

**DIN IEC 62566-2
(VDE 0491-3-9)**
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 27.120.20

Einsprüche bis 2017-11-08

Entwurf

**Kernkraftwerke – Leittechnik für Systeme mit sicherheitstechnischer Bedeutung –
Entwicklung HDL-programmierter integrierter Schaltkreise –
Teil 2: HDL-programmierte integrierte Schaltkreise für Systeme, die Funktionen der Kategorie B oder C ausführen
(IEC 45A/1155/CD:2017)**

Nuclear power plants – Instrumentation and control systems important to safety –
Development of HDL-programmed integrated circuits –
Part 2: HDL-programmed integrated circuits for systems performing category B or C functions
(IEC 45A/1155/CD:2017)

Centrales nucléaires de puissance – Instrumentation et contrôle-commande importants pour la sûreté –
Développement des circuits intégrés programmés en HDL –
Circuits intégrés programmés en HDL pour les systèmes réalisant des fonctions de catégorie B ou C
(IEC 45A/1155/CD:2017)

Anwendungswarnvermerk

Dieser Norm-Entwurf mit Erscheinungsdatum 2017-09-08 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 des DIN unter www.entwuerfe.din.de 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/stellungnahme oder für Stellungnahmen zu Norm-Entwürfen der DKE unter www.dke.de/stellungnahme abgerufen werden;
- oder in Papierform an die DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE, Stresemannallee 15, 60596 Frankfurt am Main.

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

Gesamtumfang 97 Seiten

DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE

Anwendungsbeginn

Anwendungsbeginn dieser Norm ist

Inhalt	Seite
Nationales Vorwort.....	5
Einleitung	6
1 Anwendungsbereich	9
1.1 Allgemeines	9
1.2 Anwendung dieser Norm	9
2 Normative Verweisungen	9
3 Begriffe	10
4 Abkürzungen	13
5 Allgemeine Anforderungen für HDP-Projekte.....	14
5.1 Allgemeines	14
5.2 Lebenszyklus	14
5.3 Abstufungsprinzipien	16
5.4 HPD-Qualitätssicherung	17
5.5 Konfigurationsmanagement	18
5.6 HPD-Verifizierung	18
6 HPD-Anforderungsspezifikation	19
6.1 Allgemeines	19
6.2 Funktionale Aspekte der Anforderungsspezifikation	20
6.3 Fehlerentdeckung und Fehlertoleranz.....	21
6.4 Anforderungserfassung unter Benutzung von ESL-Werkzeugen	21
6.4.1 Allgemeines	21
6.4.2 Anforderungen an den Formalismus von Werkzeugen, die auf ESL-Ebene verwendet werden.....	21
7 Annahmeverfahren für programmierbare integrierte Schaltkreise, interne Blöcke und vor-entwickelte Blöcke	22
7.1 Allgemeines	22
7.2 Annahmeprozess für programmierbare integrierte Schaltkreise und eingeschlossene native Blöcke	22
7.2.1 Allgemeines	22
7.2.2 IC-Eignungsanalyse	23
7.2.3 Annahme nativer Blöcke in gewähltem IC	23
7.2.4 Dokumentation der IC-Annahme.....	24
7.3 Annahmeprozess für PDBs	24
7.3.1 Allgemeines	24
7.3.2 Funktionale Eignung von PDBs.....	25
7.3.3 Dokumentation zur Sicherheit von PDBs	25

7.3.4	Nachweis der Korrektheit von PDBs in Hinblick auf die Sicherheitsdokumentation.....	26
7.3.5	Ergänzende Prüfungen	28
7.3.6	Verwendungsregeln	28
7.3.7	Änderung für die Annahme	28
7.3.8	Änderung nach der Annahme	29
7.3.9	Dokumentation der PDB-Annahme.....	29
8	HPD-Auslegung und -Realisierung	29
8.1	Allgemeines.....	29
8.2	Hardware-Beschreibungssprachen (HDL) und zugehörige Werkzeuge.....	29
8.3	Auslegung	30
8.3.1	Allgemeines.....	30
8.3.2	Fehlerentdeckung	31
8.3.3	Sprach- und Kodierungsregeln	32
8.3.4	Synchrone vs. asynchrone Auslegung.....	33
8.3.5	Management der Energieversorgung	33
8.3.6	Dokumentation der Auslegung.....	33
8.4	Realisierung	34
8.4.1	Allgemeines.....	34
8.4.2	Produkte	34
8.4.3	Dateien von Parametern und Beschränkungen	34
8.4.4	Durch Werkzeuge eingebrachte oder entfernte Redundanzen	34
8.4.5	Zustandsmaschinen	35
8.4.6	Statische Zeitanalyse	35
8.4.7	Dokumentation der Realisierung.....	35
8.5	Werkzeuge auf Systemebene und automatische Codeerzeugung.....	36
9	Integration und Validierung der HPD	36
9.1	Allgemeines.....	36
9.2	Prüfumgebungen für die funktionale Simulation der HPD	37
9.3	Testabdeckung.....	37
9.4	Prüfungsdurchführung.....	38
10	HPD-Aspekte der Systemintegration	38
10.1	Allgemeines.....	38
10.2	Anforderungen.....	38
11	HPD-Aspekte der Systemvalidierung	39
11.1	Allgemeines.....	39
11.2	Anforderungen.....	39
12	Änderungen.....	40
12.1	Änderung der Anforderungen, Auslegung oder Realisierung	40
12.2	Änderung der mikroelektronischen Technologie.....	41

