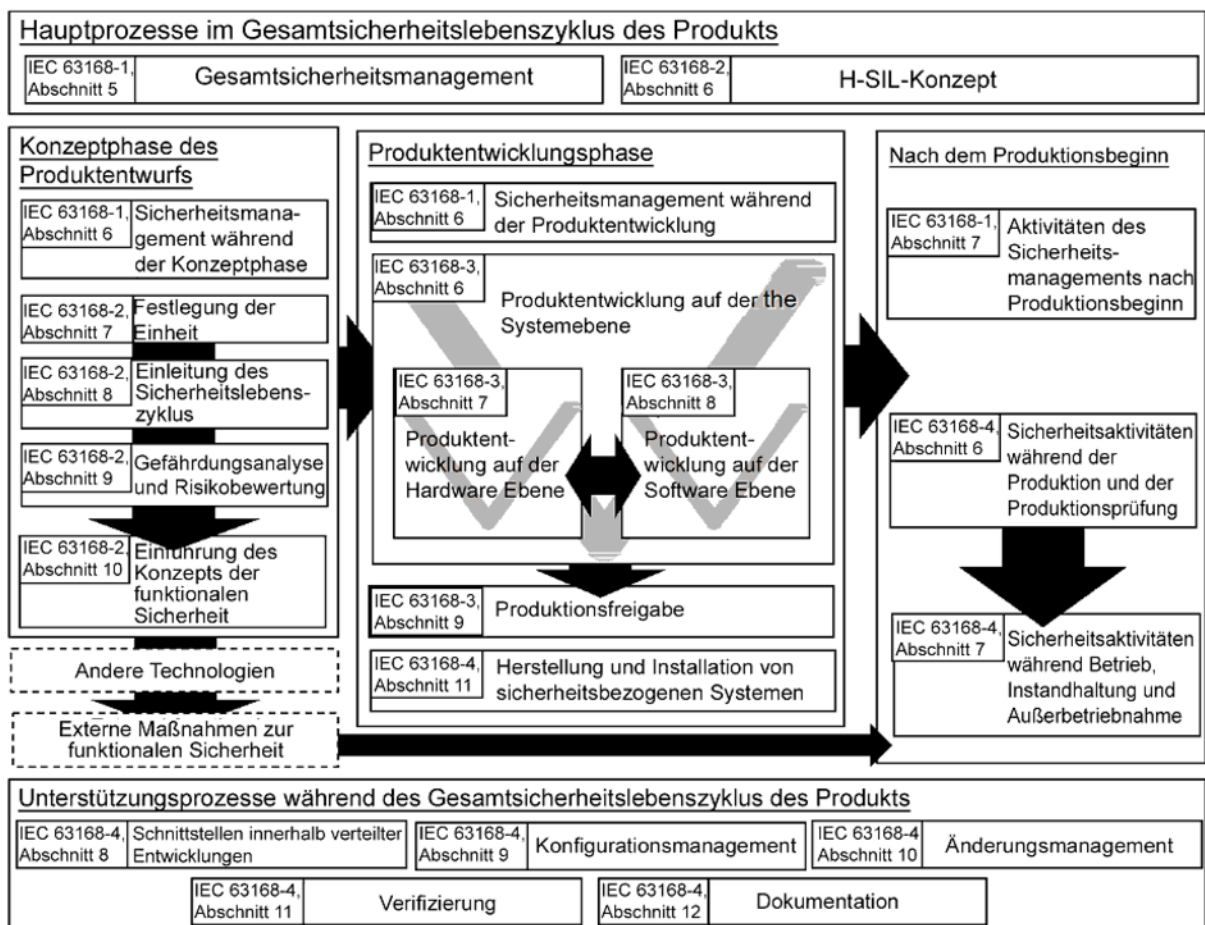
wie in [Tabelle 1](#) angegeben.

