

	DIN IEC 63168-3 (VDE 0750-34-3)	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 3: Produktentwicklung
(IEC SyCAAL/209/CDV:2021);
Text Deutsch und Englisch**

Cooperative multiple systems in connected home environments –
AAL functional safety requirements of electronic safety-related systems –
Part 3: Product development
(IEC SyCAAL/209/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 156 Seiten

DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE

Anwendungsbeginn

Anwendungsbeginn dieser Norm ist ...

Inhalt

	Seite
Nationales Vorwort.....	8
Einleitung.....	9
1 Anwendungsbereich.....	12
2 Normative Verweisungen.....	12
3 Begriffe.....	12
4 Abkürzungen.....	15
5 Überblick und Anmerkungen.....	15
5.1 Überblick über Sicherheitsaktivitäten während der Produktentwicklungsphase des Produktentwurfs.....	15
5.2 Notationen und Interpretationen von Tabelle 2 bis Tabelle 21.....	16
5.3 Vom H-SIL abhängige Anforderungen und Empfehlungen.....	16
6 Produktentwicklung auf der Systemebene.....	17
6.1 Planung der Systementwicklung.....	17
6.1.1 Zweck.....	17
6.1.2 Allgemeines.....	17
6.1.3 Für die Planung der Systementwicklung erforderliche Informationen.....	18
6.1.4 Anforderungen an die Planung der Systementwicklung.....	19
6.1.5 Arbeitsergebnisse der Planung der Systementwicklung.....	19
6.2 Festlegung der Anforderungsspezifikation für die technische Sicherheit.....	19
6.2.1 Zweck dieser Unterphase.....	19
6.2.2 Allgemeines.....	19
6.2.3 Informationen für die Festlegung der Anforderungsspezifikation für die technische Sicherheit.....	19
6.2.4 Anforderungen und Empfehlungen.....	20
6.2.5 Arbeitsergebnisse.....	21
6.3 Sicherheitsaktivitäten während des Systemdesigns.....	21
6.3.1 Zweck der Sicherheitsaktivitäten während des Systemdesigns.....	21
6.3.2 Allgemeines.....	21
6.3.3 Für Sicherheitsaktivitäten während des Systementwurfs erforderliche Informationen.....	22
6.3.4 Anforderungen und Empfehlungen.....	22
6.3.5 Arbeitsergebnisse.....	25
6.4 Integration und Prüfung von Einheiten.....	25
6.4.1 Zweck der Integration und Prüfung von Einheiten.....	25
6.4.2 Allgemeines.....	26
6.4.3 Für die Integration und Prüfung von Einheiten erforderliche Informationen.....	26
6.4.4 Anforderungen und Empfehlungen.....	26
6.4.5 Arbeitsergebnisse.....	29

6.5	Sicherheitsvalidierung.....	29
6.5.1	Zweck der Sicherheitsvalidierung.....	29
6.5.2	Allgemeines.....	29
6.5.3	Für die Sicherheitsvalidierung erforderliche Informationen.....	29
6.5.4	Anforderungen und Empfehlungen.....	29
6.5.5	Arbeitsergebnisse.....	30
7	Produktentwicklung auf der Hardware-Ebene.....	30
7.1	Planung der Hardware-Entwicklung.....	30
7.1.1	Zweck.....	30
7.1.2	Allgemeines.....	30
7.1.3	Für die Planung der Hardware-Entwicklung erforderliche Informationen.....	31
7.1.4	Anforderungen und Empfehlungen.....	32
7.1.5	Arbeitsergebnis.....	32
7.2	Festlegung der Spezifikation der Hardware-Sicherheitsanforderungen.....	32
7.2.1	Zweck.....	32
7.2.2	Allgemeines.....	32
7.2.3	Für die Festlegung der Spezifikation der Hardware-Sicherheitsanforderungen erforderliche Informationen.....	32
7.2.4	Anforderungen und Empfehlungen.....	33
7.2.5	Arbeitsergebnisse.....	34
7.3	Hardware-Design.....	34
7.3.1	Zweck des Hardware-Designs.....	34
7.3.2	Allgemeines.....	34
7.3.3	Für das Hardware-Design erforderliche Informationen.....	34
7.3.4	Anforderungen und Empfehlungen.....	35
7.3.5	Arbeitsergebnisse.....	37
7.4	Bewertung von Verletzungen der Sicherheitsziele aufgrund zufälliger Hardware-Ausfälle.....	37
7.4.1	Zweck.....	37
7.4.2	Allgemeines.....	37
7.4.3	Für die Bewertung der Verletzungen von Sicherheitszielen durch zufällige Hardware-Ausfälle erforderliche Informationen.....	37
7.4.4	Anforderungen und Empfehlungen.....	38
7.4.5	Arbeitsergebnisse.....	39
7.5	Hardware-Integration und Prüfung.....	39
7.5.1	Zweck der Integration und Prüfung von Hardware.....	39
7.5.2	Allgemeines.....	39
7.5.3	Für die Integration und Prüfung von Hardware erforderliche Informationen.....	39
7.5.4	Anforderungen und Empfehlungen.....	39
7.5.5	Arbeitsergebnisse.....	40
8	Produktentwicklung auf der Software-Ebene.....	40

8.1	Planung der Software-Entwicklung.....	40
8.1.1	Zweck der Planung der Software-Entwicklung.....	40
8.1.2	Allgemeines.....	40
8.1.3	Für die Planung der Software-Entwicklung erforderliche Informationen.....	41
8.1.4	Anforderungen und Empfehlungen.....	42
8.1.5	Arbeitsergebnisse.....	42
8.2	Festlegung der Spezifikation der Software-Sicherheitsanforderungen.....	42
8.2.1	Zweck der Festlegung der Spezifikation der Software-Sicherheitsanforderungen.....	42
8.2.2	Allgemeines.....	42
8.2.3	Für die Festlegung der Spezifikation der Software-Sicherheitsanforderungen erforderliche Informationen.....	42
8.2.4	Anforderungen und Empfehlungen.....	43
8.2.5	Arbeitsergebnisse.....	44
8.3	Software-Architekturdesign.....	44
8.3.1	Zweck des Software-Architekturdesigns.....	44
8.3.2	Allgemeines.....	44
8.3.3	Für das Software-Architekturdesign erforderliche Informationen.....	45
8.3.4	Anforderungen und Empfehlungen.....	45
8.3.5	Arbeitsergebnisse.....	47
8.4	Design und Implementierung von Software-Einheiten.....	47
8.4.1	Zweck des Designs und der Implementierung von Software-Einheiten.....	47
8.4.2	Allgemeines.....	47
8.4.3	Für das Design und die Implementierung von Software-Einheiten erforderliche Informationen.....	48
8.4.4	Anforderungen und Empfehlungen.....	48
8.4.5	Arbeitsergebnisse.....	50
8.5	Prüfung von Software-Einheiten.....	50
8.5.1	Zweck der Prüfung von Software-Einheiten.....	50
8.5.2	Allgemeines.....	50
8.5.3	Für die Prüfung von Software-Einheiten erforderliche Informationen.....	50
8.5.4	Anforderungen und Empfehlungen.....	51
8.5.5	Arbeitsergebnisse.....	51
8.6	Software-Integration und Prüfung.....	51
8.6.1	Zweck der Software-Integration und Prüfung.....	51
8.6.2	Allgemeines.....	52
8.6.3	Für die Software-Integration und Prüfung erforderliche Informationen.....	52
8.6.4	Anforderungen und Empfehlungen.....	52
8.6.5	Arbeitsergebnisse.....	53
8.7	Verifizierung der Software-Sicherheitsanforderungen.....	53
8.7.1	Ziel der Verifizierung der Software-Sicherheitsanforderungen.....	53
8.7.2	Allgemeines.....	53

8.7.3	Für die Verifizierung der Software-Sicherheitsanforderungen erforderliche Informationen.....	53
8.7.4	Anforderungen und Empfehlungen.....	54
8.7.5	Arbeitsergebnisse.....	54
8.8	Software-basierte Parametrierung.....	55
8.8.1	Ziel der Software-basierten Parametrierung.....	55
8.8.2	Allgemeines.....	55
8.8.3	Für die Software-basierte Parametrierung erforderliche Informationen.....	55
8.8.4	Anforderungen und Empfehlungen.....	55
8.8.5	Arbeitsergebnisse.....	56
9	Produktionsfreigabe.....	56
9.1	Zweck.....	56
9.2	Allgemeines.....	56
9.3	Für die Produktionsfreigabe erforderliche Informationen.....	56
9.4	Anforderungen und Empfehlungen.....	56
9.4.1	Produktionsfreigabe.....	56
9.4.2	Dokumentation für die Produktionsfreigabe.....	57
9.5	Arbeitsergebnisse.....	57
Anhang A (informativ)	Bewertung einer Wahrscheinlichkeitsmetrik für zufällige Hardware-Ausfälle.....	58
A.1	Allgemeines.....	58
A.2	MTTF _d -Werte der Komponenten.....	58
A.2.1	Ermittlung der MTTF _d -Werte von Komponenten.....	58
A.2.2	MTTF _d für Komponenten aus B ₁₀	59
A.3	Quantitative FMEA.....	59
A.4	Teilezahlverfahren.....	60
Anhang B (informativ)	Beurteilung des Diagnosedeckungsgrads.....	61
B.1	Allgemeines.....	61
B.2	Schätzung des erforderlichen Diagnosedeckungsgrads.....	61
Anhang C (normativ)	Überblick über Verfahren und Maßnahmen zum Erreichen der Sicherheitsintegrität der Software (siehe Abschnitt 8).....	64
C.1	Allgemeines.....	64
C.2	Spezifikationsverfahren für die Software-Sicherheitsanforderungen.....	64
C.2.1	Anforderungsspezifikation in natürlicher Sprache.....	64
C.2.2	Nichtformale Designmethoden.....	64
C.2.3	Semiformale Designmethoden.....	64
C.2.4	Formale Designmethoden.....	65
C.2.5	Rechnerunterstützte Spezifikationswerkzeuge.....	65
C.3	Software-Architektur und -Designmethoden.....	65
C.3.1	Ausfallanalyse – Bottom-up-Verfahren.....	65
C.3.2	Ausfallanalyse – Top-down-Verfahren.....	66
C.4	Methoden für Design und Implementierung von Software-Modulen.....	66

C.4.1	Geeignete Programmiersprache.....	66
C.4.2	Streng typisierte Programmiersprache oder Leitlinienprüfung.....	67
C.4.3	Werkzeuge und Übersetzer – erhöhtes Vertrauen durch die Anwendung.....	67
C.4.4	Verwendung bewährter/verifizierter Software-Module und -Komponenten (wenn verfügbar).....	68
C.4.5	Defensive Programmierung.....	69
C.4.6	Strukturierte Programmierung.....	69
C.4.7	Modularer Ansatz.....	70
C.4.8	Bibliothek bewährter/verifizierter Software-Module und -Komponenten.....	70
C.4.9	Rechnerunterstützte Designwerkzeuge.....	71
C.4.10	Anwendung von Codierstandards.....	71
C.4.11	Design- und Codierstandards – Keine Verwendung dynamischer Variablen oder Objekte.....	72
C.4.12	Design- und Codierstandards – Begrenzte Verwendung von Interrupts.....	72
C.4.13	Design- und Codierstandards – Definierte Verwendung von Zeigern.....	72
C.4.14	Design- und Codierstandards – Begrenzte Verwendung von Rekursionen.....	73
C.5	Prüfverfahren für Software-Einheiten.....	73
C.5.1	Dynamische Analyse und Prüfung.....	73
C.5.2	Durchführung von Prüffällen nach einer Grenzwertanalyse.....	73
C.5.3	Strukturgestützte Prüfungen.....	74
C.5.4	Grenzwertanalyse.....	74
C.5.5	Checklisten.....	75
C.5.6	Statische Analyse – Kontrollflussanalyse.....	76
C.5.7	Statische Analyse – Datenflussanalyse.....	76
C.5.8	Statische Analyse – Walk-through/Designüberprüfung.....	76
C.5.9	Prüfung von Äquivalenzklassen und Eingabepartitionen.....	77
C.5.10	Leistungsprüfungen.....	77
C.5.11	Leistungsprüfung – Prüfung des Ressourcenbudgets.....	77
C.5.12	Leistungsprüfung – Antwortzeiten und Speichergrenzen.....	78
C.5.13	Leistungsprüfung – Leistungsanforderungen.....	78
C.5.14	Leistungsprüfung – Avalanche-/Belastungsprüfungen.....	79
C.5.15	Schnittstellenprüfung.....	79
C.5	Prüfverfahren für Software-Einheiten.....	73
C.6.1	Funktionsprüfungen.....	80
C.7	Verifizierung der Verfahren zur Erfüllung der Software-Sicherheitsanforderungen.....	80
C.7.1	Prüfschnittstelle.....	80
C.7.2	Prüfungen innerhalb des Netzwerks der elektronischen Steuerungseinheit.....	80
C.7.3	Hardware-in-the-Loop-Prüfungen.....	80
C.7.4	Prüfungen in vernetzten Wohnumfeldern.....	80
Anhang D (informativ)	Checkliste für technische Unterlagen.....	81
Literaturhinweise		84

Bilder

Bild 1 – Kooperative Mehrfachsysteme.....	9
Bild 2 – Sicherheitslebenszyklus.....	10
Bild 3 – Referenzphasenmodell für die Entwicklung einer sicherheitsbezogenen Einheit.....	18
Bild 4 – Referenzphasenmodell für die Produktentwicklung auf Hardware-Ebene.....	31
Bild 5 – Referenzphasenmodell für die Produktentwicklung auf der Software-Ebene.....	41

Tabellen

Tabelle 1 – Struktur von IEC 63168 (alle Teile)/betreffende Leser jedes Teils.....	10
Tabelle 2 – Analyse des Systementwurfs.....	23
Tabelle 3 – Merkmale des modularen Systementwurfs.....	23
Tabelle 4 – Verifizierung des Systementwurfs.....	25
Tabelle 5 – Verfahren für Hardware-Software-Integrationsprüfung	27
Tabelle 6 – Verfahren für die Systemintegrationsprüfung.....	27
Tabelle 7 – Verfahren für die Integrationsprüfungen für das vernetzte Wohnumfeld.....	28
Tabelle 8 – Merkmale des modularen Hardware-Designs.....	35
Tabelle 9 – Sicherheitsanalyse des Hardware-Designs.....	36
Tabelle 10 – Verifizierung des Hardware-Designs.....	36
Tabelle 11 – Mögliche Quelle für die Ableitung der Zielwerte für zufällige Hardware-Ausfälle.....	38
Tabelle 12 – Verfahren der Hardware-Integrationsprüfung.....	39
Tabelle 13 – Spezifikation der Software-Sicherheitsanforderungen.....	44
Tabelle 14 – Verfahren für das Software-Architekturdesign.....	45
Tabelle 15 – Verfahren für den Verifizierung des Software-Architekturdesigns.....	47
Tabelle 16 – Entwurfs- und Implementierungsverfahren von Software-Einheiten.....	48
Tabelle 17 – Verfahren für die Verifizierung von Design und Implementierung von Software-Einheiten.....	49
Tabelle 18 – Prüfverfahren für Software-Einheiten.....	51
Tabelle 19 – Prüfverfahren für die Software-Integration.....	53
Tabelle 20 – Verifizierungsverfahren für Software-Sicherheitsanforderungen.....	54
Tabelle 21 – Verfahren für die Datenintegrität.....	55
Tabelle A.1 – Beispiel für die Berechnung der $MTTF_{dc}$ für Leiterplatten.....	60
Tabelle B.1 – Elektrische Teilsysteme (ohne Mikrocontroller).....	61
Tabelle B.2 – Elektronische Teilsysteme (mit Mikrocontroller).....	61
Tabelle B.3 – Verarbeitungseinheiten.....	62
Tabelle B.4 – Unveränderliche Speicherbereiche.....	62
Tabelle B.5 – Veränderliche Speicherbereiche.....	62
Tabelle B.6 – E/A-Einheiten und Schnittstellen (externe Kommunikation).....	63
Tabelle B.7 – Energieversorgung (gilt für Systeme mit und ohne Mikrocontroller).....	63
Tabelle D.1 – Checkliste für technische Unterlagen.....	81

Nationales Vorwort

Das internationale Dokument IEC SyCAAL/209/CDV:2021-01 „Cooperative multiple systems in connected home environments – AAL functional safety requirements of electronic safety-related systems – Part 3: Product development“ (CDV, en: Committee Draft for Vote) ist unverändert in diesen Norm-Entwurf übernommen worden. Dieser Norm-Entwurf enthält eine noch nicht autorisierte deutsche Übersetzung.