	Seite
13 HPD-Produktion.....	42
13.1 Allgemeines	42
13.2 Produktionsprüfungen	42
13.3 Programmierungsdateien und -tätigkeiten	42
14 HPD-Aspekte von Installation, Abnahme und Betrieb.....	42
14.1 Allgemeines	42
14.2 Anomalieberichte.....	43
15 Softwarewerkzeuge für die Entwicklung von HPDs	43
15.1 Allgemeines	43
15.2 Zusätzliche Anforderungen für Werkzeuge zur Auslegung, Implementierung und Simulation.....	45
16 Segmentierung oder Aufteilung der Auslegung	45
16.1 Hintergrund.....	45
16.2 Hilfs- oder Unterstützungsfunktionen	45
16.2.1 Allgemeines	45
16.2.2 Segmentierung von Hilfs- und Unterstützungsfunktionen oder Funktionen einer untergeordneten Sicherheitskategorie	46
17 Maßnahmen gegen Versagen aufgrund gemeinsamer Ursache (CCF)	46
Anhang A (informativ) Elektronische Systemebene	47
Bilder	
Bild 1 – System-Lebenszyklus (informativ, wie in IEC 61513 definiert)	14
Bild 2 – HPD-Lebenszyklus	15
Bild 3 – Empfohlener Auswahl- und Annahmeprozess für blanke integrierte Schaltkreise und eingeschlossene native Blöcke	23
Bild 4 – Empfohlener Auswahl- und Annahmeprozess für PDBs.....	24

Nationales Vorwort

Das internationale Dokument IEC 45A/1155/CD:2017 „Nuclear power plants – Instrumentation and control systems important to safety – Development of HDL-programmed integrated circuits – Part 2: HDL-programmed integrated circuits for systems performing category B or C functions“ (CD, en: Committee Draft) ist unverändert in diesen Norm-Entwurf übernommen worden. Dieser Norm-Entwurf enthält eine noch nicht autorisierte deutsche Übersetzung.

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

Das internationale Dokument wurde vom SC 45A „Instrumentation, control and electrical systems of nuclear facilities“ der Internationalen Elektrotechnischen Kommission (IEC) erarbeitet und den nationalen Komitees zur Stellungnahme vorgelegt.

Da der Abstimmungszeitraum für einen FDIS (en: Final Draft International Standard) bzw. Schluss-Entwurf prEN nur 2 Monate beträgt, und dann keine sachlichen Stellungnahmen mehr abgegeben werden können, sondern nur noch eine „JA/NEIN“-Entscheidung möglich ist, wobei eine „NEIN“-Entscheidung fundiert begründet werden muss, wird bereits der CD als DIN-Norm-Entwurf veröffentlicht, um die Stellungnahmen aus der Öffentlichkeit frühzeitig berücksichtigen zu können.

Für dieses Dokument ist das nationale Arbeitsgremium UK 967.1 „Elektro- und Leittechnik für kerntechnische Anlagen“ der DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE (www.dke.de) zuständig.

Für den Fall einer undatierten Verweisung im normativen Text (Verweisung auf ein Dokument ohne Angabe des Ausgabedatums und ohne Hinweis auf eine Abschnichtsnummer, 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. ISO [und/oder] IEC sind nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren.

**Kernkraftwerke –
Leittechnik für Systeme mit sicherheitstechnischer Bedeutung –
Entwicklung HDL-programmierter integrierter Schaltkreise –
Teil 2: HDL-programmierte integrierte Schaltkreise für Systeme, die Funktionen
der Kategorie B oder C ausführen**

Einleitung

a) Technischer Hintergrund, hauptsächliche Inhalte und Organisation der Norm

Die in Kernkraftwerken verwendeten elektronischen Systeme der Klassen 2 und 3 nach IEC 61513, benötigen eine vollständige Validierung und Qualifizierung entsprechend ihrer Sicherheitsklasse. Diese Internationale Norm enthält Anforderungen für die Entwicklung HDL-programmierter Gerätschaften (HPDs) der Klassen 2 und 3, die Funktionen der Klassen B oder C nach IEC 61226 ausführen. Sie ergänzt IEC 62566-1^{N1)}, in der Anforderungen zur Entwicklung von HPDs für Kategorie-A-Funktionen bereitgestellt werden.