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

Teil	Titel	Betreffende Leser
1	Allgemeine Anforderungen an Design und Entwicklung	Alle mit Sicherheitsfragen in einem vernetzten Wohnumfeld Beschäftigten
2	Konzeptphase des Produktdesigns	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 2 Zu Instandhaltungsdienstleistern gehören auch Organisationen von Instandhaltungsdienstleistern.

Dieses Dokument legt die Sicherheitsaktivitäten fest, die in der Betriebsphase des Sicherheitslebenszyklus durchgeführt werden, wie in Bild 2 dargestellt. Die betreffenden Leser dieses Dokuments sind Errichter, Instandhaltungsdienstleister und Planer von kooperativen Mehrfachsystemen in vernetzten Wohnumfeldern, die für den Betrieb und die Instandhaltung von kooperativen Systemen verantwortlich sind. Dieses Dokument stellt wirksame Mittel zur fortlaufenden Verbesserung des kooperativen Systems bereit.



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

Bild 2 – Sicherheitslebenszyklus

Kooperative Mehrfachsysteme in vernetzten Wohnumfeldern – AAL Anforderungen an funktionale Sicherheit von elektronischen sicherheitsbezogenen Systemen – Teil 4: Produktion, Betrieb, Modifikation und Unterstützungsprozess

1 Anwendungsbereich

Dieses Dokument legt Verfahren für den fortgesetzten sicheren Betrieb von kooperativen Mehrfachsystemen, die für den Einsatz im vernetzten AAL-Heim Umfeld vorgesehen sind, nach dem Produktionsbeginn fest. Die Verfahren sind für Errichter, Instandhaltungsdienstleister und Planer bestimmt und gelten für den gesamten Systemlebenszyklus.

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

2 Normative Verweisungen

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

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

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

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

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

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

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

IEC 63168-2:20XX, *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*

3 Begriffe

Für die Anwendung dieses Dokuments gelten die Begriffe nach IEC 63168-1, IEC 63168-2, IEC 63168-3 und 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

Leistungsschnittstellenvereinbarung

LSV

Vereinbarung zwischen Kunde und Lieferant, in der die Verantwortlichkeiten für die auszuführenden Tätigkeiten, die zu prüfenden Nachweise oder die von jeder Partei auszutauschenden Arbeitsergebnisse im Zusammenhang mit der Entwicklung von Einheiten oder Elementen festgelegt werden

[QUELLE: ISO 26262-1:2018, 3.32, modifiziert – Anmerkung 1 zum Begriff gestrichen]

3.2

verteilte Entwicklung

Entwicklung einer Einheit oder eines Elements mit geteilter Entwicklungsverantwortung zwischen Kunde und Lieferant(en) für die gesamte Einheit oder das gesamte Element

Anmerkung 1 zum Begriff: Kunde und Lieferant sind die Rollen der kooperierenden Parteien.

[QUELLE: ISO 26262-1:2018, 3.36]

3.3

Felddaten

Daten, die aus dem Einsatz einer Einheit oder eines Elements gewonnen werden, einschließlich der kumulativen Betriebsstunden, aller Ausfälle und Sicherheitsanomalien während des Betriebs

Anmerkung 1 zum Begriff: Felddaten stammen in der Regel aus dem Einsatz beim Kunden.

[QUELLE: ISO 26262-1:2018, 3.62]

3.4

Modifikation

Schaffung einer neuen Einheit aus einer bestehenden Einheit

Anmerkung 1 zum Begriff: Modifikation wird in IEC 63168 (alle Teile) in Bezug auf die Wiederverwendung zur 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 Einheit zu schaffen.

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

4 Abkürzungen

Für die Anwendung dieses Dokuments gelten die Abkürzungen nach IEC 63168-1, IEC 63168-2, IEC 63168-3 und die folgenden Abkürzungen.