Um Zweifelsfälle in der Übersetzung auszuschließen, ist die englische Originalfassung des CDV entsprechend der diesbezüglich durch die IEC erteilten Erlaubnis beigefügt. 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 Abschnitsnummer, 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.

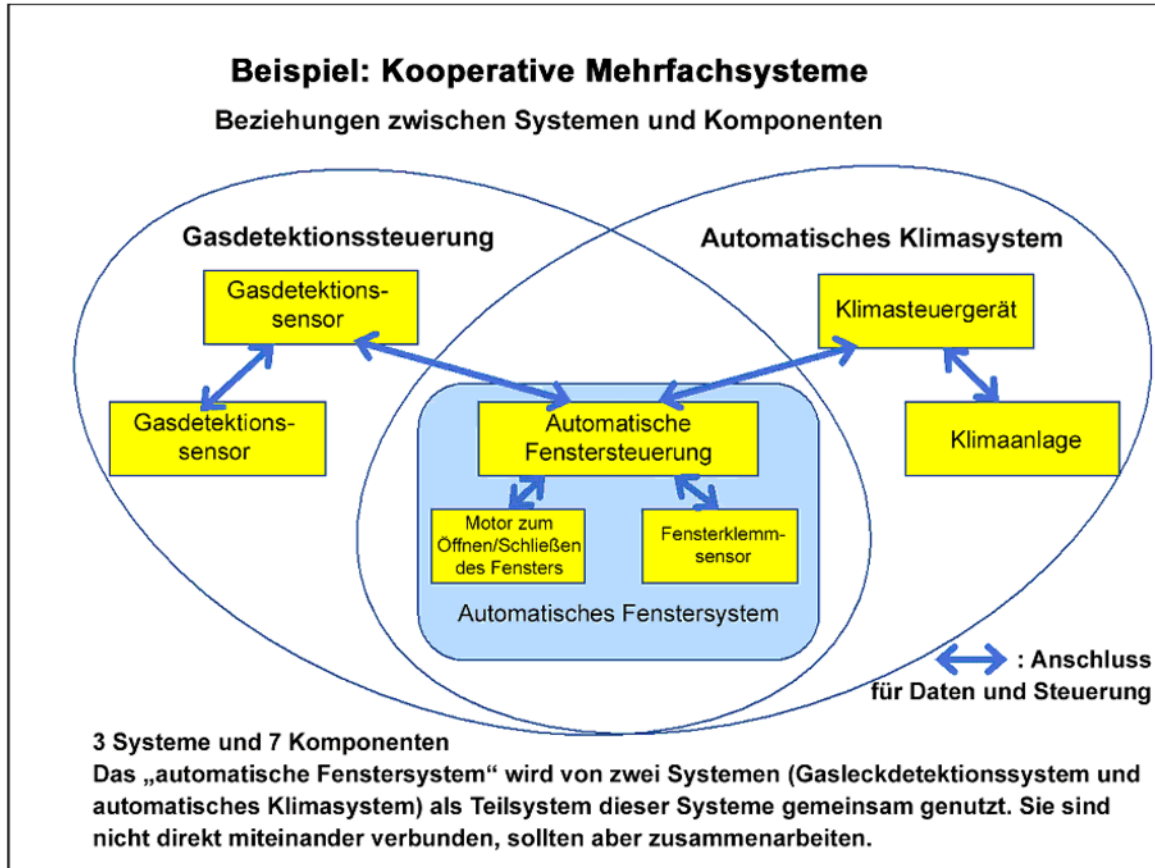


Bild 1 – Kooperative Mehrfachsysteme

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

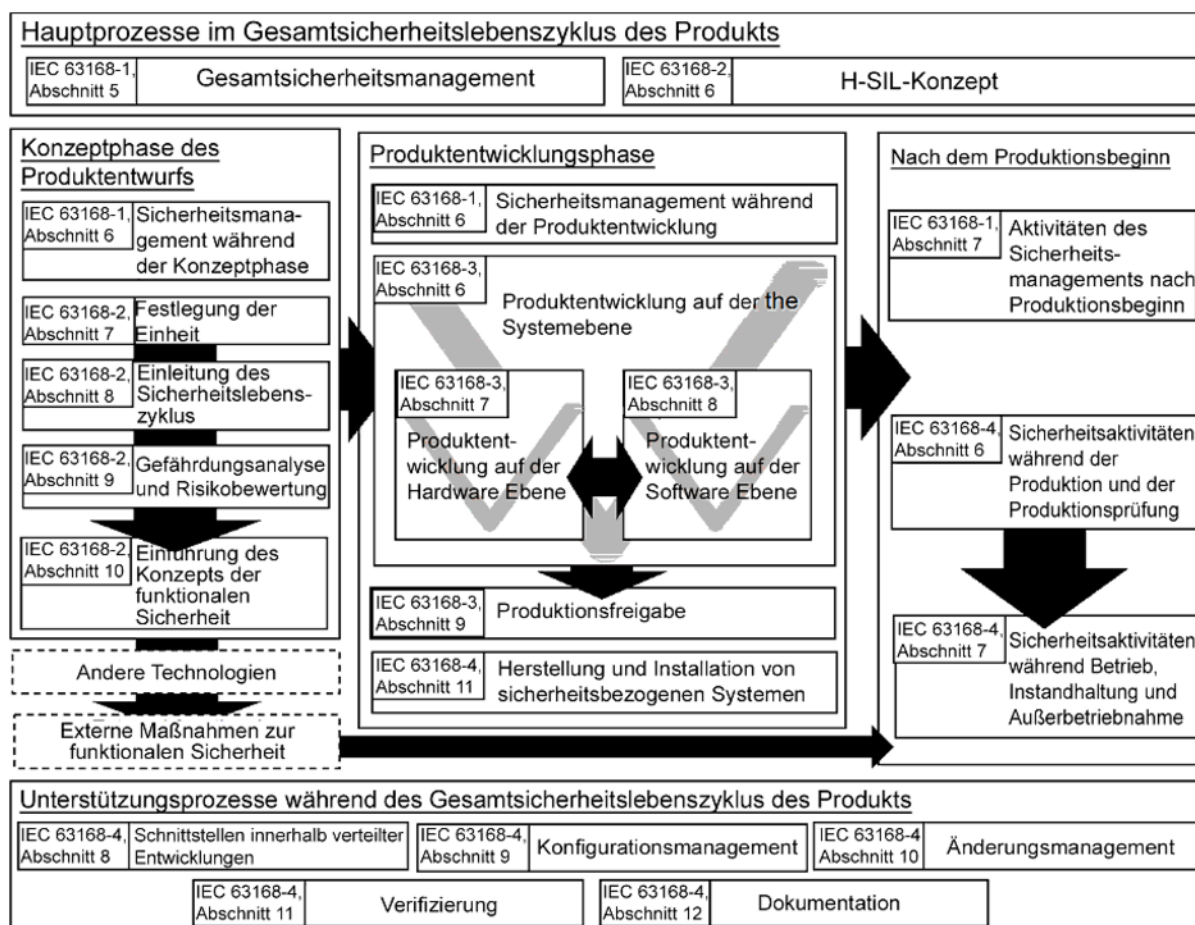
wie in [Tabelle 1](#) angegeben.

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 Phase der Produktentwicklung im Sicherheitslebenszyklus durchgeführt werden, wie in [Bild 2](#) dargestellt. Die betreffenden Leser dieses Dokuments sind Systementwickler von kooperativen Mehrfachsystemen in vernetzten Wohnumfeldern. Die Systementwickler von kooperativen Mehrfachsystemen bauen das System mit Haushaltsgeräten, Ausrüstungen, Heimgeräten usw. auf der Grundlage des Konzeptdesigns auf, um den Dienst für AAL-Nutzer in vernetzten Wohnumfeldern zu realisieren.



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

Bild 2 – Sicherheitslebenszyklus

Dieses Dokument legt die Verfahren fest, nach denen Entwickler von kooperativen Systemen im vernetzten Wohnumfeld vorgehen, um die Sicherheit der AAL-Aspekte des Systemdesigns sowohl für die Hardware als auch die Software sicherzustellen. Diese Aspekte beruhen auf dem Konzept der funktionalen Sicherheit mit dem H-SIL, der in der in IEC 63168-2: 20XX festgelegten Konzeptphase aufgestellt wird.

Kooperative Mehrfachsysteme in vernetzten Wohnumfeldern – AAL Anforderungen an funktionale Sicherheit von elektronischen sicherheitsbezogenen Systemen – Teil 3: Produktentwicklung

1 Anwendungsbereich

Dieses Dokument legt die Verfahren als „Produktentwicklungsphase“ im Sicherheitslebenszyklus fest, nach denen Systementwickler von kooperativen Mehrfachsystemen im vernetzten Wohnumfeld vorgehen, um Sicherheitsmaßnahmen unter Berücksichtigung von AAL-Aspekten zu entwerfen.

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

IEC 63044 (all parts), *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 63168-4:20XX, *Cooperative multiple systems in connected home environments – AAL functional safety requirements of electrical/electronic safety-related systems – Part 4: Production, operation, modification and supporting process*

3 Begriffe

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

Diagnosedeckungsgrad

Prozentsatz der Ausfallrate eines Hardware-Elements oder Prozentsatz der Ausfallrate einer Ausfallart eines Hardware-Elements, der durch den implementierten Sicherheitsmechanismus erkannt oder gesteuert wird

[QUELLE: ISO 26262-1:2018, 3.33, modifiziert – alle Anmerkungen zum Begriff gestrichen]

3.2

Ausfallrate

Quotient aus der Wahrscheinlichkeitsdichte von Ausfällen und der Überlebenswahrscheinlichkeit für ein Hardware-Element

Anmerkung 1 zum Begriff: Die Ausfallrate wird als konstant angenommen und allgemein mit „ λ “ bezeichnet.

[QUELLE: ISO 26262-1:2018, 3.53]

3.3

formale Notation

Beschreibungstechnik, die in ihrer Syntax sowie in ihrer Semantik vollständig definiert ist

BEISPIEL B-Methode, Z-Notation (Zed), NuSMV (symbolische Modellprüfung), Prototyp-Verifizierungssystem (PVS), Wiener Entwicklungsmethode (VDM).

[QUELLE: ISO 26262-1:2018, 3.63, modifiziert – „B-Methode“ wurde hinzugefügt und „mathematische Gleichung“ wurde gestrichen.]

3.4

Hardware-Sicherheitsanforderung

Anforderung, die sich auf sicherheitsbezogene Hardware bezieht und als Element in eine Anforderung an die technische Sicherheit einbezogen wird

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

3.5

nichtformale Notation

Beschreibungstechnik, die in ihrer Syntax nicht vollständig definiert ist

Anmerkung 1 zum Begriff: Eine nicht vollständige Syntaxdefinition bedeutet, dass auch die Semantik nicht vollständig definiert ist.

[QUELLE: ISO 26262-1:2018, 3.80]

3.6

Inspektion

Untersuchung von Arbeitsergebnissen nach einem formalen Verfahren, um Sicherheitsanomalien zu erkennen

Anmerkung 1 zum Begriff: Die Inspektion ist ein Mittel zur Verifizierung.

Anmerkung 2 zum Begriff: Die Inspektion unterscheidet sich von der Prüfung dadurch, dass sie normalerweise nicht den Betrieb der zugehörigen Einheit oder des zugehörigen Elements einschließt

Anmerkung 3 zum Begriff: Ein formales Verfahren umfasst in der Regel eine vorher festgelegte Vorgehensweise, eine Checkliste, einen Moderator und ein Review der Ergebnisse.

[QUELLE: ISO 26262-1:2018, 3.82]

3.7

latenter Fehlzustand

Mehrfach-Fehlzustand, dessen Vorhandensein weder von einem Sicherheitsmechanismus erkannt noch vom

Bediener oder Nutzer innerhalb des Erfassungszeitintervalls wahrgenommen wird

[QUELLE: ISO 26262-1:2018, 3.85, modifiziert – „vom Fahrer innerhalb des Erfassungszeitintervalls“, wurde ersetzt durch „vom Bediener oder Nutzer innerhalb des Erfassungszeitintervalls“.]

3.8

modellgestützte Entwicklung

Entwicklung, die Modelle verwendet, um das Verhalten oder die Eigenschaften eines zu entwickelnden Elements zu beschreiben

Anmerkung 1 zum Begriff: Abhängig von der Abstraktionsebene, die für ein solches Modell verwendet wird, kann das Modell für die Simulation oder die Codegenerierung oder beides verwendet werden.

[QUELLE: ISO 26262-1:2018, 3.90]

3.9

zufälliger Hardware-Ausfall

Ausfall, der während der Lebensdauer eines Hardware-Elements unvorhersehbar auftreten kann und einer Wahrscheinlichkeitsverteilung entspricht

Anmerkung 1 zum Begriff: Raten zufälliger Hardware-Ausfälle können mit angemessener Genauigkeit vorhergesagt werden.

[QUELLE: ISO 26262-1:2018, 3.118, modifiziert – Anmerkung 2 zum Begriff gestrichen]

3.10

Sicherheitsmechanismus

technische Lösung, die durch E/E-Funktionen oder -Elemente oder durch andere Technologien implementiert wird, um Fehlzustände zu erkennen und zu mildern oder zu tolerieren oder Ausfälle zu beherrschen oder zu vermeiden, um die vorgesehene Funktionalität zu erhalten oder einen sicheren Zustand zu erreichen oder aufrechtzuerhalten

Anmerkung 1 zum Begriff: Sicherheitsmechanismen werden innerhalb der Einheit implementiert, um zu verhindern, dass Fehlzustände zu Einfach-Ausfällen führen oder um nicht systematische Ausfälle zu verringern und um zu verhindern, dass Fehlzustände latent vorhanden sind.

Anmerkung 2 zum Begriff: Der Sicherheitsmechanismus ist in der Lage, entweder

- a) die Einheit in einen sicheren Zustand zu überführen oder in diesem zu halten, oder
- b) den Bediener oder Nutzer so zu alarmieren, dass dieser die Auswirkungen des Fehlzustands kontrollieren kann, wie im Konzept der funktionalen Sicherheit festgelegt.

[QUELLE: ISO 26262-1:2018, 3.142, modifiziert – „den Fahrer so zu alarmieren, dass dieser“ in Anmerkung 2 zum Begriff, Punkt b), wurde ersetzt durch „den Bediener oder Nutzer so zu alarmieren, dass dieser“.]

3.11

Software-Sicherheitsanforderung

Anforderung, die sich auf sicherheitsbezogene Software bezieht und als Element in eine Anforderung an die technische Sicherheit einbezogen wird

[QUELLE: ISO 25119-1:2018, 3.49]

3.12

systematischer Ausfall

Ausfall, bei dem deterministisch auf eine Ursache geschlossen werden kann, die nur durch eine Änderung des Entwurfs oder des Fertigungsprozesses, der Art und Weise des Betriebes, der Bedienungsanleitung oder anderer Einflussfaktoren beseitigt werden kann

[QUELLE: ISO 26262-1:2018, 3.164]

3.13

systematischer Fehlzustand

Fehlzustand, dessen Ausfall sich in einer deterministischen Weise offenbart, die nur durch Anwendung von Prozess- oder Entwurfsmaßnahmen beseitigt werden kann

[QUELLE: ISO 26262-1:2018, 3.165]

3.14

technische Sicherheitsanforderung

Anforderung, die für die Implementierung von zugehörigen Anforderungen an die funktionale Sicherheit abgeleitet wird

Anmerkung 1 zum Begriff: Die abgeleitete Anforderung umfasst Anforderungen für die Milderung.

[QUELLE: ISO 26262-1:2018, 3.168]

3.15

Walk-through

systematische Untersuchung von Arbeitsergebnissen, um Sicherheitsanomalien zu erkennen

Anmerkung 1 zum Begriff: Der Walk-through ist ein Mittel zur Verifizierung.

Anmerkung 2 zum Begriff: Der Walk-through unterscheidet sich von der Prüfung dadurch, dass er normalerweise nicht den Betrieb der zugehörigen Einheit oder des zugehörigen Elements einschließt.

Anmerkung 3 zum Begriff: Während eines Walk-through erklärt der Entwickler einem oder mehreren Prüfer(n) das Arbeitsergebnis Schritt für Schritt. Ziel ist es, ein gemeinsames Verständnis für das Arbeitsergebnis zu schaffen und etwaige Sicherheitsanomalien innerhalb des Arbeitsergebnisses festzustellen. Sowohl Inspektionen als auch Walk-throughs sind Arten des Peer-Reviews, wobei ein Walk-through eine weniger strenge Form des Peer-Reviews ist als eine Inspektion.