In traditionellen rechnerbasierten Systemen kann ein Trennstrich zwischen Hardware- und Softwareteilen gezogen werden. Die Hardware ist hauptsächlich aus standardisierten Komponenten mit vordefinierten elektronischen Funktionen wie Mikroprozessoren, Timer oder Netzwerk-Controllern aufgebaut, wogegen die Software zur Koordinierung der verschiedenen Hardwareteile und zur Realisierung von Anwendungsfunktionen eingesetzt wird.

Heute können bei der Leittechnikauslegung Anwendungsfunktionen direkt in einen integrierten Schaltkreis eingebaut werden, indem man FPGAs oder ähnliche Technologien verwendet. Die Funktion eines solchen integrierten Schaltkreises wird nicht von dem Lieferanten der physikalischen Komponente oder der mikroelektronischen Technologie festgelegt, sondern vom Entwickler der Leittechnik.

Die in dieser Norm speziell angesprochenen integrierten Schaltkreise

- 1) basieren auf vor-entwickelten mikroelektronischen Ressourcen,
- 2) sind in einem Leittechnikprojekt entwickelt,
- 3) sind mit Hardware-Beschreibungssprachen (HDL) und zugehörigen Werkzeugen, die zur Realisierung der Anforderungen in einer geeigneten Anordnung der vor-entwickelten mikroelektronischen Ressourcen verwendet werden, entwickelt.

Daher werden diese Schaltkreise „HDL-programmierte Schaltkreise“ (HPD) genannt. Die HDL-Festlegungen, die einen HPD beschreiben, können die unmittelbare Verwendung von vorgefertigten Blöcken (PDB) mit einschließen, die typischerweise in Bibliotheken, Makros oder intelligenten Kernen vorgehalten werden.

HPDs können eine effektive Lösung zur Realisierung von erforderlichen Funktionen in einem leittechnischen Projekt sein. Jedoch können Verifizierung und Validierung durch Punkte wie große Anzahl interner Pfade und begrenzter Beobachtbarkeit eingeschränkt sein, wenn bei der Entwicklung des HPD seine Verifizierbarkeit nicht mitbedacht wurde.

Um die hohe Zuverlässigkeit zu erreichen, die für Geräte der Sicherheitsleittechnik gefordert wird, muss die Entwicklung der HPDs strikten prozesstechnischen und technischen Anforderungen, so wie sie in dieser Norm zur Verfügung gestellt werden, entsprechen, und zwar einschließlich Anforderungsspezifikation, Auswahl der integrierten Schaltkreise und PDBs, Auslegung und Realisierung, Verifizierung und Prozeduren für Betrieb und Instandhaltung.

Diese Norm ist zur Verwendung für die Hardwareauslegung, für Kernkraftwerksbetreiber (EVUs) und Genehmigungsbehörden vorgesehen. Mit der Genehmigung befasste Institutionen finden Anleitungen zur Bewertung wichtiger Aspekte betreffend Auslegung, Realisierung, Verifizierung und Validierung von HPDs.

^{N1)} Nationale Fußnote: Zurzeit veröffentlicht als IEC 62566.

b) Einordnung der vorliegenden Norm in die Struktur der Normen des IEC/SC 45A

Das Eingangsdokument zu den Normen des IEC/SC 45A ist die **IEC 61513**. Sie enthält Anleitungen zur Leittechnik auf Systemebene und wird ergänzt durch Anleitungen für Hardware (**IEC 60987**) und Software (**IEC 60880** und **IEC 62138**) sowie HPD (IEC 62566-1 und IEC 62566-2). **IEC 62340** enthält Anforderungen zur Reduzierung und Vermeidung von CCF (en: common cause failure) bei Funktionen der Kategorie A.

Die vorliegende Norm ist ein IEC-SC45A-Dokument der zweiten Ebene, das sich auf die Aktivitäten bei der Entwicklung von HPDs für Funktionen der Kategorien B oder C konzentriert. Hinsichtlich HPDs für Kategorie-B-Funktionen ergänzt sie **IEC 60987**, die sich mit generischen Fragen der Hardwareauslegung rechnerbasierter Systeme befasst.

c) Empfehlungen und Einschränkungen der Anwendung der Norm

Es ist wichtig, darauf hinzuweisen, dass in dieser Norm keine zusätzlichen funktionalen Anforderungen für Sicherheitssysteme definiert werden.

Im Hinblick auf folgende Aspekte wurden spezielle Anforderungen und Empfehlungen erarbeitet:

- 1) Eine Vorgehensweise zur Spezifikation von Anforderungen für Auslegung, Realisierung und Verifizierung von „HDL-programmierten Schaltkreisen“ (HPD, 3.9) und Behandlung der zugehörigen Aspekte der Systemintegration und Validierung;
- 2) eine Vorgehensweise zu Analyse und Auswahl integrierter Schaltkreise, mikroelektronischer Technologien und vor-entwickelter Blöcke (PDB, 3.13), die zur Entwicklung von HPDs verwendet werden;
- 3) Prozeduren zur Änderungs- und Konfigurationskontrolle von HPDs;
- 4) Anforderungen zu Auswahl und Verwendung von Softwarewerkzeugen für die Entwicklung von HPDs.