LSV	Leistungsschnittstellenvereinbarung (en: development interface agreement)
RFQ	Angebotsanforderung (en: request for quotation)

5 Überblick

5.1 Überblick über die Sicherheitsaktivitäten nach der Produktionsfreigabe

Die Sicherheitsaktivitäten, die in der Phase nach der Produktionsfreigabe des Produktdesigns durchgeführt werden, werden in die folgenden zwei Prozesse unterteilt:

- Sicherheitsaktivitäten während der Produktion und der Produktionsprüfung ([Abschnitt 6](#)); und
- Sicherheitsaktivitäten während des Betriebs, der Instandhaltung und der Außerbetriebnahme ([Abschnitt 7](#)).

5.2 Unterstützungsprozesse in der gesamten Norm IEC 63168 (alle Teile)

Nachstehend werden die Unterstützungsprozesse angegeben, die in Abhängigkeit von der Situation für die Durchführung der Sicherheitsaktivitäten nach IEC 63168 (alle Teile) erforderlich sind:

- Schnittstellen innerhalb verteilter Entwicklungen ([Abschnitt 8](#));
- Konfigurationsmanagement ([Abschnitt 9](#));
- Änderungsmanagement ([Abschnitt 10](#));
- Verifizierung ([Abschnitt 11](#)); und
- Dokumentation ([Abschnitt 12](#)).

6 Sicherheitsaktivitäten während der Produktion und der Produktionsprüfung

6.1 Zweck der Beschreibung der Sicherheitsaktivitäten während der Produktion und der Produktionsprüfung

Das erste Ziel ist die Entwicklung und Aufrechterhaltung eines Produktionsprozesses für sicherheitsbezogene Elemente oder Einheiten, die in einem vernetzten Wohnumfeld installiert werden.

Das zweite Ziel ist das Erreichen der funktionalen Sicherheit während des Produktionsprozesses durch den jeweiligen Hersteller oder die für den Prozess verantwortliche Person oder Organisation (Hersteller der Einheit, Lieferant, Unterlieferant usw.).

6.2 Allgemeines

Die Übereinstimmung mit sicherheitsbezogenen Sondereigenschaften von Einheiten oder Elementen während ihrer Produktion, die in den Entwicklungsphasen festgelegt werden, ist notwendig, um funktionale Sicherheit zu erreichen. Beispiele für solche sicherheitsbezogenen Sondereigenschaften sind bestimmte Prozessparameter (z. B. Temperaturbereich oder Anzugsdrehmoment), Materialeigenschaften, Fertigungstoleranzen oder Konfiguration.

In dieser Phase werden Anforderungen definiert, die sicherstellen, dass die funktionale Sicherheit während des Produktionsprozesses erreicht wird, indem diese sicherheitsbezogenen Sondereigenschaften auch in die Produktionsplanung und -prüfung einbezogen werden.

6.3 Für Sicherheitsaktivitäten während der Produktion und der Produktionsprüfung erforderliche Informationen

Die folgenden Informationen müssen zur Verfügung gestellt werden:

- Anforderungsspezifikation für Produktion, Betrieb, Instandhaltung und Außerbetriebnahme in Übereinstimmung mit IEC 63168-3:20XX, 6.3.5 und 7.3.5; und
- Produktionsfreigabebericht in Übereinstimmung mit IEC 63168-3:20XX.

Die folgenden Informationen können berücksichtigt werden:

- Produktionsplan (von einer externen Quelle);
- Anmerkungen zur Montage (Dokumentation der Komponenten oder Funktionen, die durch die Montage beeinflusst werden können; von einer externen Quelle); und
- Anmerkungen zu Prüfungen (von einer externen Quelle).

6.4 Anforderungen und Empfehlungen

6.4.1 Produktionsplan

Der Produktionsplan muss unter Berücksichtigung der Montageanweisungen Folgendes enthalten:

- Kennzeichnung von sicherheitsbezogenen Eigenschaften;
- Reihenfolge und Verfahren der Produktionsschritte;
- Montageausrüstung/Werkzeuge.