[QUELLE: ISO 26262-1:2018, 3.182, modifiziert – Anmerkung 3 zum Begriff wurde gestrichen und das BEISPIEL ist jetzt Anmerkung 3 zum Begriff]

4 Abkürzungen

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

ECU	elektronische Steuerungseinheit (en: electronic control unit)
EMV	elektromagnetische Verträglichkeit
EMI	elektromagnetische Beeinflussung (en: electromagnetic interference)
ESD	Entladung statischer Elektrizität (en: electro-static discharge)
PMHF	Wahrscheinlichkeitsmetrik für zufällige Hardware-Ausfälle (en: probabilistic metric for random hardware failures)

5 Überblick und Anmerkungen

5.1 Überblick über Sicherheitsaktivitäten während der Produktentwicklungsphase des Produktentwurfs

Die in der Produktentwicklungsphase des Produktentwurfs durchgeführten Sicherheitsaktivitäten werden in die folgenden vier Prozesse unterteilt:

- Produktentwicklung auf der Systemebene ([Abschnitt 6](#)): einschließlich von fünf Unterphasen in [6.1 bis 6.5](#);
- Produktentwicklung auf der Hardware-Ebene ([Abschnitt 7](#)): einschließlich von fünf Unterphasen in [7.1 bis 7.5](#);
- Produktentwicklung auf der Software-Ebene ([Abschnitt 8](#)): einschließlich von acht Unterphasen in [8.1 bis 8.8](#); und
- Produktionsfreigabe ([Abschnitt 9](#)).

Als Ergebnis der Sicherheitsaktivitäten in der Konzeptentwurfsphase werden jedem E/E-Teilsystem Sicherheitsanforderungen zugeordnet, die mit einem H-SIL auf der Grundlage des Sicherheitsziels verbunden sind (IEC 63168-2:20XX). Die Entwicklung jedes Teilsystems erfordert Sicherheitsaktivitäten auf der Grundlage des zugeordneten H-SIL. Bezüglich der erforderlichen Sicherheitsaktivitäten für jede Entwicklung auf der Systemebene, der Hardware-Ebene und der Software-Ebene gibt es Anforderungen in einer auf die Teilprozesse wie Planung, Entwicklung und Prüfung zugeschnittenen Form. Die erforderlichen Sicherheitsaktivitäten beim Übergang vom Abschluss der Entwicklung zur Produktions-/ Implementierungsphase werden in der Produktionsfreigabe dargestellt.

5.2 Notationen und Interpretationen von [Tabelle 2](#) bis [Tabelle 21](#)

In diesem Dokument gibt es 20 Tabellen, die die Beziehung zwischen dem Inhalt der Sicherheitsaktivitäten und dem Grad des H-SIL angeben. Jede Tabelle ist abhängig vom jeweiligen Kontext normativ oder informativ. Die verschiedenen in einer Tabelle aufgeführten Verfahren tragen zum Grad des Vertrauens in die Einhaltung der entsprechenden Anforderung und des H-SIL bei. Jedes Verfahren in einer Tabelle ist entweder:

- a) ein fortlaufender Eintrag (gekennzeichnet durch eine laufende Nummer in der Spalte ganz links, z. B. 1, 2, 3), oder
- b) ein alternativer Eintrag (gekennzeichnet durch eine Zahl gefolgt von einem Buchstaben in der Spalte ganz links, z. B. 2a, 2b, 2c).

Bei aufeinanderfolgenden Einträgen müssen alle Verfahren, wie in Übereinstimmung mit dem H-SIL empfohlen, angewendet werden. Wenn andere als die aufgeführten Verfahren angewendet werden, muss begründet werden, dass diese die entsprechende Anforderung erfüllen.

Bei alternativen Einträgen muss eine geeignete Kombination von Verfahren in Übereinstimmung mit dem angegebenen H-SIL angewendet werden, unabhängig davon, ob sie in der Tabelle aufgeführt ist oder nicht. Wenn Verfahren mit unterschiedlichen Empfehlungsgraden für ein H-SIL aufgeführt sind, muss das Verfahren mit der höchsten Empfehlung bevorzugt werden. Es muss begründet werden, dass die gewählte Kombination von Verfahren die entsprechende Anforderung erfüllt.

ANMERKUNG 1 Eine Begründung auf der Grundlage der in jeder Tabelle aufgeführten Verfahren ist ausreichend. Dies bedeutet jedoch keine Bevorzugung oder Ablehnung von Verfahren, die nicht in dieser Tabelle aufgeführt sind.

Für jedes Verfahren hängt der Grad der Empfehlung für die Verwendung des entsprechenden Verfahrens vom H-SIL ab und ist wie folgt kategorisiert:

- „++“ zeigt an, dass das Verfahren für den bezeichneten H-SIL sehr empfohlen wird;

ANMERKUNG 2 Wenn es eine besser geeignete Technik oder Maßnahme als diese gibt, darf diese mit entsprechender Begründung angewendet werden.

- „+“ zeigt an, dass das Verfahren für den bezeichneten H-SIL empfohlen wird;
- „o“ zeigt an, dass es für das Verfahren keine Empfehlung für oder gegen seine Verwendung für den bezeichneten H-SIL gibt.

5.3 Vom H-SIL abhängige Anforderungen und Empfehlungen

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

Wenn in diesem Dokument ein H-SIL in Klammern angegeben ist, muss die entsprechende Unterphase als Empfehlung und nicht als Anforderung für diesen H-SIL betrachtet werden.

6 Produktentwicklung auf der Systemebene

6.1 Planung der Systementwicklung

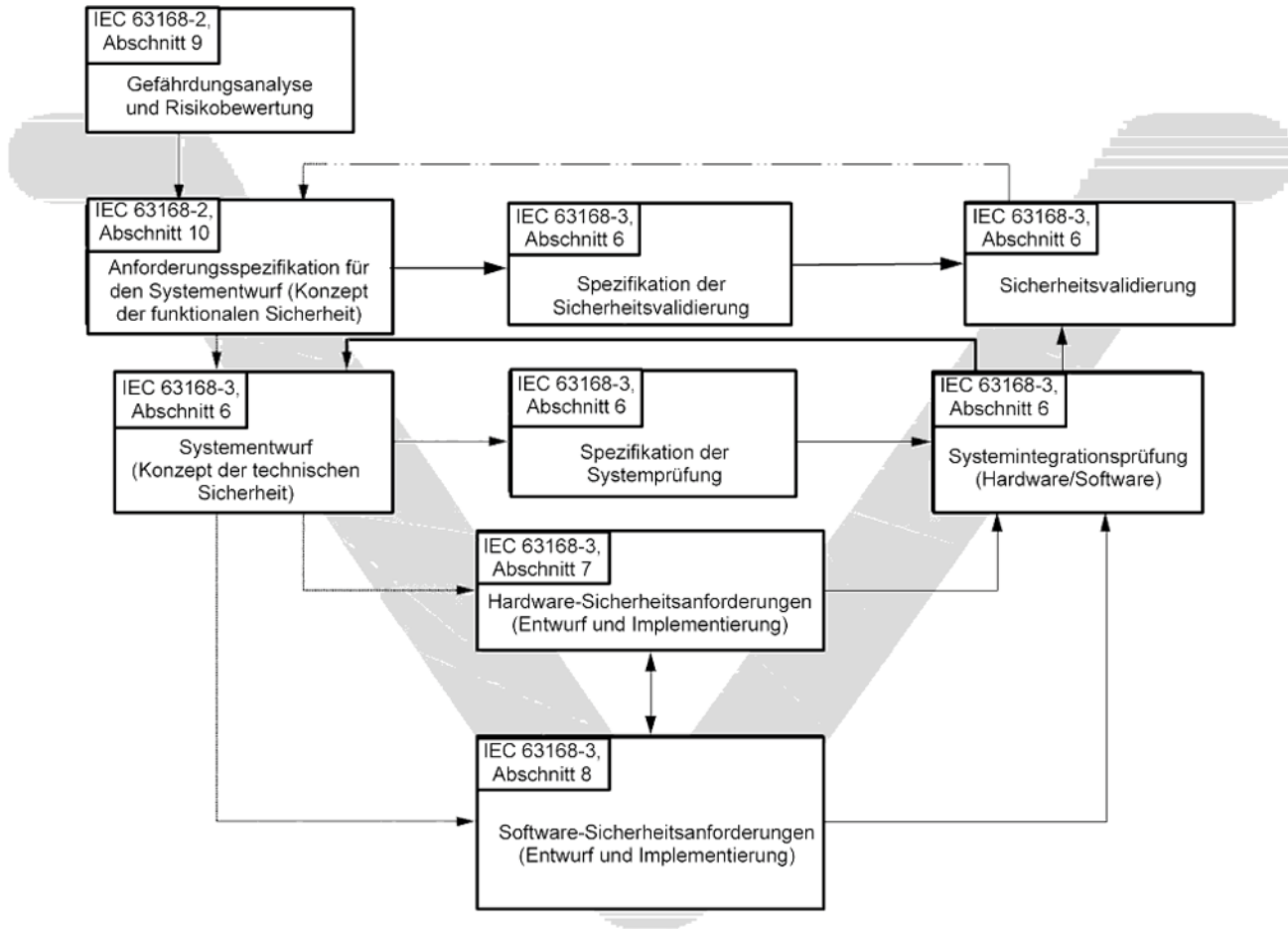
6.1.1 Zweck

Ziel der Planung der Systementwicklung ist die Festlegung und Planung der Aktivitäten zur funktionalen Sicherheit während der einzelnen Unterphasen der Systementwicklung. Dazu gehören auch die notwendigen Unterstützungsprozesse, die in IEC 63168-4 beschrieben sind.

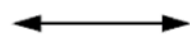
Diese Planung der Sicherheitsaktivitäten auf der Systemebene wird in den Sicherheitsplan aufgenommen.

6.1.2 Allgemeines

Die notwendigen Aktivitäten während der Entwicklung eines Systems sind in [Bild 2](#) dargestellt. Nach der Einleitung der Produktentwicklung und der Spezifikation der Anforderungen an die technische Sicherheit wird der Systementwurf durchgeführt. Während des Systemdesigns wird die Systemarchitektur festgelegt und die Anforderungen an die technische Sicherheit werden der Hardware und der Software zugeordnet. Darüber hinaus werden die Anforderungen an die technische Sicherheit präzisiert und Anforderungen, die sich aus der Systemarchitektur ergeben, werden hinzugefügt. Abhängig von der Komplexität der Architektur können die Anforderungen an Teilsysteme iterativ abgeleitet werden. Nach ihrer Entwicklung werden die Hardware- und Software-Elemente integriert und geprüft, um eine Einheit zu bilden, die dann in ein vernetztes Wohnumfeld integriert wird. Nach der Integration auf der Ebene des vernetzten Wohnumfelds wird eine Sicherheitsvalidierung durchgeführt, um den Nachweis der funktionalen Sicherheit im Hinblick auf die Sicherheitsziele zu erbringen.



Legende



Querverweisung



Ergebnis



Verifizierung



Validierung

Bild 3 – Referenzphasenmodell für die Entwicklung einer sicherheitsbezogenen Einheit

6.1.3 Für die Planung der Systementwicklung erforderliche Informationen

Die folgenden Informationen müssen zur Verfügung gestellt werden:

- Projektplan (präzisiert) in Übereinstimmung mit IEC 63168-1:20XX, 5.3;
- Sicherheitsplan in Übereinstimmung mit IEC 63168-2:20XX, 8.3; und
- Konzept der funktionalen Sicherheit in Übereinstimmung mit IEC 63168-2:20XX, 10.5.

Die folgenden Informationen können berücksichtigt werden:

- vorläufige Architekturannahmen (von einer externen Quelle); und
- Festlegung der Elemente (siehe IEC 63168-2:20XX, 7.3).

6.1.4 Anforderungen an die Planung der Systementwicklung

6.1.4.1 Planung der Sicherheitsaktivitäten auf der Systemebene

Die Sicherheitsaktivitäten für die Produktentwicklung auf der Systemebene müssen, einschließlich der Festlegung der geeigneten Verfahren und Maßnahmen während des Entwurfs und der Integration, geplant werden.

6.1.4.2 Planung der Validierung

Die Validierungsaktivitäten müssen geplant werden.

6.1.4.3 Planung der Bewertung der funktionalen Sicherheit

Die Aktivitäten der Bewertung der funktionalen Sicherheit für die Produktentwicklung auf der Systemebene müssen geplant werden (siehe auch IEC 63168-1).

6.1.4.4 Anpassung des Sicherheitslebenszyklus auf der Systemebene

Die Anpassung des Lebenszyklus für die Produktentwicklung auf der Systemebene muss nach IEC 63168-1 und basierend auf dem in [Bild 3](#) angegebenen Referenzphasenmodell durchgeführt werden.

6.1.5 Arbeitsergebnisse der Planung der Systementwicklung

- a) Projektplan (präzisiert) nach [6.1.4](#).
- b) Sicherheitsplan (präzisiert) nach [6.1.4](#).

6.2 Festlegung der Anforderungsspezifikation für die technische Sicherheit

6.2.1 Zweck dieser Unterphase

Das erste Ziel dieser Unterphase ist die Spezifikation der Anforderungen an die technische Sicherheit. Die Spezifikation der Anforderungen an die technische Sicherheit präzisiert das Konzept der funktionalen Sicherheit, wobei sowohl das funktionale Konzept als auch die vorläufigen Architekturannahmen berücksichtigt werden (siehe IEC 63168-2).

Das zweite Ziel ist es, durch Analyse zu verifizieren, dass die Anforderungen an die technische Sicherheit mit den Anforderungen an die funktionale Sicherheit übereinstimmen.

6.2.2 Allgemeines

Innerhalb des gesamten Entwicklungslebenszyklus sind die Anforderungen an die technische Sicherheit die technischen Anforderungen, die zur Umsetzung des Konzepts der funktionalen Sicherheit erforderlich sind, wobei die Absicht darin besteht, die Anforderungen an die funktionale Sicherheit auf Elementebene in den Anforderungen an die technische Sicherheit auf Systemebene ausführlich zu beschreiben.

6.2.3 Informationen für die Festlegung der Anforderungsspezifikation für die technische Sicherheit

Die folgenden Informationen müssen zur Verfügung gestellt werden:

- Konzept der funktionalen Sicherheit in Übereinstimmung mit IEC 63168-2:20XX, 10.5; und
- Sicherheitsplan in Übereinstimmung mit [6.1.5](#).

Die folgenden Informationen können berücksichtigt werden:

- Sicherheitsziele (siehe IEC 63168-2:20XX, 9.3);
- Konzept der funktionalen Sicherheit (von einer externen Quelle, siehe IEC 63168-2:20XX, 7.2.3); und
- vorläufige Architekturannahmen (von einer externen Quelle, siehe IEC 63168-2:20XX, 10.3).

6.2.4 Anforderungen und Empfehlungen

6.2.4.1 Anforderungsspezifikation für die technische Sicherheit

Die Anforderungen an die technische Sicherheit müssen das Verhalten des Systems oder der Elemente bei Stimuli, die das Erreichen der Sicherheitsziele beeinflussen, festlegen. Dazu gehören Ausfälle und entsprechende Kombinationen von Stimuli zusammen mit jeder einschlägigen Betriebsart und jedem definierten Systemzustand.

Die Anforderungen an die technische Sicherheit müssen in Übereinstimmung mit dem Konzept der funktionalen Sicherheit, den vorläufigen Architekturannahmen für die Einheit und den folgenden Systemeigenschaften festgelegt werden:

- a) externe Schnittstellen, wie z. B. Kommunikations- und Benutzerschnittstellen, falls zutreffend;
- b) Randbedingungen, z. B. Umgebungsbedingungen oder funktionale Einschränkungen; und
- c) Anforderungen an die Systemkonfiguration.

6.2.4.2 Sicherheitsmechanismen

Die Anforderungen an die technische Sicherheit müssen die notwendigen Sicherheitsmechanismen festlegen, einschließlich von:

- a) Maßnahmen zur Erkennung, Anzeige und Beherrschung von Fehlzuständen im System selbst;

ANMERKUNG 1 Dazu gehört die Selbstüberwachung des Systems oder der Elemente zur Erkennung von zufälligen Hardware-Fehlern und gegebenenfalls zur Erkennung von systematischen Ausfällen.

ANMERKUNG 2 Dazu gehören Maßnahmen zur Erkennung und Beherrschung von Ausfallarten der Kommunikationskanäle (z. B. Datenschnittstellen, Kommunikationsbusse, Funkverbindung).