Es ist zu berücksichtigen, dass sich die digitale Technologie nach wie vor rasch entwickelt und dass es in einer Norm wie dieser nicht möglich ist, Verweisungen auf alle modernen Entwicklungstechniken mit einzuschließen.

Um sicherzustellen, dass die Norm über längere Zeit unverändert gültig bleibt, wurde der Schwerpunkt auf Prinzipien und nicht auf spezielle Technologien gelegt. Wenn neu entwickelte Techniken zur Verfügung stehen, sollte es möglich sein, ihre Eignung durch die in dieser Norm enthaltenen Sicherheitsprinzipien zu beurteilen.

d) Beschreibung der Struktur der Normen des IEC/SC 45A und der Beziehungen zu weiteren Dokumenten der IEC sowie Dokumenten anderer Organisationen (IAEA, ISO)

IEC 61513 stellt das Eingangsdokument zu den Normen des IEC/SC 45A dar. Sie enthält allgemeine Anforderungen an die leittechnischen Systeme und Geräte, die zur Ausführung sicherheitstechnisch wichtiger Funktionen in Kernkraftwerken genutzt werden. IEC 63046 enthält allgemeine Anforderungen für Stromversorgungssysteme in Kernkraftwerken; sie deckt die elektrische Energieversorgung einschließlich der Versorgungssysteme für die Leittechnik ab. **IEC 61513** und IEC 63046 sind zusammengehörend auf gleicher Ebene zu betrachten. Durch **IEC 61513** und IEC 63046 werden die Normen des IEC/SC 45A strukturiert und ein komplettes Rahmenwerk für allgemeine Anforderungen zu leittechnischen und elektrischen Systemen in Kernkraftwerken geschaffen.

In **IEC 61513** und IEC 63046 wird direkt auf andere Normen des IEC/SC 45A verwiesen, die allgemeine Themen behandeln, wie die Kategorisierung von Funktionen und die Klassifizierung von Systemen, Qualifizierung, Trennung, Maßnahmen gegen Versagen aufgrund gemeinsamer Ursache, Wartenauslegung, Elektromagnetische Verträglichkeit, Cybersicherheit, Software- und Hardwareaspekte programmierbarer digitaler Systeme, Koordinierung von Anforderungen zur Sicherheit und zur IT-Security sowie Änderungsmanagement. Die Normen, auf die direkt verwiesen wird, bilden die zweite Ebene und sollten zusammen mit **IEC 61513** und IEC 63046 als ein in sich konsistenter Satz von Dokumenten betrachtet werden.

Die dritte Ebene bilden Normen des IEC/SC 45A, auf die in **IEC 61513** oder IEC 63046 nicht direkt verwiesen wird. Diese Normen behandeln spezielles Gerät, technische Methoden oder spezifische Aktivitäten. Sie beziehen sich hinsichtlich der allgemeinen Themen auf die Dokumente der zweiten Ebene, können jedoch im Allgemeinen für sich allein benutzt werden.

Eine vierte Ebene erweitert die Normen des IEC/SC 45A um Technische Berichte, die nicht normativ sind.

In den Normen des IEC/SC 45A werden die Prinzipien und grundsätzlichen Aspekte der Sicherheit und IT-Security in den einschlägigen IAEA Safety Standards und den entsprechenden Dokumenten der IAEA Nuclear Security Series (NSS) umgesetzt: Dies umfasst speziell die Requirements SSR-2/1 betreffend Sicherheitsanforderungen für die Auslegung von Kernkraftwerken, den Safety Guide SSG-30 bezüglich der Sicherheitsklassifizierung von Strukturen, Systemen und Komponenten in Kernkraftwerken, SSG-39 betreffend die Auslegung der Leittechnik in Kernkraftwerken, SSG-34 betreffend die Auslegung der Stromversorgung in Kernkraftwerken und die Implementierungsleitlinie NSS 17 für IT-Security von Rechnern in nuklearen Einrichtungen. Terminologie und Definitionen in den Normen des IEC/SC 45A stimmen mit den von der IAEA verwendeten überein.

Für IEC 61513 und IEC 63046 wird ein Darstellungsformat verwendet, das dem der grundlegenden Sicherheitsnorm IEC 61508 ähnlich ist, mit einem Sicherheits-Lebenszyklus als Gesamtrahmen und zusätzlich einem System-Lebenszyklus. Mit IEC 61513 und IEC 63046 werden die allgemeinen Anforderungen von IEC 61508-1, IEC 61508-2 und IEC 61508-4, für die Anwendung auf dem nuklearen Sektor umgesetzt. In diesem Rahmen entsprechen IEC 60880, IEC 62138 und IEC 62566 für den nuklearen Sektor der IEC 61508-3. IEC 61513 und IEC 63046 beziehen sich bei Themen der Qualitätssicherung (QS) sowohl auf ISO als auch auf IAEA GS-R Part 2 und IAEA GS-G-3.1 und IAEA GS-G-3.5.