6.4.2 Produktionsprüfplan

Die Prüfplan muss umfassen:

- Kennzeichnung von sicherheitsbezogenen Eigenschaften;
- Reihenfolge und Verfahren der Produktionsschritte;
- Prüfeinrichtungen/Werkzeuge, Prüfkriterien; und
- Häufigkeit von Produktionsprüfungen.

6.4.3 Personal

Produktion und Prüfungen müssen von ausgebildetem Personal nach den Produktions- und Prüfplänen durchgeführt werden.

6.4.4 Prozessfähigkeit

Die Prozessfähigkeit muss durch branchenübliche Anforderungen sichergestellt werden.

6.4.5 Dokumentation

Die Durchführung der Prüfungen nach dem Prüfplan muss dokumentiert werden. Die Prüfdokumentation muss mindestens das Datum der Prüfung, den Prüfer, eine eindeutige Kennzeichnung des Teils und die Prüfergebnisse enthalten.

6.4.6 Nichterfüllung

Eine Vorgehensweise im Fall der Nichterfüllung eines Prüfkriteriums muss aufgestellt werden. Eine Nachbearbeitung ist nur bei Nachweis einer geeigneten Prozesssteuerung zulässig.

6.4.7 Lager- und Transportbedingungen

Bei Lagerung und Transport des Produkts müssen alle besonderen Handhabungs- und Verpackungsanforderungen für die Einheit oder das Element eingehalten werden.

6.5 Arbeitsergebnisse

- a) Sicherheitsbezogener Inhalt des Produktionsplans nach [6.4.1 bis 6.4.7](#).
- b) Sicherheitsbezogener Inhalt des Produktionsprüfplans nach [6.4.1 bis 6.4.6](#).
- c) Produktionsprüfbericht nach [6.4.2 bis 6.4.6](#).

7 Sicherheitsaktivitäten während Betrieb, Instandhaltung und Außerbetriebnahme

7.1 Zweck der Beschreibung der Sicherheitsaktivitäten während Betrieb, Instandhaltung und Außerbetriebnahme

Das Ziel ist die Festlegung von Benutzerinformationen, Instandhaltungs- und Reparaturanweisungen sowie Demontageanweisungen für die Einheit oder das Element, um die geforderte funktionale Sicherheit während Betrieb, Instandhaltung, Reparatur und Außerbetriebnahme aufrechtzuerhalten.

7.2 Allgemeines

Die Anforderungen an die funktionale Sicherheit während der Instandhaltungs- und Reparaturtätigkeiten können sich von denen unterscheiden, die während des Betriebs erforderlich sind.

Der Inhalt von [Abschnitt 7](#) stellt Anforderungen für die Erstellung von Reparaturanweisungen und Benutzerinformationen sowie für die Planung, Durchführung und Überwachung von Instandhaltungsarbeiten unter Berücksichtigung der sicherheitsbezogenen Sondereigenschaften der Einheit bereit.

7.3 Für die Sicherheitsaktivitäten während Betrieb, Instandhaltung und Außerbetriebnahme erforderliche Informationen

Die folgenden Informationen müssen zur Verfügung gestellt werden:

- Anforderungsspezifikation für Produktion, Betrieb, Instandhaltung und Außerbetriebnahme in Übereinstimmung mit IEC 63168-3:20XX, 6.3.5 und 7.3.5;
- Produktionsfreigabebericht in Übereinstimmung mit IEC 63168-3:20XX, 9.5; und
- Konzept der funktionalen Sicherheit in Übereinstimmung mit IEC 63168-2:20XX, 9.5.

Die folgenden Informationen können berücksichtigt werden:

- Instandhaltungsplan (von einer externen Quelle).