- b) Maßnahmen zur Erkennung, Anzeige und Beherrschung von Fehlzuständen in externen Geräten, die mit dem System in Wechselwirkung stehen;

BEISPIEL Zu den externen Geräten gehören andere elektronische Steuerungseinheiten, Stromversorgungs- oder Kommunikationsgeräte.

- c) Maßnahmen, die es dem System ermöglichen, einen sicheren Zustand zu erreichen oder aufrechtzuerhalten;

ANMERKUNG 3 Dazu gehören Priorisierungs- und Arbitrierungslogik im Fall von kollidierenden Sicherheitsmechanismen.

Für jeden Sicherheitsmechanismus, der es einer Einheit ermöglicht, einen sicheren Zustand zu erreichen oder aufrechtzuerhalten, muss Folgendes festgelegt werden:

- der Übergang in den sicheren Zustand;

ANMERKUNG 4 Dazu gehören die Anforderungen an die Steuerung der Stellglieder.

- die Fehlertoleranzzeit;
- Maßnahmen zur Aufrechterhaltung des sicheren Zustands.

6.2.4.3 Vermeidung von latenten Fehlzuständen

Diese Anforderungen gelten für die H-SILs (A), (B), C und D nach 5.3: gegebenenfalls müssen Sicherheitsmechanismen festgelegt werden, um zu verhindern, dass Fehlzustände latent werden.

BEISPIEL On-Board-Prüfungen sind Sicherheitsmechanismen, die den Zustand von Komponenten während der verschiedenen Betriebsarten wie Hochfahren, Herunterfahren, während der Laufzeit oder in einer zusätzlichen Prüfbetriebsart überprüfen, um latente Fehlzustände zu erkennen.

6.2.4.4 Produktion, Betrieb, Instandhaltung und Außerbetriebnahme

Die Anforderungen an die technische Sicherheit in Bezug auf die funktionale Sicherheit der Einheit oder ihrer Elemente während Produktion, Betrieb, Instandhaltung, Reparatur und Außerbetriebnahme, die in IEC 63168-4 behandelt werden, müssen festgelegt werden.

ANMERKUNG Es gibt zwei Aspekte, die die Sicherheit während Produktion, Betrieb, Instandhaltung, Reparatur und Außerbetriebnahme sicherstellen. Der erste Aspekt bezieht sich auf die Aktivitäten während der Entwicklungsphase, die in den Anforderungen 6.2.4.4 und 6.3.4.7 (Anforderungen für Produktion, Betrieb, Instandhaltung und Außerbetriebnahme) aufgeführt sind, während der zweite Aspekt sich auf die Aktivitäten während der Produktions- und Betriebsphase bezieht, die in IEC 63168-4 behandelt werden.

6.2.4.5 Verifizierung und Validierung

Die Anforderungen an die technische Sicherheit müssen in Übereinstimmung mit IEC 63168-4:20XX, Abschnitt 11, verifiziert werden, um Folgendes nachzuweisen:

- a) Übereinstimmung und Vereinbarkeit mit dem Konzept der funktionalen Sicherheit; und
- b) Übereinstimmung mit den vorläufigen Architekturannahmen.

Die Kriterien für die Sicherheitsvalidierung der Einheit müssen auf der Grundlage der Anforderungen an die technische Sicherheit neu definiert werden.

ANMERKUNG Die Planung und die Spezifikationen der Systemvalidierung werden gleichzeitig mit den Anforderungen an die technische Sicherheit entwickelt (siehe 6.5).

6.2.5 Arbeitsergebnisse

- a) Anforderungsspezifikation für die technische Sicherheit nach 6.2.4.1 bis 6.2.4.4.
- b) System-Verifizierungsbericht nach 6.2.4.5.
- c) Sicherheitsplan (präzisiert) nach 6.2.4.5.

6.3 Sicherheitsaktivitäten während des Systemdesigns

6.3.1 Zweck der Sicherheitsaktivitäten während des Systemdesigns

Das erste Ziel dieser Unterphase ist die Entwicklung des Systemdesigns und des Konzepts der technischen Sicherheit, die den funktionalen Anforderungen und der Anforderungsspezifikation für die technische Sicherheit der Einheit entsprechen.

Das zweite Ziel dieser Unterphase ist die Verifizierung, dass das Systemdesign und das Konzept der technischen Sicherheit mit der Anforderungsspezifikation für die technische Sicherheit übereinstimmen.

6.3.2 Allgemeines

Die Entwicklung des Systemdesigns und des Konzepts der technischen Sicherheit basiert auf der Anforderungsspezifikation für die technische Sicherheit, die aus dem Konzept der funktionalen Sicherheit abgeleitet wird. Wenn das System aus Teilsystemen besteht, kann diese Unterphase iterativ durchgeführt werden.

Um ein Systemarchitekturdesign zu entwickeln, werden Anforderungen an die funktionale Sicherheit, an die technische Sicherheit und nicht sicherheitsbezogene Anforderungen implementiert. Somit werden in dieser Unterphase sicherheitsbezogene und nicht sicherheitsbezogene Anforderungen innerhalb eines Entwicklungsprozesses behandelt.

6.3.3 Für Sicherheitsaktivitäten während des Systementwurfs erforderliche Informationen

Die folgenden Informationen müssen zur Verfügung gestellt werden:

- Sicherheitsplan in Übereinstimmung mit 6.1.5; und
- Anforderungsspezifikation für die technische Sicherheit in Übereinstimmung mit 6.2.5.

Die folgenden Informationen können berücksichtigt werden:

- vorläufige Architekturannahmen (von einer externen Quelle, siehe IEC 63168-2:20XX, 10.3);
- Funktionskonzept (von einer externen Quelle); und
- Konzept der funktionalen Sicherheit (siehe IEC 63168-2:20XX, 10.5).

6.3.4 Anforderungen und Empfehlungen

6.3.4.1 Spezifikation des Systemdesigns und Konzept der technischen Sicherheit

Das Systemdesign muss auf dem Funktionskonzept, den vorläufigen Architekturannahmen und den Anforderungen an die technische Sicherheit beruhen.

Die Anforderungen an die technische Sicherheit müssen den Elementen des Systemdesigns zugeordnet werden.

Das Systemdesign muss die Anforderungen an die technische Sicherheit umsetzen.

Im Hinblick auf die Umsetzung der Anforderungen an die technische Sicherheit muss beim Systemdesign folgendes berücksichtigt werden:

- a) die Fähigkeit, das Systemdesign zu verifizieren;
- b) die technischen Fähigkeiten des vorgesehenen Hardware- und Software-Designs in Bezug auf die Erfüllung der funktionalen Sicherheit; und
- c) die Fähigkeit zur Durchführung von Prüfungen während der Systemintegration.

6.3.4.2 Randbedingungen des Systemarchitekturdesigns

Jedes Element der Systemarchitektur muss den höchsten H-SIL aus den Anforderungen an die technische Sicherheit erben, die es implementiert.

Besteht ein Element aus Unterelementen, denen unterschiedliche H-SILs zugeordnet sind, oder aus nicht sicherheitsbezogenen Unterelementen und sicherheitsbezogenen Unterelementen, muss jedes dieser Elemente entsprechend dem höchsten H-SIL behandelt werden, es sei denn, das Nebeneinanderbestehen wird begründet.

6.3.4.3 Maßnahmen zur Vermeidung systematischer Ausfälle

Sicherheitsanalysen des Systemdesigns zur Ermittlung der Ursachen systematischer Ausfälle und der Auswirkungen systematischer Fehlzustände müssen nach [Tabelle 2](#) durchgeführt werden.

Tabelle 2 – Analyse des Systementwurfs

Verfahren		H-SIL			
		A	B	C	D
1	Deduktive Analyse ^a	0	+	++	++
2	Induktive Analyse ^b	++	++	++	++
^a Zu deduktiven Analyseverfahren gehören FTA, Zuverlässigkeitsblockdiagramme, Ishikawa-Diagramm. ^b Zu induktiven Analyseverfahren gehören FMEA, ETA, Markov-Modellierung.					

ANMERKUNG 1 Der Zweck dieser Analysen ist die Unterstützung beim Entwurf. Daher ist in dieser Phase eine qualitative Analyse wahrscheinlich ausreichend. Gegebenenfalls kann eine quantitative Analyse durchgeführt werden.

ANMERKUNG 2 Die Analyse wird mit dem Detaillierungsgrad durchgeführt, der erforderlich ist, um Ursachen und Auswirkungen von systematischen Ausfällen festzustellen oder auszuschließen.

Festgestellte interne Ursachen für systematische Ausfälle müssen beseitigt oder ihre Auswirkungen gemildert werden.

Diese Anforderung gilt für die H-SILs (A), (B), C und D nach 5.3, um Ausfälle zu vermeiden, die sich aufgrund einer hohen Komplexität ergeben. Das Architekturdesign muss unter Anwendung der Grundsätze in Tabelle 3 alle der folgenden Merkmale aufweisen:

- a) Modularität;
- b) eine angemessene Granularität; und
- c) Einfachheit.

Tabelle 3 – Merkmale des modularen Systementwurfs

Merkmale		H-SIL			
		A	B	C	D
1	Hierarchischer Entwurf	+	+	++	++
2	Genau definierte Schnittstellen	+	+	+	+
3	Vermeidung unnötiger Komplexität von Hardware- und Software-Komponenten	+	+	+	+
4	Vermeidung unnötiger Komplexität von Schnittstellen	+	+	+	+
5	Instandhaltbarkeit während des Dienstes	+	+	+	+
6	Überprüfbarkeit während der Entwicklung und des Betriebs	+	+	++	++

6.3.4.4 Maßnahmen für die Beherrschung zufälliger Hardware-Ausfälle während des Betriebs

Maßnahmen zur Erkennung und Beherrschung oder Milderung zufälliger Hardware-Ausfälle müssen in Bezug auf das in 6.3.4.1 angegebenen Systemdesign festgelegt werden.

BEISPIEL Solche Maßnahmen können Hardware-Diagnosefunktionen und deren Nutzung durch die Software sein, um zufällige Hardware-Ausfälle zu erkennen.

Diese Anforderung gilt für die H-SILs (B), C und D nach 5.3: Der Zielwert für die Durchführung der Bewertung der Verletzung des Sicherheitsziels aufgrund zufälliger Hardware-Ausfälle (siehe 7.4) muss für die abschließende Bewertung auf der Einheitenebene festgelegt werden (siehe 6.5.4.3).

6.3.4.5 Zuordnung zu Hardware und Software

Die Anforderungen an die technische Sicherheit müssen der Hardware, der Software oder beidem direkt oder durch weitere Präzisierung zugeordnet werden.

6.3.4.6 Hardware-Software-Schnittstellenspezifikation (HSI)

Die HSI-Spezifikation muss das Zusammenwirken von Hardware und Software festlegen und mit dem Konzept der technischen Sicherheit vereinbar sein. Die HSI-Spezifikation muss die Hardware-Einrichtungen der Komponente, die von der Software gesteuert werden, und die Hardware-Ressourcen, die die Ausführung der Software unterstützen, umfassen.

Die HSI-Spezifikation muss folgende Eigenschaften umfassen:

- a) die zutreffenden Betriebsarten der Hardware-Einrichtungen und die zutreffenden Konfigurationsparameter;

BEISPIEL 1 Betriebsarten von Hardware-Einrichtungen wie Voreinstellung, Initialisierung, Prüfung oder erweiterte Betriebsarten.

BEISPIEL 2 Konfigurationsparameter wie Verstärkungsregelung, Bandpassfrequenz oder Takt-Vorteiler.

- b) gemeinsame und ausschließliche Nutzung von Hardware-Ressourcen;

BEISPIEL 3 Speicherabbildung, Zuweisung von Registern, Zeitgeber, Interrupts, E/A-Ports.

- c) den Zugriffsmechanismus auf Hardware-Einrichtungen; und

BEISPIEL 4 Seriell, parallel, Slave, Master/Slave.

- d) die Zeitbeschränkungen, die für jeden in das Konzept der technischen Sicherheit einbezogenen Dienst festgelegt sind.

Die zutreffenden Diagnosefähigkeiten der Hardware und deren Nutzung durch die Software müssen in der HSI-Spezifikation festgelegt werden.

BEISPIEL Erkennung von Überstrom, Kurzschluss oder Übertemperatur.

6.3.4.7 Anforderungen an Produktion, Betrieb, Instandhaltung und Außerbetriebnahme

Die Diagnosefunktionen müssen so festgelegt werden, dass sie die erforderlichen Daten bereitstellen, die eine Feldüberwachung und Erkennung von Fehlzuständen für die Einheit oder deren Elemente während des Betriebs ermöglichen, wobei die Ergebnisse von Sicherheitsanalysen und die implementierten Sicherheitsmechanismen zu berücksichtigen sind.

Die beim Systemdesign ermittelten Anforderungen an Produktion, Betrieb, Instandhaltung und Außerbetriebnahme müssen festgelegt werden. Dazu gehören:

- a) die Anforderungen an die Montageanweisungen;
- b) die sicherheitsbezogenen Sondereigenschaften;
- c) die Anforderungen, um eine einwandfreie Identifikation von Systemen oder Elementen sicherzustellen;

BEISPIEL 1 Kennzeichnung von Elementen.

- d) die Verifizierungsverfahren und -maßnahmen für die Produktion;
- e) die Instandhaltungsmaßnahmen, einschließlich Diagnosedaten und Instandhaltungshinweise; und
- f) die Anforderungen an die Außerbetriebnahme.

BEISPIEL 2 Anweisungen für die Außerbetriebnahme.

6.3.4.8 Verifizierung des Systemdesigns

Das Systemdesign muss mit den in [Tabelle 4](#) aufgeführten Verifizierungsverfahren auf Übereinstimmung und Vollständigkeit in Bezug auf das Konzept der technischen Sicherheit überprüft werden.

Tabelle 4 – Verifizierung des Systementwurfs

Verfahren		H-SIL			
		A	B	C	D
1a	Inspektion des Systemdesigns ^a	+	++	++	++
1b	Walk-through des Systemdesigns ^a	++	+	o	o
2a	Simulation ^b	+	+	++	++
2b	Prototypenentwicklung des Systems und Prüfungen im vernetzten Wohnumfeld ^b	+	+	++	++
3	Analysen des Systemdesigns	siehe Tabelle 2			
^a Die Verfahren 1a und 1b dienen der Überprüfung der vollständigen und einwandfreien Umsetzung der Anforderungen an die technische Sicherheit.					
^b Die Verfahren 2a und 2b können vorteilhaft als Fehlerinjektionstechnik eingesetzt werden.					

6.3.5 Arbeitsergebnisse

- a) Konzept der technischen Sicherheit nach [6.3.4.1](#) und [6.3.4.5](#).
- b) Spezifikation des Systemdesigns nach [6.3.4.1](#) bis [6.3.4.5](#).
- c) Hardware-Software-Schnittstellenspezifikation (HSI) nach [6.3.4.6](#).
- d) Spezifikation der Anforderungen an Produktion, Betrieb, Instandhaltung und Außerbetriebnahme nach [6.3.4.7](#).
- e) System-Verifizierungsbericht (präzisiert) nach [6.3.4.8](#).
- f) Bericht der Sicherheitsanalyse nach [6.3.4.3](#).

6.4 Integration und Prüfung von Einheiten

6.4.1 Zweck der Integration und Prüfung von Einheiten

Die Integrations- und Prüfphase umfasst drei Phasen und zwei primäre Ziele, die im Folgenden beschrieben werden: Die erste Phase ist die Integration der Hardware und der Software jedes Elements, aus denen die Einheit besteht. Die zweite Phase ist die Integration der Elemente, aus denen eine Einheit besteht, um ein vollständiges System zu bilden. Die dritte Phase ist die Integration der Einheit in andere Systeme innerhalb eines Wohnumfelds.

Das erste Ziel des Integrationsprozesses ist die Prüfung der Einhaltung aller Sicherheitsanforderungen in Übereinstimmung mit ihrer Spezifikation und H-SIL-Klassifizierung.

Das zweite Ziel besteht in der Verifizierung, ob das „Systemdesign“, der die Sicherheitsanforderungen (siehe [6.3](#)) erfüllt, von der gesamten Einheit ordnungsgemäß umgesetzt wird.

6.4.2 Allgemeines

Die Integration der Elemente der Einheit erfolgt auf systematische Weise, beginnend mit der Software-Hardware-Integration über die Systemintegration bis hin zur Integration in das Wohnumfeld. In jeder Integrationsphase werden festgelegte Integrationsprüfungen durchgeführt, um den Nachweis des einwandfreien Zusammenwirkens der integrierten Elemente zu erbringen.