Auf Ebene 2 ist in Hinblick auf IT-Sicherheit IEC 62645 das Eingangsdokument für die IEC/SC45A-IT-Sicherheitsstandards. Es baut auf die übergeordneten Prinzipien und Hauptkonzepte der generischen IT-Sicherheitsstandards auf, insbesondere auf ISO/IEC 27001 und ISO/IEC 27002; es adaptiert sie und vervollständigt sie, um in den nuklearen Kontext zu passen, und koordiniert sie mit IEC 62443.

Auf Ebene 2 ist in Hinblick auf Warten IEC 60964 das Eingangsdokument für die IEC/SC45A-Wartennormen, und IEC 62342 ist das Eingangsdokument für die IEC-SC45A-Normen zum Alterungsmanagement.

ANMERKUNG 1 Es wird angenommen, dass für die Auslegung von leittechnischen Systemen in Kernkraftwerken, die konventionelle Sicherheitsfunktionen enthalten (z. B. in Bezug auf Arbeitssicherheit, Schutz von Vermögenswerten, chemische und prozesstechnische Gefährdungen), internationale und nationale Normen angewendet werden.

ANMERKUNG 2 Der Scope des IEC/SC 45A wurde 2013 erweitert, um auch elektrische Systeme abzudecken. In den Jahren 2014 und 2015 wurde in SC 45A diskutiert, wie und wo allgemeine Anforderungen für die Auslegung behandelt werden sollten. Die Experten des SC 45A empfahlen, eine selbständigen Norm auf derselben Ebene wie IEC 61513 zu entwickeln und allgemeine Anforderungen für elektrische Systeme zu erstellen. Dazu wurde jetzt das Projekt IEC 63046 begonnen. Sobald IEC 63046 veröffentlicht wird, verliert diese Anmerkung 2 der allgemeinen Einleitung für die Normen des IEC/SC 45A ihre Gültigkeit.

1 Anwendungsbereich

1.1 Allgemeines

In dieser Internationalen Norm werden Anforderungen für hochzuverlässige „HDL-programmierte Baugruppen“ (HPD) für die Verwendung in leittechnischen Systemen von Kernkraftwerken, die Funktionen der Kategorien B oder C nach IEC 61226 ausführen, zur Verfügung gestellt.

Die Programmierung von HPDs beruht auf Hardware-Beschreibungssprachen (HDL) und zugehörigen Softwarewerkzeugen. HPDs basieren typischerweise auf feldprogrammierbaren logischen Gattern (FPGAs) oder ähnlichen mikroelektronischen Technologien (programmierbare logische Baugruppen (PLD), komplexe programmierbare Baugruppen (CPLD), programmierbare Array-Logik (PAL) usw.). Universelle integrierte Schaltkreise für allgemeine Anwendungen (wie Mikroprozessoren) sind keine HPDs.

Diese Norm enthält Anforderungen betreffend

- a) eines fest zugeordneten HPD-Lebenszyklus, in dem jede Phase der HPD-Entwicklung angesprochen wird, die Planung, Spezifikation der Anforderungen, Auslegung, Realisierung, Integration und Validierung sowie die Verifizierungsarbeiten im Zusammenhang mit jeder Phase;
- b) Planung und ergänzende Tätigkeiten wie Änderungen und Produktion;
- c) Auswahl vor-entwickelter Komponenten. Diese umfasst mikroelektronische Ressourcen, vor-entwickelte Blöcke (PDB);
- d) Werkzeuge für Auslegung, Realisierung und Verifizierung von HPDs.

Diese Norm enthält keine Anforderungen zur Entwicklung der mikroelektronischen Ressourcen, die gewöhnlich kommerziell verfügbar sind und nicht unter nuklearen Qualitätssicherungsstandards entwickelt werden. Sie spricht vielmehr die Entwicklungen an, die mit diesen mikroelektronischen Ressourcen in einem leittechnischen Projekt mit HDLs und zugehörigen Werkzeugen getätigt werden.

Diese Norm enthält Anleitungen, wie latente Fehler in HPDs so weit wie möglich vermieden werden können, und sich so die Empfindlichkeit für Einzelfehler und mögliche CCF verringert.

Zuverlässigkeitsaspekte in Bezug auf Qualifizierung hinsichtlich Umgebungsbedingungen und Versagen aufgrund Alterung oder physikalischer Abnutzung werden hier nicht behandelt. In anderen Normen wie IEC 60987, IEC/IEEE 60780-323 und IEC 62342 werden diese Themen angesprochen.

In dieser Norm werden Aspekte der Cybersicherheit für Leittechnik nicht behandelt. IEC 62645 enthält Anforderungen zur IT-Sicherheit für programmierbare digitale leittechnische Systeme.