7.4 Anforderungen und Empfehlungen

7.4.1 Instandhaltungsplanung

Der Instandhaltungsplan muss parallel zum Systemdesign aufgestellt werden und muss Folgendes enthalten:

- Kennzeichnung von Komponenten mit sicherheitsbezogenen Eigenschaften unter Berücksichtigung der jeweiligen freigegebenen Teilsystem- oder Systemkonfiguration; und
- Ablauffolge, Verfahren (gegebenenfalls Werkzeuge) und Festlegung von Zeitintervall und Umfang der Instandhaltung für die Betriebszeit.

7.4.2 Reparaturanweisungen

Die Reparaturanweisungen müssen enthalten:

- Kennzeichnung von Komponenten mit sicherheitsbezogenen Eigenschaften;
- Arbeitsschritte und Arbeitsablauf, Verfahren und Werkzeuge (z. B. Programmier- und Diagnosegeräte, falls zutreffend);
- die jeweilige freigegebene Konfiguration des Systems oder Teilsystems;
- die zulässige Deaktivierung von Teilsystemen oder Systemen und die zusätzlichen Anpassungen, die an der gesamten Einheit erforderlich sind; und
- die Ersatzteilversorgung mit neuen Komponenten oder zugelassenen Ersatzkomponenten.

7.4.3 Technische Instandhaltungsanweisungen

Reparatur- und Instandsetzungsarbeiten müssen:

- von entsprechend ausgebildetem Personal durchgeführt werden; und
- nach dem Instandhaltungszeitplan oder den Reparaturanweisungen durchgeführt und dokumentiert werden.

7.4.4 Benutzerinformationen

Benutzerinformationen (z. B. Betriebsanweisungen) müssen vorbereitet werden. Diese Betriebsanweisungen müssen in das Betriebshandbuch aufgenommen werden und Folgendes enthalten:

- Kennzeichnung von Komponenten mit sicherheitsbezogenen Eigenschaften;
- Warnungen vor möglichen Gefährdungen, die sich aus der Interaktion mit Produkten Dritter ergeben;
- Beschreibung des Teilsystems oder Systems und von Zustandsinformationen (Anzeigekonzept) und der erforderlichen Benutzerreaktion;
- Beschreibung der erforderlichen Komponenten für die Instandhaltung; und
- Warnungen vor Modifikationen am sicherheitsbezogenen System.

7.4.5 Felduntersuchungen

Es muss ein Prozess der Felduntersuchung eingerichtet werden. Auf der Grundlage der Ergebnisse der Analysen müssen geeignete Maßnahmen eingeleitet werden.

7.4.6 Außerbetriebnahme und Demontage

Die Anforderungen an die Außerbetriebnahme und Demontage der Einheit müssen vom Hersteller angegeben werden.

7.5 Arbeitsergebnisse

- a) Sicherheitsbezogener Inhalt des Instandhaltungsplans nach 7.4.1 und 7.4.3.
- b) Reparaturanweisungen nach 7.4.1 und 7.4.2.
- c) Sicherheitsbezogener Inhalt der Informationen, die dem Benutzer zur Verfügung gestellt werden, nach 7.4.4.
- d) Anweisungen für Felduntersuchungen nach Anforderung 7.4.5.
- e) Sicherheitsbezogener Inhalt der Anweisungen für die Außerbetriebnahme nach 7.4.6.

8 Schnittstellen innerhalb verteilter Entwicklungen

8.1 Zweck

Das Ziel der Einbeziehung von Inhalten für Schnittstellen innerhalb verteilter Entwicklungen ist die Beschreibung der Verfahren und die Zuweisung der zugehörigen Verantwortlichkeiten innerhalb verteilter Entwicklungen für Einheiten und Elemente, die nach IEC 63168 (alle Teile) ausgeführt werden.