Nach einer ausreichenden Hardware- und Software-Entwicklung nach [Abschnitt 7](#) und [Abschnitt 8](#) kann die Systemintegration nach [6.4](#) (Integration und Prüfung von Einheiten) beginnen.

6.4.3 Für die Integration und Prüfung von Einheiten erforderliche Informationen

Die folgenden Informationen müssen zur Verfügung gestellt werden:

- Sicherheitsziele in Übereinstimmung mit IEC 63168-2:20XX, 9.3;
- Konzept der funktionalen Sicherheit in Übereinstimmung mit IEC 63168-2:20XX, 10.5;
- Sicherheitsplan in Übereinstimmung mit [6.1.5](#).
- Konzept der technischen Sicherheit in Übereinstimmung mit [6.3.5](#);
- Systemdesignspezifikation in Übereinstimmung mit [6.3.5](#); und
- Hardware-Software-Schnittstellenspezifikation (HSI) in Übereinstimmung mit [6.3.5](#).

Die folgenden Informationen können berücksichtigt werden:

- Architektur des vernetzten Wohnumfelds (von einer externen Quelle);
- Konzepte der technischen Sicherheit anderer Systeme (von einer externen Quelle); und
- Berichte der Sicherheitsanalyse (siehe [6.3.5](#)).

6.4.4 Anforderungen und Empfehlungen

6.4.4.1 Schritte der Integration und Prüfung

Zum Nachweis, dass das Systemdesign mit den Anforderungen an die funktionale und die technische Sicherheit übereinstimmt, müssen Integrations- und Prüfaktivitäten durchgeführt werden für jede Ebene:

- der Hardware-Software-Integration;
- der Systemintegration; und
- der Integration in das vernetzte Wohnumfeld.

Jede Ebene der Integrationsprüfung muss ausgeführt werden, um nachzuweisen, dass das System Folgendes erreicht:

- a) die einwandfreie Implementierung der Anforderungen an die funktionale und die technische Sicherheit;
- b) das einwandfreie funktionale Verhalten, die Genauigkeit und den Zeitablauf der Sicherheitsmechanismen;
- c) die widerspruchsfreie und einwandfreie Implementierung der Schnittstellen;
- d) die Wirksamkeit des Diagnose- oder Ausfalldeckungsgrads der Sicherheitsmechanismen; und

ANMERKUNG Für eine detaillierte Erläuterung des Diagnosedeckungsgrads siehe [Anhang B](#).

- e) den erforderlichen Grad der Widerstandsfähigkeit.

6.4.4.2 Hardware-Software-Integration und Prüfung

Die nach [Abschnitt 7](#) entwickelte Hardware und die nach [Abschnitt 8](#) entwickelte Software müssen integriert werden, damit sie als Gegenstand der Prüfaktivitäten verwendet werden können.

Die Prüfung der Hardware-Software-Integration muss nach [Tabelle 5](#) durchgeführt werden.

Tabelle 5 – Verfahren für Hardware-Software-Integrationsprüfung

Verfahren		H-SIL			
		A	B	C	D
1	Funktionsprüfung				
1.1	Analyse der Anforderungen	++	++	++	++
1.2	Analyse und Erzeugung von Äquivalenzklassen	+	++	++	++
1.3	Grenzwertanalyse	+	+	++	++
1.4	Fehlerinjektionsprüfung	+	+	++	++
1.5	Langzeitprüfung	o	o	o	o
1.6	Nutzerprüfung unter Praxisbedingungen	o	o	o	o
2	Schnittstellenprüfung				
2.1	Prüfung von externen Schnittstellen	+	++	++	++
2.2	Prüfung von internen Schnittstellen	+	++	++	++
2.3	Interaktions-/Kommunikationsprüfung	o	o	o	o
3	Leistungsprüfung				
3.1	Analyse der Leistungsanforderungen	+	++	++	++
3.2	Ressourcennutzungsprüfung	+	+	+	++
3.3	Beanspruchungsprüfung	+	+	+	++
3.4	Prüfung der Störfestigkeit und der Widerstandsfähigkeit unter bestimmten Umgebungsbedingungen	o	o	o	o

6.4.4.3 Systemintegration und Prüfung

Die einzelnen Elemente, die in das System einbezogen werden, müssen in Übereinstimmung mit dem Systementwurf integriert und entsprechend den Systemintegrationsprüfungen geprüft werden.

ANMERKUNG Die Prüfungen dienen dem Nachweis dafür, dass alle Systemelemente einwandfrei zusammenwirken, die Anforderungen an die technische und funktionale Sicherheit erfüllen und ein angemessenes Vertrauensniveau bieten, dass ein unbeabsichtigtes Verhalten, welches ein Sicherheitsziel verletzen kann, nicht auftritt.

Die Systemintegrationsprüfung muss nach [Tabelle 6](#) durchgeführt werden.

Tabelle 6 – Verfahren für die Systemintegrationsprüfung

Verfahren		H-SIL			
		A	B	C	D
1	Funktionsprüfung				
1.1	Analyse der Anforderungen	++	++	++	++
1.2	Analyse und Erzeugung von Äquivalenzklassen	o	o	o	o
1.3	Grenzwertanalyse	+	+	++	++
1.4	Fehlerinjektionsprüfung	+	+	++	++
1.5	Langzeitprüfung	o	o	o	o
1.6	Nutzerprüfung unter Praxisbedingungen	o	o	o	o

Verfahren		H-SIL			
		A	B	C	D
2	Schnittstellenprüfung				
2.1	Prüfung von externen Schnittstellen	+	++	++	++
2.2	Prüfung von internen Schnittstellen	+	++	++	++
2.3	Interaktions-/Kommunikationsprüfung	++	++	++	++
3	Leistungsprüfung				
3.1	Analyse der Leistungsanforderungen	o	+	++	++
3.2	Ressourcennutzungsprüfung	o	+	+	++
3.3	Beanspruchungsprüfung	o	+	+	++
3.4	Prüfung der Störfestigkeit und der Widerstandsfähigkeit unter bestimmten Umgebungsbedingungen	++	++	++	++

6.4.4.4 Integration in das vernetzte Wohnumfeld und Prüfung

Die Einheit muss in das vernetzte Wohnumfeld integriert werden und es müssen die Integrationsprüfungen für das vernetzte Wohnumfeld durchgeführt werden.

Die Integrationsprüfungen für das vernetzte Wohnumfeld müssen nach [Tabelle 7](#) durchgeführt werden.

Tabelle 7 – Verfahren für die Integrationsprüfungen für das vernetzte Wohnumfeld

Verfahren		H-SIL			
		A	B	C	D
1	Funktionsprüfung				
1.1	Analyse der Anforderungen	++	++	++	++
1.2	Analyse und Erzeugung von Äquivalenzklassen	o	o	o	o
1.3	Grenzwertanalyse	+	+	++	++
1.4	Fehlerinjektionsprüfung	++	++	++	++
1.5	Langzeitprüfung	++	++	++	++
1.6	Nutzerprüfung unter Praxisbedingungen	++	++	++	++
2	Schnittstellenprüfung				
2.1	Prüfung von externen Schnittstellen	+	+	++	++
2.2	Prüfung von internen Schnittstellen	o	o	o	o
2.3	Interaktions-/Kommunikationsprüfung	++	++	++	++
3	Leistungsprüfung				
3.1	Analyse der Leistungsanforderungen	+	+	+	++
3.2	Ressourcennutzungsprüfung	o	+	+	++
3.3	Beanspruchungsprüfung	o	+	++	++
3.4	Prüfung der Störfestigkeit und der Widerstandsfähigkeit unter bestimmten Umgebungsbedingungen	o	+	++	++

6.4.5 Arbeitsergebnisse

- a) Sicherheitsplan (präzisiert) nach 6.4.4.1 bis 6.4.4.4.
- b) Spezifikation(en) der Integrationsprüfung nach 6.4.4.1 bis 6.4.4.4.
- c) Bericht(e) der Integrationsprüfung nach 6.4.4.1 bis 6.4.4.4.

6.5 Sicherheitsvalidierung

6.5.1 Zweck der Sicherheitsvalidierung

Das erste Ziel ist der Nachweis, dass die Sicherheitsziele eingehalten werden und die Konzepte der funktionalen Sicherheit für die funktionale Sicherheit der Einheit geeignet sind.

Das zweite Ziel ist der Nachweis, dass die Sicherheitsziele auf der Ebene des vernetzten Wohnumfelds fehlerfrei, vollständig und in vollem Umfang erreicht werden.

6.5.2 Allgemeines

Der Zweck der vorangegangenen Verifizierungsaktivitäten (z. B. Designverifizierung, Sicherheitsanalysen, Hardware-, Software- und Einheitenintegration und Prüfungen) besteht in dem Nachweis, dass die Ergebnisse der einzelnen Aktivitäten den festgelegten Anforderungen entsprechen.

Die Sicherheitsvalidierung umfasst auf der Grundlage von Untersuchungen und Prüfungen die Zusicherung, dass die Sicherheitsziele ausreichend sind und erreicht wurden.

6.5.3 Für die Sicherheitsvalidierung erforderliche Informationen

Die folgenden Informationen müssen zur Verfügung gestellt werden:

- a) Gefährdungsanalyse und Risikobewertung in Übereinstimmung mit IEC 63168-2:20XX, 9.3;
- a) Sicherheitsziele in Übereinstimmung mit IEC 63168-2:20XX, 9.3; und
- b) Konzept der funktionalen Sicherheit in Übereinstimmung mit IEC 63168-2:20XX, 10.5.

Die folgenden Informationen können berücksichtigt werden:

- Projektplan (präzisiert) (siehe 6.1.5);
- Konzept der technischen Sicherheit (siehe 6.3.5);
- Konzept der funktionalen Sicherheit (von einer externen Quelle);
- Sicherheitsplan (präzisiert) (siehe 6.4.5); und
- Berichte der Sicherheitsanalyse (siehe 6.3.5).

6.5.4 Anforderungen und Empfehlungen

6.5.4.1 Validierungsumgebung

Die Sicherheitsziele müssen für die in ein repräsentatives vernetztes Wohnumfeld integrierte Einheit validiert werden.

6.5.4.2 Planung der Validierung

Der Validierungsplan muss präzisiert werden, einschließlich:

- a) der Konfiguration der Einheit, die der Validierung unterzogen wird;
- b) der Spezifikation der Validierungsverfahren, der Prüffälle und der Annahmekriterien; und
- a) der Einrichtungen und der erforderlichen Umgebungsbedingungen.

6.5.4.3 Ausführung der Validierung

Die Sicherheitsziele der Einheit müssen auf der Ebene des vernetzten Wohnumfelds validiert werden, indem Folgendes bewertet wird:

- a) die Fähigkeit zur Unterstützung;
- b) die Wirksamkeit von Sicherheitsmaßnahmen zur Beherrschung von zufälligen und systematischen Ausfällen;
- c) die Wirksamkeit äußerer Maßnahmen.

Diese Anforderung gilt für die H-SILs (B), C und D nach 5.3: Die Validierung der Metriken für zufällige Hardware-Ausfälle muss auf der Ebene der Einheit für die Bewertung von Verletzungen der Sicherheitsziele aufgrund zufälliger Hardware-Ausfälle nach Abschnitt 7.4 anhand der in 6.3.4.4 definierten Zielwerte durchgeführt werden.

Es muss ein geeigneter Satz der folgenden Verfahren angewendet werden:

- wiederholbare Prüfungen mit festgelegten Prüfverfahren, Prüffällen und Annahme-/Rückweisungskriterien;

ANMERKUNG Werden die Prüfungen zur Validierung durchgeführt, können die gleichen Anforderungen, die für die Verifizierungsprüfung gelten, abgewendet werden.

- Analysen;

BEISPIEL FMEA, FTA, ETA, Simulation.

- Langzeitprüfungen;
- Nutzerprüfungen unter Praxisbedingungen; und
- Reviews.

6.5.4.4 Bewertung

Die Validierungsergebnisse müssen bewertet werden.

6.5.5 Arbeitsergebnisse

- a) Sicherheitsplan (präzisiert) nach 6.5.4.2.
- b) Validierungsbericht nach 6.5.4.3 und 6.5.4.4.

7 Produktentwicklung auf der Hardware-Ebene

7.1 Planung der Hardware-Entwicklung

7.1.1 Zweck

Ziel der Planung der Hardware-Entwicklung ist die Festlegung und Planung der Aktivitäten für die funktionale Sicherheit während der einzelnen Unterphasen der Hardware-Entwicklung. Dazu gehören auch die notwendigen Unterstützungsprozesse, die in IEC 63168-4 beschrieben sind.

Diese Planung der Hardware-spezifischen Sicherheitsaktivitäten ist im Sicherheitsplan enthalten (siehe IEC 63168-1:20XX, 5.4.7, und 6.1.4 dieses Dokuments).

7.1.2 Allgemeines

Die notwendigen Aktivitäten und Prozesse zur Entwicklung der Hardware, die die Sicherheitsanforderungen erfüllt, werden geplant. Bild 4 veranschaulicht die Schritte des Produktentwicklungsprozesses auf der Hardware-Ebene, um die Anforderungen dieses Dokuments zu erfüllen.

Zu den notwendigen Aktivitäten und Prozessen für die Produktentwicklung auf der Hardware-Ebene gehören:

- die Hardware-Implementierung des Konzepts der technischen Sicherheit nach 6.3.5;
- die Analyse potentieller Hardware-Fehler und von deren Auswirkungen; und
- die Abstimmung mit der Software-Entwicklung.

Im Gegensatz zu den Unterphasen der Software-Entwicklung enthalten die Unterphasen der Hardware-Entwicklung einen Abschnitt, der quantitative Bewertungen der gesamten Hardware-Architektur der Einheit beschreibt. In 7.4 wird ein Verfahren beschrieben, um zu bewerten, ob das Restrisiko von Verletzungen der Sicherheitsziele ausreichend gering ist.

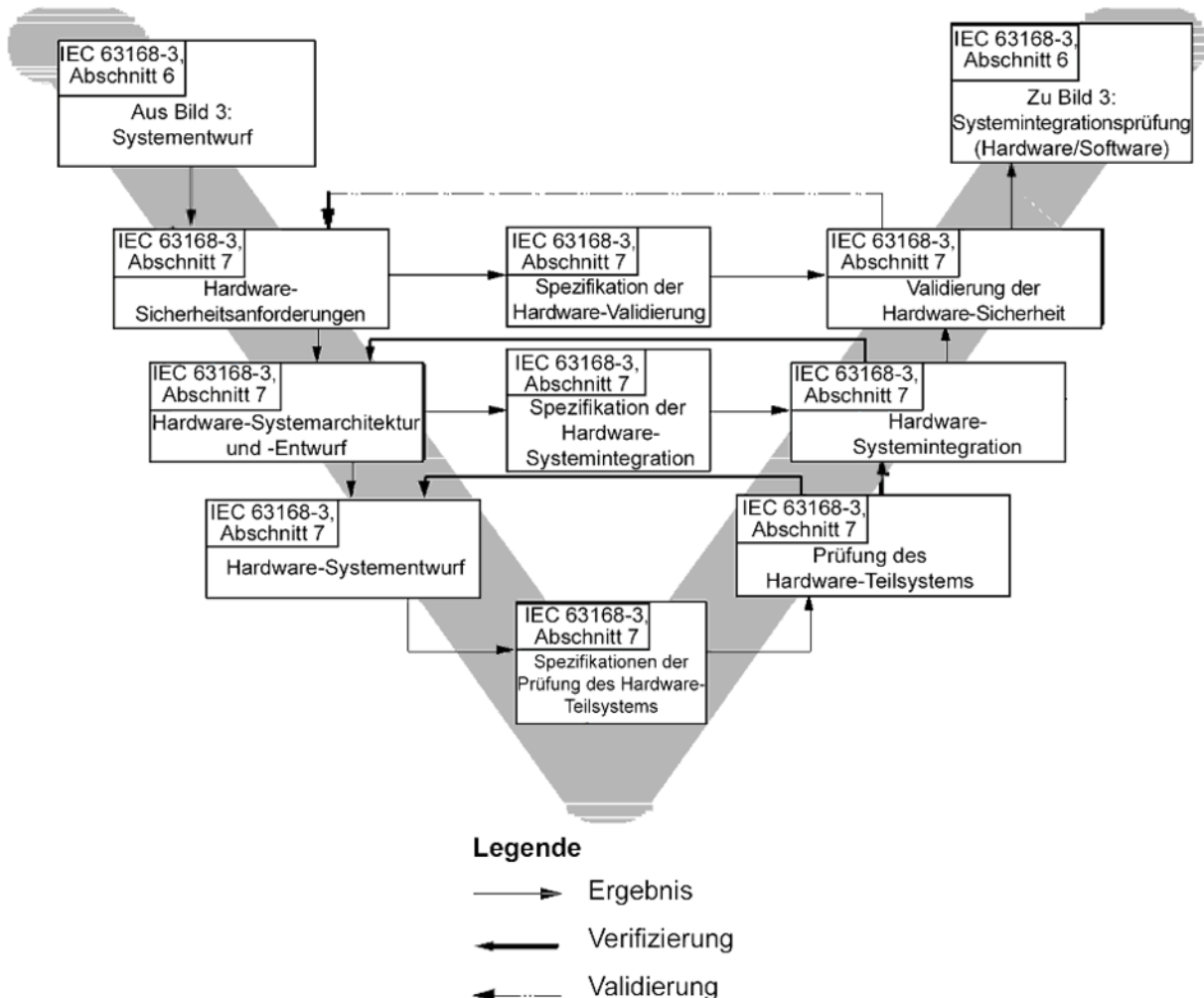


Bild 4 – Referenzphasenmodell für die Produktentwicklung auf Hardware-Ebene

7.1.3 Für die Planung der Hardware-Entwicklung erforderliche Informationen

Die folgenden Informationen müssen zur Verfügung gestellt werden:

- Projektplan (präzisiert) in Übereinstimmung mit 6.1. 5; und
- Sicherheitsplan (präzisiert) in Übereinstimmung mit 6.1.5.