1.2 Anwendung dieser Norm

Diese Norm enthält Anleitungen und Anforderungen für verifizierbare HPD-Auslegungen und -Realisierungen, die Nachweise erforderlich machen, z. B. hinsichtlich der Sicherheitsbedeutung ihrer Funktion oder ihres Verhaltens. Diese Norm beschreibt die Tätigkeiten zur Entwicklung von HPDs, die im Rahmen eines fest zugeordneten Lebenszyklus organisiert sind. Sie beschreibt auch Tätigkeiten und gibt Anleitungen, die zusätzlich zu den Anforderungen in IEC 61513 für Systemintegration und -validierung bei Verwendung von HPDs zu benutzen sind^{N2)}.

2 Normative Verweisungen

Liste der Normen siehe englisches Original

^{N2)} Nationale Fußnote: Anforderungen der IEC 60987, die sich auf die Entwicklung programmierbarer logischer Einrichtungen beziehen, sind zusätzlich zu jenen in der vorliegenden Norm anwendbar, wenn HPDs in den leittechnischen Systemen der Klasse 1 enthalten sind.

3 Begriffe

Für die Anwendung dieser Norm gelten folgende Begriffe

3.1

anwendungsorientierte Sprache

(en: application-oriented language)

Rechnersprache, speziell entwickelt für ein bestimmtes Anwendungsgebiet und zur Verwendung für Personen, die Spezialisten auf diesem Anwendungsgebiet sind

Anmerkung 1 zum Begriff: Geräte-Plattformen bevorzugen gewöhnlich anwendungsorientierte Sprachen mit leicht zu nutzenden Fähigkeiten für die Anpassung des Geräts an spezifische Anforderungen.

Anmerkung 2 zum Begriff: Anwendungsorientierte Sprachen können verwendet werden, um funktionale Anforderungen eines leittechnischen Systems zu spezifizieren und/oder Anwendungssoftware zu spezifizieren oder zu entwickeln. Sie können auf Texten oder/und Graphiken basieren.

Anmerkung 3 zum Begriff: Z. B. Sprachen basierend auf Funktionsblock-Diagrammen, Sprachen definiert nach IEC 61131-3.

Anmerkung 4 zum Begriff: Siehe auch allgemeine Sprache (3.7)

[QUELLE: IEC 60880, 3.3]

3.2

anwendungsspezifischer integrierter Schaltkreis

ASIC

(en: Application Specific Integrated Circuit)

integrierter Schaltkreis, der für spezifische Anwendungen ausgelegt ist

[QUELLE: IEC 521-11-18]

Anmerkung 1 zum Begriff: Spezieller integrierter Schaltkreis, der für die von einer Firma spezifizierten Zwecke ausgelegt wurde. Er realisiert also von dieser Firma vorab definierte Funktionen.

3.3

Block

(en: block)

einer der Teile, aus denen eine Auslegung besteht; ein Block kann in weitere Blöcke unterteilt sein

Anmerkung 1 zum Begriff: Ein Block ist entweder ein vor-entwickelter Block oder ein nativer Block oder ein im Rahmen des in Rede stehenden Projekts entwickelter Block.

[QUELLE: IEC 62566-1, 3.2]

3.4

Versagen/Ausfall aufgrund gemeinsamer Ursache

CCF

(en: Common Cause Failure)

Versagen von zwei oder mehr Strukturen, Systemen oder Komponenten infolge eines einzigen spezifischen Ereignisses oder Grundes

[QUELLE: IEA Safety Glossary: 2016]

Anmerkung 1 zum Begriff: Gemeinsame Ursachen können innerhalb oder außerhalb eines leittechnischen Systems liegen.

3.5

Elektroniksystemebene

ESL

(en: Electronic System Level)

Beschreibung eines elektronischen Systems, basierend auf einem Satz von Prozessen, die für die Funktionalität von Komponenten wie Mikroprozessoren, Speichern, speziellen Recheneinheiten oder Kommunikationskanälen repräsentativ sind

Anmerkung 1 zum Begriff: Diese Beschreibung erlaubt es, im Zuge der Auslegung das System in Komponenten zu zerlegen, um ihre Leistungsfähigkeit bei unterschiedlicher Abbildung der Funktionen auf die Komponenten zu beurteilen und die Anforderungen an die Komponenten zu formulieren.

Sie wird üblicherweise mit Sprachen wie C++, SystemC (IEEE 1666), SystemVerilog (IEEE 1800) oder Matlab (R) durchgeführt.

[QUELLE: IEC 62566-1, 3.4]

3.6

feldprogrammierbares logisches Gatter

FPGA

(en: Field Programmable Gate Array)

integrierter Schaltkreis, der vom Hersteller der Leittechnik vor Ort programmiert werden kann. Er umfasst programmierbare Logik-Blöcke (kombinatorisch und sequentiell), programmierbare Verbindungen zwischen den Blöcken und programmierbare Blöcke für Eingänge und/oder Ausgänge. Die Funktion wird dann bei der Auslegung der Leittechnik festgelegt, nicht vom Lieferanten des Schaltkreises.

[QUELLE: IEC 62566-1, 3.4]

Anmerkung 1 zum Begriff: Während FPGAs im Grunde digitale Einrichtungen sind, können sie auch analoge Eingänge/Ausgänge und A/D-Wandler enthalten. FPGAs können fortschrittliche digitale Funktionen wie Hardware-Multiplier, zugeordnete Speicher und eingebettete Prozessorkerne mit einschließen.