8.2 Allgemeines

Der Kunde (z. B. Hausbauer) und die Lieferanten für die Entwicklung von Einheiten erfüllen gemeinsam die in IEC 63168 (alle Teile) festgelegten Anforderungen. Die Verantwortlichkeiten werden zwischen dem Kunden und den Lieferanten vereinbart. Beziehungen zu Unterauftragnehmern sind zulässig. Ebenso wie bei den sicherheitsbezogenen Spezifikationen des Kunden für Planung, Durchführung und Dokumentation bei Eigenentwicklungen von Einheiten werden vergleichbare Verfahren für die Zusammenarbeit mit dem

Lieferanten bei verteilten Entwicklungen von Einheiten oder bei Entwicklungen von Einheiten, bei denen der Lieferant die volle Sicherheitsverantwortung trägt, vereinbart.

ANMERKUNG Ein „Kunde“ ist definiert als eine Organisation, die Teile oder Systeme von anderen Lieferanten bezieht, um ein koordiniertes System zu entwickeln und zu errichten. Eine Organisation kann sowohl Kunde als auch Lieferant sein.

8.3 Für Schnittstellen innerhalb verteilter Entwicklungen erforderliche Informationen

Es werden Informationen zu den entsprechenden Phasen des Sicherheitslebenszyklus benötigt, in denen die verteilte Entwicklung geplant und durchgeführt wird.

Die folgenden Informationen können berücksichtigt werden:

- die Entwurfsversion einer Leistungsschnittstellenvereinbarung (LSV) (von einer externen Quelle);
- das Angebot des Lieferanten auf der Grundlage einer Angebotsanforderung (RFQ) (von einer externen Quelle).

8.4 Anforderungen und Empfehlungen

8.4.1 Anwendung der Anforderungen

Die Anwendung der Anforderungen muss für jede Einheit und jedes Element gelten, die/das nach IEC 63168 (alle Teile) entwickelt wurde, mit Ausnahme von serienmäßigen Hardware-Teilen, wenn einer der folgenden Punkte zutrifft:

- a) Es gibt keine spezifischen Hardware-Sicherheitsanforderungen, die den Hardware-Teilen zugeordnet sind, oder
- b) die serienmäßigen Hardware-Teile werden nach gut eingeführten Verfahren auf der Grundlage weltweiter Qualitätsnormen qualifiziert und die Qualifizierung der serienmäßigen Hardware-Teile deckt Parameterbereiche im Hinblick auf die vorgesehene Anwendung ab.

Die Anforderungen an die Kunde-Lieferant-Beziehung (Schnittstellen und Interaktionen) müssen für jede Ebene der Kunde-Lieferant-Beziehung gelten.

8.4.2 Lieferantenauswahlkriterien

Die Lieferantenauswahlkriterien müssen eine Beurteilung der Fähigkeit des Lieferanten umfassen, Einheiten und Elemente mit vergleichbarer Komplexität und vergleichbarem H-SIL nach IEC 63168 (alle Teile) zu entwickeln und herzustellen.

8.4.3 Einleitung und Planung einer verteilten Entwicklung

Der Kunde und der Lieferant müssen eine LSV festlegen, die Folgendes umfasst:

- a) die Ernennung der Sicherheitsmanager des Kunden und des Lieferanten;
- b) die gemeinsame Anpassung des Sicherheitslebenszyklus in Übereinstimmung mit IEC 63168-1:20XX;
- c) die Aktivitäten und Prozesse, die vom Kunden durchgeführt werden, und die Aktivitäten und Prozesse, die vom Lieferanten durchgeführt werden;
- d) die Informationen und die Arbeitsergebnisse, die ausgetauscht werden;
- e) die Parteien oder Personen, die für die Aktivitäten verantwortlich sind;
- f) die Übermittlung der Zielwerte, die aus den Zielen auf Systemebene anhand der Beurteilung von Verletzungen des Sicherheitsziels aufgrund zufälliger Hardware-Ausfälle (siehe IEC 63168-3:20XX, Abschnitt 7) abgeleitet werden, an jede betreffende Partei, damit diese die Zielwerte einhalten kann; und
- g) die Unterstützungsprozesse und Werkzeuge, einschließlich von Schnittstellen, um die Kompatibilität zwischen Kunde und Lieferant sicherzustellen.