Die folgenden Informationen können berücksichtigt werden:

- Qualifizierungsbericht (der Hardware-Komponenten oder -Teile), falls anwendbar.

7.1.4 Anforderungen und Empfehlungen

7.1.4.1 Planung der Sicherheitsaktivitäten auf der Hardware-Ebene

Der Sicherheitsplan nach IEC 63168-1 muss in Übereinstimmung mit der Planung der Aktivitäten in [8.1](#) in Bezug auf die Aktivitäten für die Produktentwicklung auf der Hardware-Ebene ausführlich beschrieben werden, einschließlich der Festlegung geeigneter Verfahren und Maßnahmen.

7.1.4.2 Anpassung des Sicherheitslebenszyklus auf der Hardware-Ebene

Die Anpassung der Aktivitäten des Sicherheitslebenszyklus für die Produktentwicklung auf der Hardware-Ebene muss nach IEC 63168-1:20XX, 5.4.7.3.4, erfolgen und basiert auf dem in [Bild 4](#) dargestellten Referenzphasenmodell.

7.1.4.3 Wiederverwendung von Hardware-Komponenten

Die Wiederverwendung von Hardware-Komponenten oder die Verwendung von qualifizierten Hardware-Komponenten oder -Teilen muss ermittelt werden und die sich daraus ergebende Anpassung der Sicherheitsaktivitäten muss beschrieben werden.

7.1.5 Arbeitsergebnis

Das Arbeitsergebnis der Planung der Hardware-Entwicklung ist der Sicherheitsplan (präzisiert) nach [7.1.4](#).

7.2 Festlegung der Spezifikation der Hardware-Sicherheitsanforderungen

7.2.1 Zweck

Das erste Ziel dieser Unterphase ist die Festlegung der Hardware-Sicherheitsanforderungen. Diese werden aus dem Konzept der technischen Sicherheit und der Spezifikation des Systementwurfs abgeleitet.

Das zweite Ziel besteht im Nachweis, dass die Hardware-Sicherheitsanforderungen mit dem Konzept der technischen Sicherheit und der Spezifikation des Systementwurfs vereinbar sind.

Ein weiteres Ziel dieser Phase ist die genaue Beschreibung der in [6.3.4.6](#) eingeleiteten Hardware-Software-Schnittstellenspezifikation (HSI).

7.2.2 Allgemeines

Die Anforderungen an die technische Sicherheit werden der Hardware und der Software zugeordnet. Die Anforderungen, die beidem zugeordnet werden, werden weiter unterteilt, um die Sicherheitsanforderungen nur für die Hardware zu erhalten. Die Hardware-Sicherheitsanforderungen werden unter Berücksichtigung der Entwurfsbeschränkungen und der Auswirkungen dieser Entwurfsbeschränkungen auf die Hardware weiter detailliert.

7.2.3 Für die Festlegung der Spezifikation der Hardware-Sicherheitsanforderungen erforderliche Informationen

Die folgenden Informationen müssen zur Verfügung gestellt werden:

- Sicherheitsplan (präzisiert) in Übereinstimmung mit [7.1.5](#);
- Konzept der technischen Sicherheit in Übereinstimmung mit [6.3.5](#);
- Spezifikation des Systementwurfs in Übereinstimmung mit [6.3.5](#); und
- Hardware-Software-Schnittstellenspezifikation in Übereinstimmung mit [6.3.5](#).

Die folgenden Informationen können berücksichtigt werden:

- Spezifikation der Software-Sicherheitsanforderungen (siehe 8.2.5).

7.2.4 Anforderungen und Empfehlungen

7.2.4.1 Hardware-Sicherheitsanforderungen

Eine Spezifikation der Hardware-Sicherheitsanforderungen für die Hardware-Elemente der Einheit muss von den Anforderungen an die technische Sicherheit, die der Hardware zugeordnet sind, abgeleitet werden.

Die Spezifikation der Hardware-Sicherheitsanforderungen muss alle auf die Sicherheit bezogenen Hardware-Anforderungen enthalten, einschließlich der folgenden:

ANMERKUNG 1 Die unter a), b), c) oder d) beschriebenen Hardware-Sicherheitsanforderungen umfassen die Attribute, die zur Sicherstellung der Wirksamkeit der genannten Sicherheitsmechanismen erforderlich sind.

- a) die Hardware-Sicherheitsanforderungen und die entsprechenden Attribute der Sicherheitsmechanismen zur Beherrschung interner Ausfälle der Hardware der Einheit, dazu gehören auch interne Sicherheitsmechanismen zur Abdeckung transienter Fehlzustände aufgrund der verwendeten Technologie;

BEISPIEL 1 Zu den Attributen können die Zeitablauf- und Erkennungsfähigkeiten eines Watchdogs gehören.

- b) die Hardware-Sicherheitsanforderungen und die entsprechenden Attribute der Sicherheitsmechanismen, um sicherzustellen, dass das Element gegenüber Ausfällen außerhalb des Elements tolerant ist;

BEISPIEL 2 Das für eine elektronische Steuerungseinheit erforderliche funktionale Verhalten im Falle eines externen Ausfalls, z. B. eines offenen Stromkreises an einem Eingang der elektronischen Steuerungseinheit.

- c) die Hardware-Sicherheitsanforderungen und die entsprechenden Attribute der Sicherheitsmechanismen, um die Sicherheitsanforderungen anderer Elemente zu erfüllen;

BEISPIEL 3 Diagnose von Sensoren oder Stellgliedern.

- d) die Hardware-Sicherheitsanforderungen und die entsprechenden Attribute der Sicherheitsmechanismen, um die internen und externen Ausfälle zu erkennen und anzuzeigen; und

BEISPIEL 4 Die festgelegte Fehlerreaktionszeit des Hardware-Teils eines Sicherheitsmechanismus, die mit der Fehlertoleranzzeit übereinstimmt.

- e) die Hardware-Sicherheitsanforderungen, die keine Sicherheitsmechanismen festlegen.

BEISPIEL 5 Beispiele sind:

- Anforderungen an die Hardware-Elemente zur Einhaltung der Zielwerte für zufällige Hardware-Ausfälle, wie beschrieben;
- Anforderungen zur Vermeidung eines bestimmten Verhaltens (z. B. „ein bestimmter Sensor darf keine instabile Ausgangsgröße erzeugen“);
- Anforderungen an Hardware-Elemente, die die vorgesehene Funktionalität implementieren; und
- Anforderungen, die Entwurfsmaßnahmen an Kabelbäumen oder Steckverbindern festlegen.

Die Kriterien für die Designverifizierung der Hardware der Einheit oder des Elements müssen festgelegt werden, einschließlich der Umgebungsbedingungen (Temperatur, Schwingung, elektromagnetische Beeinflussung usw.), der spezifischen Betriebsumgebung (Versorgungsspannung, Einsatzprofil usw.) und der komponentenspezifischen Anforderungen.

7.2.4.2 Verifizierung der Software-Sicherheitsanforderungen

Das Software-Sicherheitsanforderungen müssen in Übereinstimmung mit IEC 63168-4:20XX, Abschnitt 11, verifiziert werden, um Folgendes nachzuweisen:

- a) Übereinstimmung mit dem Konzept der technischen Sicherheit, der Spezifikation des Systementwurfs und den Hardware-Spezifikationen;
- b) Vollständigkeit bezüglich der Anforderungen an die technische Sicherheit, die dem Hardware-Element zugeordnet sind;
- c) Übereinstimmung mit den entsprechenden Software-Sicherheitsanforderungen; und
- d) Fehlerfreiheit und Genauigkeit.

7.2.4.3 Hardware-Software-Schnittstellenspezifikation

Die in 6.3.4.6 eingeleitete HSI-Spezifikation muss so weit präzisiert werden, dass die einwandfreie Steuerung und Nutzung der Hardware durch die Software möglich ist, und sie muss alle sicherheitsbezogenen Abhängigkeiten zwischen der Hardware und der Software beschreiben.

7.2.5 Arbeitsergebnisse

- a) Spezifikation der Hardware-Sicherheitsanforderungen (einschließlich Prüf- und Qualifizierungskriterien) nach 7.2.4.1.
- b) Hardware-Software-Schnittstellenspezifikation (präzisiert) nach 7.2.4.3.
- c) Verifizierungsbericht der Hardware-Sicherheitsanforderungen nach 7.2.4.2.

7.3 Hardware-Design

7.3.1 Zweck des Hardware-Designs

Das erste Ziel des Hardware-Designs ist es, die Hardware in Übereinstimmung mit der Systemdesignspezifikation und den Hardware-Sicherheitsanforderungen zu entwerfen.

Das zweite Ziel besteht darin, das Hardware-Design anhand der Systemdesignspezifikation und der Hardware-Sicherheitsanforderungen zu verifizieren.

7.3.2 Allgemeines

Das Hardware-Design umfasst das Hardware-Architekturdesign und das detaillierte Hardware-Design. Das Hardware-Architekturdesign stellt alle Hardware-Komponenten und ihre Interaktionen untereinander dar. Das detaillierte Hardware-Design findet auf der Ebene der elektrischen Schaltpläne statt, die die Verbindungen zwischen den Hardware-Teilen, die die Hardware-Komponenten bilden, darstellen.

Um ein einzelnes Hardware-Design zu entwickeln, müssen sowohl die Hardware-Sicherheitsanforderungen als auch alle nicht sicherheitsbezogenen Anforderungen erfüllt werden. Daher werden in dieser Unterphase die Sicherheitsanforderungen und die nicht sicherheitsbezogenen Anforderungen innerhalb eines Entwicklungsprozesses behandelt.

7.3.3 Für das Hardware-Design erforderliche Informationen

Die folgenden Informationen müssen zur Verfügung gestellt werden:

- Spezifikation der Hardware-Sicherheitsanforderungen in Übereinstimmung mit 7.2.5;
- Hardware-Software-Schnittstellenspezifikation (präzisiert) in Übereinstimmung mit 7.2.5;
- Systementwurfsspezifikation in Übereinstimmung mit 6.3.5; und
- Sicherheitsplan (präzisiert) in Übereinstimmung mit 7.1.5.

Die folgenden Informationen können berücksichtigt werden:

- Spezifikation der Software-Sicherheitsanforderungen (siehe 8.2.5).

7.3.4 Anforderungen und Empfehlungen

7.3.4.1 Hardware-Architekturdesign

Die Hardware-Architektur muss die in 7.2.4 definierten Hardware-Sicherheitsanforderungen umsetzen.

Jede Hardware-Komponente muss den höchsten H-SIL aus den Hardware-Sicherheitsanforderungen erben, die sie implementiert.

Um Ausfälle aufgrund einer hohen Komplexität zu vermeiden, muss das Hardware-Architekturdesign unter Anwendung der in Tabelle 8 aufgeführten Grundsätze die folgenden Merkmale aufweisen:

- a) Modularität;
- b) eine angemessene Granularität; und
- c) Einfachheit.

Tabelle 8 – Merkmale des modularen Hardware-Designs

Merkmale		H-SIL			
		A	B	C	D
1	Hierarchischer Entwurf	+	+	+	+
2	Genau definierte Schnittstellen der sicherheitsbezogenen Komponenten	++	++	++	++
3	Vermeidung unnötiger Komplexität von Schnittstellen	+	+	+	+
4	Vermeidung unnötiger Komplexität von Hardware-Komponenten	+	+	+	+
5	Instandhaltbarkeit (Wartung)	+	+	++	++
6	Prüfbarkeit ^a	+	+	++	++
^a Die Prüfbarkeit umfasst die Prüfbarkeit während der Entwicklung und des Betriebs.					

Beim Hardware-Architekturdesign müssen nicht funktionale Ursachen für den Ausfall einer sicherheitsbezogenen Hardware-Komponente berücksichtigt werden, einschließlich der folgenden Einflüsse, falls zutreffend: Temperatur, Schwingungen, Wasser, Staub, elektromagnetische Beeinflussung und Übersprechen, das entweder von anderen Hardware-Komponenten der Hardware-Architektur oder von ihrer Umgebung ausgeht.

7.3.4.2 Detailliertes Hardware-Design

Beim detaillierten Design der Hardware-Architektur müssen nicht funktionale Ursachen für den Ausfall eines sicherheitsbezogenen Hardware-Teils berücksichtigt werden, einschließlich der folgenden Einflüsse, falls zutreffend: Temperatur, Schwingungen, Wasser, Staub, elektromagnetische Beeinflussung und Übersprechen, das entweder von anderen Hardware-Teilen der Hardware-Komponenten oder von ihrer Umgebung ausgeht.

Die Betriebsbedingungen der für das detaillierte Hardware-Design verwendeten Hardware-Teile müssen mit der Spezifikation ihrer Umgebungs- und Betriebsgrenzen übereinstimmen.

Die Grundsätze eines robusten Entwurfs müssen berücksichtigt werden.

ANMERKUNG Die Grundsätze eines robusten Entwurfs können durch die Verwendung von Checklisten auf der Grundlage von QM-Verfahren nachgewiesen werden.

BEISPIEL Konservative Spezifikation von Komponenten.

7.3.4.3 Sicherheitsanalysen

Sicherheitsanalysen des Hardware-Designs zur Ermittlung der Ursachen für Ausfälle und der Auswirkungen von Fehlzuständen müssen nach [Tabelle 9](#) durchgeführt werden.

ANMERKUNG 1 Der ursprüngliche Zweck dieser Sicherheitsanalysen ist die Unterstützung der Spezifikation des Hardware-Designs. Anschließend können die Sicherheitsanalysen zur Verifizierung des Hardware-Designs verwendet werden (siehe [6.3.4.4](#)).

ANMERKUNG 2 Um die Spezifikation des Hardware-Designs zu unterstützen, kann eine qualitative Analyse angemessen und ausreichend sein.

Tabelle 9 – Sicherheitsanalyse des Hardware-Designs

Verfahren		H-SIL			
		A	B	C	D
1	Deduktive Analyse ^a	o	+	++	++
2	Induktive Analyse ^b	++	++	++	++
ANMERKUNG Der Detaillierungsgrad der Analyse richtet sich nach dem Detaillierungsgrad des Designs. Beide Verfahren können in bestimmten Fällen mit unterschiedlichen Detaillierungsgraden durchgeführt werden.					
^a Ein übliches deduktives Analyseverfahren ist die FTA.					
^b Ein übliches induktives Analyseverfahren ist die FMEA.					

7.3.4.4 Verifizierung des Hardware-Designs

Das Hardware-Design muss nach IEC 63168-4:20XX, Abschnitt 11, auf Übereinstimmung und Vollständigkeit in Bezug auf die Hardware-Sicherheitsanforderungen verifiziert werden. Dafür müssen die in [Tabelle 10](#) aufgeführten Verfahren berücksichtigt werden.

Tabelle 10 – Verifizierung des Hardware-Designs

Verfahren		H-SIL			
		A	B	C	D
1a	Walk-through des Hardware-Designs ^a	++	++	o	o
1b	Inspektion des Hardware-Designs ^a	+	+	++	++
2	Sicherheitsanalysen	Siehe Tabelle 9			
3a	Simulation ^b	o	+	+	+
3b	Entwicklung mit Hilfe eines Hardware-Prototyps ^b	o	+	+	+
ANMERKUNG Der Anwendungsbereich dieser Verifizierungsprüfungen ist die technische Fehlerfreiheit des Hardware-Designs.					
^a Die Verfahren 1a und 1b dienen der Überprüfung der vollständigen und einwandfreien Umsetzung der Hardware-Sicherheitsanforderungen im Hardware-Design.					
^b Die Verfahren 3a und 3b dienen der Überprüfung bestimmter Punkte des Hardware-Designs (z. B. als Fehlerinjektionstechnik), für die die Analyseverfahren 1 und 2 als unzureichend angesehen werden.					