3.7

allgemeine Sprache

(en: general-purpose language)

Rechnersprache, ausgelegt für jede Verwendungsart

Anmerkung 1 zum Begriff: Die Systemsoftware von Geräte-Plattformen wird gewöhnlich unter Verwendung allgemeiner Sprachen realisiert.

Anmerkung 2 zum Begriff: Beispiele sind Ada, C, Pascal.

Anmerkung 3 zum Begriff: Siehe auch anwendungsorientierte Sprache.

[QUELLE: IEC 60880, 3.20]

3.8

Hardware-Beschreibungssprache

HDL

(en: Hardware Description Language)

Sprache, die dazu verwendet wird, die Funktionen und/oder die Struktur einer elektronischen Komponente für Dokumentation, Simulation oder Synthese formal zu beschreiben

Anmerkung 1 zum Begriff: Die verbreitetsten HDLs sind VHDL (IEEE 1076) und Verilog (IEEE 1364).

[QUELLE: IEC 62556-1, 3.6]

3.9

HDL-programmierte Baugruppe

HPD

(en: HDL-programmed device)

integrierter Schaltkreis, der (für leittechnische Systeme in Kernkraftwerken) unter Verwendung von Hardware-Beschreibungssprachen und zugehörigen Softwarewerkzeugen konfiguriert wird.

Anmerkung 1 zum Begriff: HDLs und zugehörige Werkzeuge (z. B. Simulatoren, Synthesizer) werden verwendet, um die Anforderungen in eine geeignete Anordnung von vor-entwickelten mikroelektronischen Ressourcen zu implementieren.

Anmerkung 2 zum Begriff: Bei der Entwicklung von HPDs können vor-entwickelte Blöcke verwendet werden.

Anmerkung 3 zum Begriff: HPDs basieren typischerweise auf blanken FPGAs, PLDs oder ähnlichen programmierbaren integrierten Schaltkreisen.

Anmerkung 4 zum Begriff: HPD ist eine Art einer programmierbaren Baugruppe.

[QUELLE: IEC 62566-1, 3.7]

3.10

Modul

(en: module)

eines der Teile, aus denen eine Auslegung besteht; ein Modul kann in andere Module unterteilt werden

Anmerkung 1 zum Begriff: „Modul“ ist ein Synonym für „Block“. „Block“ wird oft im Zusammenhang mit elektronischen Auslegungen verwendet.

[QUELLE: IEC 62566-1, 3.8]

3.11

nativer Block

(en: native block)

Block, der eine bereits bestehende Ressource in einem integrierten Schaltkreis darstellt, z. B. ein Odergatter oder komplexere Blöcke wie Multiplizierer oder Controller für serielle Übertragungen. Durch Programmieren des HPD werden die nativen Blöcke konfiguriert und verbunden, um die gewünschte Funktion zu erzielen.

[QUELLE: IEC 62566-1, 3.9]

3.12

Netzliste

(en: netlist)

Beschreibung einer elektronischen Komponente in Form der Verbindungen zwischen ihren End-Elementen (z. B. native Blöcke).

[QUELLE: IEC 62566-1, 3.10]

3.13

vor-entwickelter Block

PDB

(en: Pre-Developed Block)

vor-entwickelter Funktionsblock, der in einer HDL-Beschreibung verwendbar ist

Anmerkung 1 zum Begriff: PDBs werden typischerweise als Bibliotheken, Makros oder eigentumsgeschützte Kerne zur Verfügung gestellt. Sie werden bei der Entwicklung einer HPD verwendet und in diese HPD integriert.

Anmerkung 2 zum Begriff: Ein PDB kann vor der Integration in eine HPD erheblichen Arbeitsaufwand verursachen, z. B. Synthese eines elektronischen Schaltkreises aus den HDL-Statements, Abbilden der nominalen Komponenten dieses Schaltkreises auf die Hardwarestrukturen des physikalischen Schaltkreises und Aufbau der Verbindungen.

[QUELLE: IEC 62566-1, 3.11]

3.14

programmierbare logische Baugruppe

PLD

(en: Programmable Logic Device)

integrierter Schaltkreis, der aus logischen Elementen mit einer Verbindungsstruktur besteht, von denen ein Teil vom Anwender programmierbar ist

Anmerkung 1 zum Begriff: Es gibt unterschiedliche PLD-Arten, z. B. löschbare PLD oder komplexe PLD (CPLD).

Anmerkung 2 zum Begriff: Der Unterschied zwischen FPGA und PLD ist nicht gut definiert, aber PLD bezieht sich gewöhnlich auf eine einfachere Baugruppe als FPGA.