7.3.4.5 Produktion, Betrieb, Instandhaltung und Außerbetriebnahme

Sicherheitsbezogene Sondereigenschaften müssen festgelegt werden, wenn die Sicherheitsanalyse zeigt, dass sie maßgeblich sind, mit:

- a) den Verifizierungsmaßnahmen für Produktion und Betrieb; und
- b) den Annahmekriterien für diese Maßnahmen.

BEISPIEL Eine Sicherheitsanalyse des Hardware-Entwurfs, der auf neuen Sensortechnologien beruht (z. B. Kamera- oder Radarsensoren), kann die Bedeutung spezieller Installationsverfahren für diese Sensoren aufzeigen. In einem solchen Fall können zusätzliche Verifizierungsmaßnahmen für diese Komponenten während der Produktionsphase erforderlich sein.

Anweisungen für die Montage, Instandhaltung, Demontage und Außerbetriebnahme von sicherheitsbezogenen Hardware-Elementen müssen festgelegt werden, wenn diese Vorgänge Auswirkungen auf das Konzept der technischen Sicherheit haben können.

7.3.5 Arbeitsergebnisse

- a) Hardware-Designspezifikation nach 7.3.4.1 und 7.3.4.2.
- b) Bericht der Hardware-Sicherheitsanalyse nach 7.3.4.3.
- c) Verifizierungsbericht des Hardware-Designs nach 7.3.4.4.
- d) Spezifikation der Anforderungen an Produktion, Betrieb, Instandhaltung und Außerbetriebnahme nach 7.3.4.5.

7.4 Bewertung von Verletzungen der Sicherheitsziele aufgrund zufälliger Hardware-Ausfälle

7.4.1 Zweck

Ziel der Anforderungen ist es, Kriterien zur Verfügung zu stellen, die in einer Begründung dafür verwendet werden können, dass das Restrisiko einer Verletzung von Sicherheitszielen aufgrund zufälliger Hardware-Ausfälle der Einheit ausreichend gering ist.

7.4.2 Allgemeines

Es wird ein Verfahren (siehe 7.4.4.1) vorgeschlagen, um zu bewerten, ob das Restrisiko der Verletzung von Sicherheitszielen ausreichend gering ist.

Das Verfahren besteht in der Verwendung einer Wahrscheinlichkeitsmetrik, die als „Wahrscheinlichkeitsmetrik für zufällige Hardware-Ausfälle“ (PMHF) bezeichnet wird, um die Verletzung des betrachteten Sicherheitsziels z. B. anhand der quantifizierten FTA zu bewerten und das Ergebnis dieser Quantifizierung mit einem Zielwert zu vergleichen.

Das Verfahren kann iterativ während des Hardware-Architekturdesigns und des detaillierten Hardware-Designs angewendet werden.

Der Anwendungsbereich dieses Abschnitts ist auf die zufälligen Hardware-Ausfälle der Einheit beschränkt. Die in den Analysen betrachteten Teile sind die elektrischen und elektronischen Hardware-Teile. Für elektromechanische Hardware-Teile werden nur die elektrischen Ausfallarten und die Ausfallrate betrachtet.

7.4.3 Für die Bewertung der Verletzungen von Sicherheitszielen durch zufällige Hardware-Ausfälle erforderliche Informationen

Die folgenden Informationen müssen zur Verfügung gestellt werden:

- a) Spezifikation der Hardware-Sicherheitsanforderungen in Übereinstimmung mit 7.2.5;
- b) Hardware-Designspezifikation in Übereinstimmung mit 7.3.5; und
- c) Analysebericht der Hardware-Sicherheit in Übereinstimmung mit 7.3.5.

Die folgenden Informationen können berücksichtigt werden:

- Konzept der technischen Sicherheit (siehe 6.3.5); und
- Spezifikation des Systemdesign (siehe 6.3.5.).

7.4.4 Anforderungen und Empfehlungen

7.4.4.1 Bewertung einer Wahrscheinlichkeitsmetrik für zufällige Hardware-Ausfälle (PMHF)

Diese Anforderung gilt für die H-SILs (B), C und D nach 5.3. Quantitative Zielwerte für die höchste Wahrscheinlichkeit der Verletzung jedes Sicherheitsziels aufgrund von zufälligen Hardware-Ausfällen nach 6.3.4.4 müssen unter Verwendung einer der Quellen a), b) oder c) von Referenzzielwerten definiert werden, wie nachstehend beschrieben:

- a) abgeleitet aus Tabelle 11, oder
- b) abgeleitet aus Felddaten von ähnlichen bewährten Designprinzipien, oder
- c) abgeleitet aus quantitativen Analyseverfahren, die für ähnliche bewährte Designprinzipien angewendet werden.

ANMERKUNG 1 Diese aus den Quellen a), b) oder c) abgeleiteten quantitativen Zielwerte haben keine absolute Bedeutung und sind nur nützlich, um einen neues Design mit bestehenden Design zu vergleichen. Sie sind als Designleitfaden bestimmt und um den Nachweis zu erbringen, dass das Design die Sicherheitsziele erfüllt.

ANMERKUNG 2 Zwei ähnliche Entwürfe haben ähnliche Funktionalitäten und ähnliche Sicherheitsziele mit dem gleichen zugeordneten H-SIL.

ANMERKUNG 3 Weitere Einzelheiten zur Bewertung einer Wahrscheinlichkeitsmetrik für zufällige Hardware-Ausfälle siehe Anhang A.

Tabelle 11 – Mögliche Quelle für die Ableitung der Zielwerte für zufällige Hardware-Ausfälle

H-SIL	Zielwerte für zufällige Hardware-Ausfälle
D	$< 10^{-8} \text{ h}^{-1}$
C	$< 10^{-7} \text{ h}^{-1}$
B	$< 10^{-7} \text{ h}^{-1}$
<p>ANMERKUNG 1 Die in dieser Tabelle beschriebenen quantitativen Zielwerte werden als mittlere Wahrscheinlichkeit je Stunde während der Betriebslebensdauer der Einheit ausgedrückt.</p> <p>ANMERKUNG 2 Die in dieser Tabelle beschriebenen quantitativen Zielwerte können nach 5.2 angepasst werden, um spezifischen Verwendungen der Einheit gerecht zu werden (z. B. wenn die Einheit in der Lage ist, das Sicherheitsziel für eine längere Dauer als die typische Verwendung zu verletzen).</p>	

7.4.4.2 Verifizierungsprüfung

Diese Anforderung gilt für die H-SILs (B), C und D nach 5.3. Eine Verifizierungsprüfung der Analyse, die sich aus dem Anforderungssatz in 7.4.4.1 ergibt, muss durchgeführt werden, um die technische Fehlerfreiheit und Vollständigkeit in Übereinstimmung mit IEC 63168-4:20XX, Abschnitt 11, nachzuweisen.

7.4.5 Arbeitsergebnisse

- a) Analyse von Verletzungen der Sicherheitsziele aufgrund zufälliger Hardware-Ausfälle nach 7.4.4.1.
- b) Review-Bericht der Verletzungen von Sicherheitszielen durch zufällige Hardware-Ausfälle nach 7.4.4.2.

7.5 Hardware-Integration und Prüfung

7.5.1 Zweck der Integration und Prüfung von Hardware

Das Ziel besteht darin, durch Prüfung die Übereinstimmung der entwickelten Hardware mit den Hardware-Sicherheitsanforderungen sicherzustellen.

Die Anforderungen nach 7.5.4 gelten für die Hardware eines Elements.

7.5.2 Allgemeines

Die in diesem Abschnitt beschriebenen Aktivitäten zielen darauf ab, Hardware-Elemente zu integrieren und das Hardware-Design zu prüfen, um dessen Übereinstimmung mit den Hardware-Sicherheitsanforderungen entsprechend dem zutreffenden H-SIL nachzuweisen.

7.5.3 Für die Integration und Prüfung von Hardware erforderliche Informationen

Die folgenden Informationen müssen zur Verfügung gestellt werden:

- Sicherheitsplan (präzisiert) in Übereinstimmung mit 6.1.5 und 7.1.5;
- Spezifikation der Hardware-Sicherheitsanforderungen in Übereinstimmung mit 7.2.5; und
- Hardware-Designspezifikation in Übereinstimmung mit 7.3.5.

Die folgenden Informationen können berücksichtigt werden:

- Projektplan (präzisiert) (siehe 6.1.5); und
- Berichte der Hardware-Sicherheitsanalyse (siehe 7.3.5).

7.5.4 Anforderungen und Empfehlungen

7.5.4.1 Verfahren für die Prüfung der Hardware-Integration

Die Aktivitäten der Hardware-Integration und der Prüfung müssen nach IEC 63168-4:20XX, Abschnitt 11, durchgeführt werden.

Die Hardware-Integrationsprüfung muss nach Tabelle 12 durchgeführt werden.

Tabelle 12 – Verfahren der Hardware-Integrationsprüfung

Verfahren		H-SIL			
		A	B	C	D
1	Funktionsprüfung				
1.1	Analyse der Anforderungen	++	++	++	++
1.2	Analyse und Erzeugung von Äquivalenzklassen	+	+	++	++
1.3	Grenzwertanalyse	+	+	++	++
1.4	Fehlerinjektionsprüfung	+	+	++	++
2	Elektrische Prüfung	++	++	++	++

Verfahren		H-SIL			
		A	B	C	D
3	Prüfung der Widerstandsfähigkeit				
3.1	Umweltprüfung mit Verifizierung der Grundfunktionen	++	++	++	++
3.2	Erweiterte Funktionsprüfung	o	+	+	++
3.3	Mechanische Prüfung	++	++	++	++
3.4	Beschleunigte Lebensdauerprüfung	+	+	++	++
3.5	EMV- und ESD-Prüfung	++	++	++	++

7.5.4.2 Zweck der Hardware-Integrationsprüfung

Mit den ausgewählten Prüfverfahren muss nachgewiesen werden, dass die Hardware Folgendes erreicht:

- a) Vollständigkeit und Fehlerfreiheit der Implementierung der Sicherheitsmechanismen gegenüber den Hardware-Sicherheitsanforderungen; und
- b) Widerstandsfähigkeit der Hardware gegenüber äußeren Beanspruchungen.

7.5.5 Arbeitsergebnisse

- a) Hardware-Verifizierungsplan (präzisiert) nach 7.5.4.1 bis 7.5.4.2.
- b) Spezifikation des Hardware-Verifizierung nach 7.5.4.1 bis 7.5.4.2.
- c) Hardware-Verifizierungsbericht nach 7.5.4.1 bis 7.5.4.2.

8 Produktentwicklung auf der Software-Ebene

8.1 Planung der Software-Entwicklung

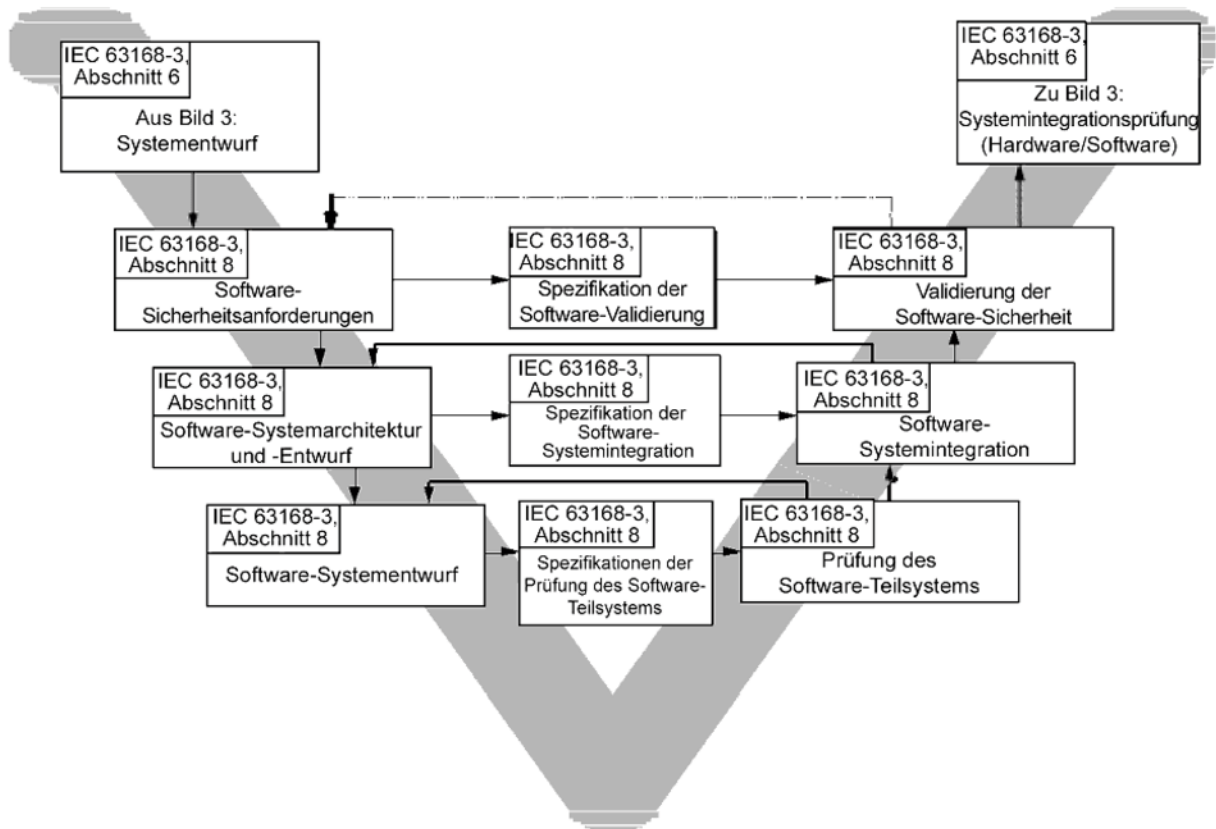
8.1.1 Zweck der Planung der Software-Entwicklung

Ziel ist die Planung und Einleitung der Aktivitäten für das Erreichen der funktionalen Sicherheit während der Unterphasen der Software-Entwicklung.

8.1.2 Allgemeines

Die Unterphasen der Software-Entwicklung und die Unterstützungsprozesse (siehe IEC 63168-4) werden entsprechend dem Umfang und der Komplexität der Entwicklung der Einheit festgelegt und geplant. Die Unterphasen der Software-Entwicklung und die Unterstützungsprozesse werden durch die Festlegung der geeigneten Verfahren eingeleitet, um die Anforderungen und den jeweiligen H-SIL zu erfüllen. Die Verfahren werden durch Leitfäden und Werkzeuge unterstützt, die für jede Unterphase und jeden Unterstützungsprozess festgelegt und geplant werden.

Bild 5 veranschaulicht den Prozess der Software-Entwicklung. In den folgenden Abschnitten und Tabellen im gesamten Abschnitt 9 wird jedes Kästchen des Diagramms im Einzelnen erläutert.



Legende

- Ergebnis
- ← Verifizierung
- ← Validierung

Bild 5 – Referenzphasenmodell für die Produktentwicklung auf der Software-Ebene

8.1.3 Für die Planung der Software-Entwicklung erforderliche Informationen

Die folgenden Informationen müssen zur Verfügung gestellt werden:

- Projektplan (präzisiert) in Übereinstimmung mit 6.1.5;
- Sicherheitsplan (präzisiert) in Übereinstimmung mit 6.4.5;
- Konzept der technischen Sicherheit in Übereinstimmung mit 6.3.5; und
- Spezifikation des Systementwurfs in Übereinstimmung mit 6.3.5.

Die folgenden Informationen können berücksichtigt werden:

- verfügbare qualifizierte Software-Werkzeuge;
- verfügbare qualifizierte Software-Komponenten;
- Entwurfs- und Codierungsleitfäden für Modellierungs- und Programmiersprachen (von einer externen Quelle);
- Anwendungsleitfäden für Verfahren (von einer externen Quelle); und
- Anwendungsleitfäden für Werkzeuge (von einer externen Quelle).

8.1.4 Anforderungen und Empfehlungen

8.1.4.1 Planung der Sicherheitsaktivitäten auf der Software-Ebene

Die Aktivitäten und die Festlegung geeigneter Verfahren für die Produktentwicklung auf der Software-Ebene müssen geplant werden.

ANMERKUNG Bei der Auswahl der Verfahren und Maßnahmen sollte berücksichtigt werden, dass neben der manuellen Codierung auch die modellbasierte Entwicklung angewendet werden kann, bei der der Quell- oder Objektcode automatisch aus Modellen erzeugt wird.

8.1.4.2 Anpassung des Sicherheitslebenszyklus auf der Software-Ebene

Die Anpassung des Lebenszyklus für die Produktentwicklung auf der Software-Ebene muss nach IEC 63168-1:20XX, 5.4.7.3.4, erfolgen.

ANMERKUNG Es ist üblich, einzelne Phasen zu kombinieren, wenn das verwendete Verfahren eine klare Unterscheidung zwischen den Phasen erschwert. So können z. B. der Entwurf der Software-Architektur und die Software-Implementierung nacheinander mit demselben rechnerunterstützten Entwicklungswerkzeug erstellt werden, wie dies im modellbasierten Entwicklungsprozess geschieht.

8.1.5 Arbeitsergebnisse

- a) Sicherheitsplan (präzisiert) nach [8.1.4.1](#) bis [8.1.4.2](#).

8.2 Festlegung der Spezifikation der Software-Sicherheitsanforderungen

8.2.1 Zweck der Festlegung der Spezifikation der Software-Sicherheitsanforderungen

Das erste Ziel ist die Ableitung der Software-Sicherheitsanforderungen, einschließlich des H-SIL, aus den Anforderungen an die technische Sicherheit.

Das zweite Ziel besteht im Nachweis, dass die Software-Sicherheitsanforderungen mit dem Konzept der technischen Sicherheit übereinstimmen.

8.2.2 Allgemeines

Die Anforderungen an die technische Sicherheit werden in der Systemdesignphase nach [Abschnitt 6](#) präzisiert und der Hardware und Software zugeordnet. Bei der Spezifikation der Software-Sicherheitsanforderungen werden die Beschränkungen der Hardware und die Auswirkungen dieser Beschränkungen auf die Software berücksichtigt. Diese Unterphase umfasst die Spezifikation der Software-Sicherheitsanforderungen zur Unterstützung der danach folgenden Designphasen.

8.2.3 Für die Festlegung der Spezifikation der Software-Sicherheitsanforderungen erforderliche Informationen

Die folgenden Informationen müssen zur Verfügung gestellt werden:

- Konzept der technischen Sicherheit in Übereinstimmung mit [6.3.5](#);
- Systemdesignspezifikation in Übereinstimmung mit [6.3.5](#);
- Hardware-Software-Schnittstellenspezifikation (HSI) in Übereinstimmung mit [6.3.5](#); und
- Sicherheitsplan in Übereinstimmung mit [8.1.5](#).

Die folgenden Informationen können berücksichtigt werden:

- Hardware-Designspezifikation in Übereinstimmung mit [7.3.5](#); und
- Anwendungsleitfäden für Verfahren (von einer externen Quelle).

8.2.4 Anforderungen und Empfehlungen

8.2.4.1 Spezifikation der Software-Sicherheitsanforderungen

Die Spezifikation der Software-Sicherheitsanforderungen muss die Software-Sicherheitsanforderungen für folgende Funktionen, falls zutreffend, beschreiben:

- Funktionen, die es dem System ermöglichen, einen sicheren Zustand zu erreichen oder aufrechtzuerhalten;
- Funktionen im Zusammenhang mit der Erkennung, Anzeige und Behandlung von Fehlzuständen sicherheitsbezogener Hardware-Elemente wie Mikrocontroller, Sensoren, Aktoren und Kommunikationssystem;
- Funktionen im Zusammenhang mit der Erkennung, Anzeige und Behandlung von Fehlzuständen in der Software selbst (Selbstüberwachung der Software);

ANMERKUNG 1 Dazu gehören sowohl die Selbstüberwachung der Software im Betriebssystem als auch eine anwendungsspezifische Selbstüberwachung der Software zur Erkennung systematischer Fehlzustände in der Anwendungssoftware.

- Funktionen im Zusammenhang mit den Online- und Offline-Prüfungen der Sicherheitsfunktionen;

ANMERKUNG 2 Eine Selbstprüfung kann während des Betriebs und beim Hochfahren der Einheit durchgeführt werden.

ANMERKUNG 3 Dies bezieht sich besonders auf die Prüfbarkeit der Sicherheitsfunktionen beim Kundendienst oder durch andere E/E-Systeme.

- Funktionen, die es ermöglichen, dass Modifikationen an der Software während der Produktion und der Wartung sicher durchgeführt werden können;
- Funktionen, die sich auf das Betriebsverhalten und die Reaktionszeit beziehen.

Die Spezifikation der Software-Sicherheitsanforderungen muss aus dem Konzept der technischen Sicherheit und dem Systemdesign abgeleitet werden und Folgendes berücksichtigen:

- a) die festgelegten System- und Hardware-Konfigurationen;
- b) die Hardware-Software-Schnittstellenspezifikation;
- c) die entsprechenden Anforderungen der Hardware-Designspezifikation;
- d) die Einschränkungen des Zeitablaufs;

BEISPIEL 1 Ausführungs- und Reaktionszeit, die aus der erforderlichen Ansprechzeit auf der Systemebene abgeleitet werden.

- e) die externen Schnittstellen; und

BEISPIEL 2 Kommunikations- und Benutzerschnittstellen.

- f) jede Betriebsart des Systems oder der Hardware, die sich auf die Software auswirkt.

BEISPIEL 3 Betriebsarten von Hardware-Einrichtungen können die Voreinstellung, Initialisierung, Prüfung oder erweiterte Betriebsarten umfassen.

Die Spezifikation der Software-Sicherheitsanforderungen muss nach [Tabelle 13](#) erfolgen.

Tabelle 13 – Spezifikation der Software-Sicherheitsanforderungen

Verfahren		H-SIL			
		A	B	C	D
1	Anforderungsspezifikation in natürlicher Sprache	++	++	++	++
2a	Nichtformale Notationen für die Anforderungsspezifikation	++	++	+	+
2b	Semiformale Notationen für die Anforderungsspezifikation	+	+	++	++
2c	Formale Notationen für die Anforderungsspezifikation	+	+	+	+
3	Rechnerunterstützte Spezifikationswerkzeuge	+	+	++	++

8.2.4.2 Hardware-Software-Schnittstellenspezifikation

Die in 6.3.5 eingeleitete Hardware-Software-Schnittstellenspezifikation muss so weit aufgeschlüsselt werden, dass die einwandfreie Steuerung und Nutzung der Hardware möglich ist, und sie muss alle sicherheitsbezogenen Abhängigkeiten zwischen Hardware und Software beschreiben.

8.2.4.3 Verifizierung der Software-Sicherheitsanforderungen

Die Software-Sicherheitsanforderungen und die präzisierten Anforderungen an die Hardware-Software-Schnittstelle müssen nach IEC 63168-4:20XX, Abschnitt 11, verifiziert werden, um Folgendes nachzuweisen:

- Übereinstimmung und Vereinbarkeit mit den Anforderungen an die technische Sicherheit;
- Übereinstimmung mit dem Systemdesign; und
- Übereinstimmung mit der Hardware-Software-Schnittstelle.

8.2.5 Arbeitsergebnisse

- a) Spezifikation der Software-Sicherheitsanforderungen nach 8.2.4.1.
- b) Hardware-Software-Schnittstellenspezifikation (präzisiert) nach 8.2.4.2.
- c) System-Verifizierungsplan (präzisiert) nach 8.2.4.3.
- d) Software-Verifizierungsbericht nach 8.2.4.3.

8.3 Software-Architekturdesign

8.3.1 Zweck des Software-Architekturdesigns

Das erste Ziel dieser Unterphase ist die Entwicklung eines Software-Architekturdesigns, das die Software-Sicherheitsanforderungen umsetzt.

Das zweite Ziel dieser Unterphase ist der Nachweis des Software-Architekturdesigns.

8.3.2 Allgemeines

Das Software-Architekturdesign stellt alle Software-Komponenten und ihre Interaktionen in einer hierarchischen Struktur dar. Es werden sowohl statische Aspekte, wie Schnittstellen und Datenpfade zwischen allen Software-Komponenten, als auch dynamische Aspekte, wie Prozessabläufe und Zeitverhalten, beschrieben.

Um eine Software-Architektur zu entwickeln, müssen alle sicherheitsbezogenen und nicht sicherheitsbezogenen Software-Anforderungen gut umgesetzt werden. Folglich werden in dieser Unterphase sicherheitsbezogene und nicht sicherheitsbezogene Anforderungen in einem Entwicklungsprozess behandelt.

8.3.3 Für das Software-Architekturdesign erforderliche Informationen

Die folgenden Informationen müssen zur Verfügung gestellt werden:

- Sicherheitsplan (präzisiert) in Übereinstimmung mit 8.1.5;
- Hardware-Software-Schnittstellenspezifikation in Übereinstimmung mit 8.2.5;
- Spezifikation der Software-Sicherheitsanforderungen in Übereinstimmung mit 8.2.5;
- Software-Verifizierungsplan (präzisiert) in Übereinstimmung mit 8.2.5; und
- Software-Verifizierungsbericht in Übereinstimmung mit 8.2.5.

Die folgenden Informationen können berücksichtigt werden:

- Konzept der technischen Sicherheit in Übereinstimmung mit 6.3.5;
- Systementwurfsspezifikation in Übereinstimmung mit 6.3.5;
- verfügbare qualifizierte Software-Komponenten; und
- Anwendungsleitfäden für Verfahren (von einer externen Quelle).

8.3.4 Anforderungen und Empfehlungen

8.3.4.1 Software-Architektur und -Designmethoden

Das Software-Architekturdesign muss die hierarchische Struktur aller sicherheitsbezogenen Software-Komponenten auf der Grundlage der Software-Sicherheitsanforderungen unter folgenden Aspekten beschreiben:

- a) die statischen Designaspekte der Software-Komponenten, und
- b) die dynamischen Designaspekte der Software-Komponenten.

ANMERKUNG Auf der obersten Ebene der Software-Architektur erfolgt in der Regel eine Trennung in Basissoftware und Anwendungssoftware.

Das Software-Architekturdesign muss nach [Tabelle 14](#) entwickelt werden.

Tabelle 14 – Verfahren für das Software-Architekturdesign

Verfahren		H-SIL			
		A	B	C	D
1	Designmethode				
1.1a	Nichtformale Notationen	++	++	+	+
1.1b	Semiformale Notationen	+	++	++	++
1.1c	Formale Notationen	+	+	+	+
1.2	Rechnerunterstützte Spezifikationswerkzeuge	+	+	++	++
2	Designsprinzipien				
2.1	Hierarchische Struktur der Software-Komponenten	++	++	++	++
2.2	Begrenzte Größe von Software-Komponenten	++	++	++	++
2.3	Begrenzte Größe von Schnittstellen	+	+	+	+
2.4	Hohe Kohäsion innerhalb jeder Software-Komponente	+	++	++	++
2.5	Begrenzte Kopplung zwischen den Software-Komponenten	+	++	++	++
2.6	Geeignete Ablaufplanungseigenschaften	++	++	++	++

Verfahren		H-SIL			
		A	B	C	D
2.7	Beschränkte Verwendung von Interrupts	+	+	+	++
3	Sicherheitsanalyse				
3.1	Bottom-up-Ausfallanalyse	+	+	++	++
3.2	Top-down-Ausfallanalyse	+	+	+	++

Die ausgewählten Entwurfsverfahren müssen Merkmale aufweisen, die die folgenden Eigenschaften unterstützen:

- a) Abstraktion, Modularität, Kapselung und andere Eigenschaften, die die Komplexität beherrschbar machen,
- b) die Beschreibung von
 - Funktionalität,
 - Informationsfluss zwischen den Komponenten,
 - Prozesssteuerung und die Informationen hinsichtlich der Zeit,
 - zeitlichen Beschränkungen,
 - gleichzeitigen Prozessen, falls zutreffend,
 - Datenstrukturen und deren Eigenschaften, und
 - Annahmen im Entwurf und ihre Abhängigkeiten,
- c) das Verständnis der Entwickler und anderer Beteiligter,
- d) Fähigkeit zur Modifikation der Software, und
- e) Verifizierung und Validierung.

Die hierarchische Struktur der Software-Architektur muss mit den Software-Einheiten auf der untersten Ebene enden.

Bei der Entwicklung der Software-Architektur muss der Umfang der sicherheitsbezogenen Komponenten so gering wie möglich gehalten werden.

Die Software-Sicherheitsanforderungen müssen den Software-Komponenten zugeordnet werden. Folglich muss jede Software-Komponente so entwickelt werden, dass sie den höchsten H-SIL aller ihr zugeordneten Anforderungen erfüllt.

Wenn die eingebettete Software Software-Komponenten mit unterschiedlichen H-SIL oder sicherheitsbezogene und nicht sicherheitsbezogene Software-Komponenten implementieren muss, ist der Gesamt-H-SIL auf die implementierte Komponente mit dem niedrigsten H-SIL beschränkt, sofern nicht eine angemessene Unabhängigkeit zwischen den Software-Komponenten nachgewiesen werden kann.

8.3.4.2 Verifizierung der Software-Architektur

Das Software-Architekturdesign muss nach IEC 63168-4:20XX, Abschnitt 11, und unter Verwendung der in [Tabelle 15](#) aufgeführten Verifizierungsverfahren für das Software-Architekturdesignverifiziert werden, um die folgenden Eigenschaften nachzuweisen:

- a) Übereinstimmung mit den Software-Sicherheitsanforderungen;
- b) Übereinstimmung mit der Ziel-Hardware; und
- c) Einhaltung der Entwurfsleitlinien.

Tabelle 15 – Verfahren für den Verifizierung des Software-Architekturdesigns

Verfahren		H-SIL			
		A	B	C	D
1a	Walk-through des Entwurfs ^a	++	+	o	o
1b	Inspektion des Designs ^a	+	++	++	++
1c	Simulation der dynamischen Teile des Designs ^b	+	+	+	++
1d	Prototypenherstellung	o	o	+	++
1e	Formale Verifizierung	o	o	+	+
1f	Kontrollflussanalyse ^c	+	+	++	++
1g	Datenflussanalyse ^c	+	+	++	++
^a Im Fall einer modellgestützten Entwicklung können diese Verfahren für das Modell angewendet werden.					
^b Verfahren 1c erfordert die Verwendung von ausführbaren Modellen für die dynamischen Teile der Software-Architektur.					
^c Die Steuerfluss- und Datenflussanalyse kann auf sicherheitsbezogene Komponenten und ihre Schnittstellen beschränkt werden.					

8.3.5 Arbeitsergebnisse

- a) Spezifikation des Software-Architekturdesign nach 8.3.4.1; und
- b) Software-Verifizierungsbericht (präzisiert) nach 8.3.4.2.

8.4 Design und Implementierung von Software-Einheiten

8.4.1 Zweck des Designs und der Implementierung von Software-Einheiten

Das erste Ziel dieser Unterphase ist die Festlegung der Software-Einheiten in Übereinstimmung mit dem Software-Architekturdesign und den zugehörigen Software-Sicherheitsanforderungen.

Das zweite Ziel dieser Unterphase ist die Implementierung der Software-Einheiten, wie festgelegt.

Das dritte Ziel dieser Unterphase ist die statische Verifizierung des Designs der Software-Einheiten und ihrer Implementierung.

8.4.2 Allgemeines

Auf der Grundlage des Software-Architekturentwurfs wird der detaillierte Entwurf der Software-Einheiten entwickelt. Der detaillierte Entwurf wird als Modell oder direkt als Quellcode implementiert, in Übereinstimmung mit dem Modellierungs- bzw. Codierungsleitfaden. Der detaillierte Entwurf und die Implementierung werden statisch verifiziert, bevor mit der Prüfphase der Software-Einheit begonnen wird. Die implementierungsbezogenen Eigenschaften sind bei manueller Code-Entwicklung auf der Quellcode-Ebene erreichbar. Bei der modellgestützten Entwicklung mit automatischer Codegenerierung gelten diese Eigenschaften für das Modell und müssen nicht für den Quellcode angewendet werden.

Bei der Entwicklung eines einzigen Entwurfs einer Software-Einheit werden sowohl die Software-Sicherheitsanforderungen als auch alle nicht sicherheitsbezogenen Anforderungen umgesetzt. Folglich werden in dieser Unterphase sicherheitsbezogene und nicht sicherheitsbezogene Anforderungen in einem Entwicklungsprozess behandelt.