[QUELLE: IEC 62566-1, 3.13]

3.15

Register-Transferebene

RTL

(en: Register Transfer Level)

synchrones Parallel-Modell eines elektronischen Schaltkreises, das dessen Verhalten mittels logisch kombinierten und zwischen Registern im Zeittakt transferierten Signalen beschreibt. Das RTL-Modell wird üblicherweise in HDL geschrieben oder aus einem HDL-Quellcode erzeugt.

[QUELLE: IEC 62566-1, 3.14]

3.16^{N3)}

nachträgliche Erläuterung

(en: back-annotation)

aufgrund von Erkenntnissen in späteren Auslegungsphasen in frühere Auslegungsphasen einzubringende zusätzliche Erläuterungen

4 Abkürzungen^{N4)}

Abkürzung	Englisch	Deutsch
ASIC	Application Specific Integrated Circuit	anwendungsspezifischer integrierter Schaltkreis
CCF	Common Cause Failure	Versagen (Ausfall) aufgrund gemeinsamer Ursache
CPLD	Complex Programmable Logic Device	komplexe programmierbare logische Baugruppe
ESL	Electronic System Level	Elektroniksystemebene
FPGA	Field Programmable Gate Array	feldprogrammierbare logische Gatter
HDL	Hardware Description Language	Hardware-Beschreibungssprache
HPD	HDL-Programmed Device	HDL-programmierte Baugruppe
IC	Integrated Circuit	integrierter Schaltkreis
IP	Intellectual Property	geistiges Eigentum
PAL	Programmable Array Logic	programmierbare Array Logik
PDB	Pre-Developed Block	vor-entwickelter Block
PDS	Pre-Developed Software	vor-entwickelte Software
PLD	Programmable Logic Device	programmierbare logische Baugruppe
RAM	Random Access Memory	RAM-Speicher, Speicher mit direktem Zugriff
RoHS	Restriction of Hazardous Substances	Beschränkung gefährlicher Substanzen
RTL	Register Transfer Level	Register-Transferebene
SEU	Single Event Upset	SEU ^{N5)}
SRAM	Static RAM	statisches RAM
STA	Static Timing Analysis	statische Zeitanalyse
VHDL	Very High Speed Integrated Circuit Hardware Description Language	Hardware-Beschreibungssprache VHDL

^{N3)} Nationale Fußnote: Im IEC-Entwurf nicht enthaltene Definition, zur Verdeutlichung in der deutschen Übersetzung ergänzt.

^{N4)} Nationale Fußnote: Abkürzungen für die deutschen Bezeichnungen wurden nicht eingeführt. Im Normtext werden die in der Praxis gebräuchlichen englischen Abkürzungen verwendet, in einigen Fällen auch im Deutschen gebräuchliche englische Fachausdrücke übernommen.

^{N5)} Nationale Fußnote: Zustandsänderung eines empfindlichen Knotens in einer mikroelektronischen Baugruppe aufgrund eines „Schlags“ durch Ionen oder elektromagnetischer Strahlung, die zu einem sogenannten weichen Fehler (soft error) am Ausgang der Baugruppe führt.

5 Allgemeine Anforderungen für HDP-Projekte

5.1 Allgemeines

In diesem Abschnitt werden zunächst die HPDs innerhalb des in IEC 61513 beschriebenen leittechnischen Systems festgestellt. Dann wird der HPD-Entwicklungs-Lebenszyklus beschrieben, der das HPD-Projekt strukturiert.

Schließlich stellt er Anforderungen an HPD-Projekte bezüglich Qualitätssicherung und Konfigurationsmanagement. Da sich diese Fragestellungen (für HPD-Projekte) nicht von denen eines Softwareentwicklungsprozesses unterscheiden, sind die Anforderungen durch Verweise auf die relevanten Abschnitte der IEC 60880 definiert, gegebenenfalls ergänzt um HPD-spezifische Anforderungen.

Unter Verweis auf Abschnitt 1 ist die Entwicklung mikroelektronischer Technologien oder blanker integrierter Schaltkreise vom Anwendungsbereich dieser Norm ausgeschlossen. Deshalb sind Begriffe wie „HPD-Entwicklung“, „HPD-Lebenszyklus“, „HPD-Auslegung“ oder „HPD-Verifikation“ darauf bezogen, was innerhalb eines Leittechnikprojektes, beginnend mit diesen Technologien oder blanken integrierten Schaltkreisen, getan wird, um den spezifischen integrierten Schaltkreis für die Verwendung in dem Leittechnikprojekt herzustellen.

5.2 Lebenszyklus

Der Produktionsprozess leittechnischer Systeme für die Verwendung in Kernkraftwerken ist in IEC 61513 behandelt; dort wird das Konzept des System-Lebenszyklus eingeführt. Dieser ist ein Mittel zur Kontrolle des Entwicklungsprozesses, dessen Verwendung auch zu der notwendigen Evidenz führen sollte, den korrekten Betrieb von Sicherheitssystemen zu rechtfertigen. Der System-Sicherheitslebenszyklus enthält Anforderungen an die zu benutzenden Projektdispositionen zur Produktion von Systemen, ohne diese jedoch zu diktieren (siehe Bild 1).

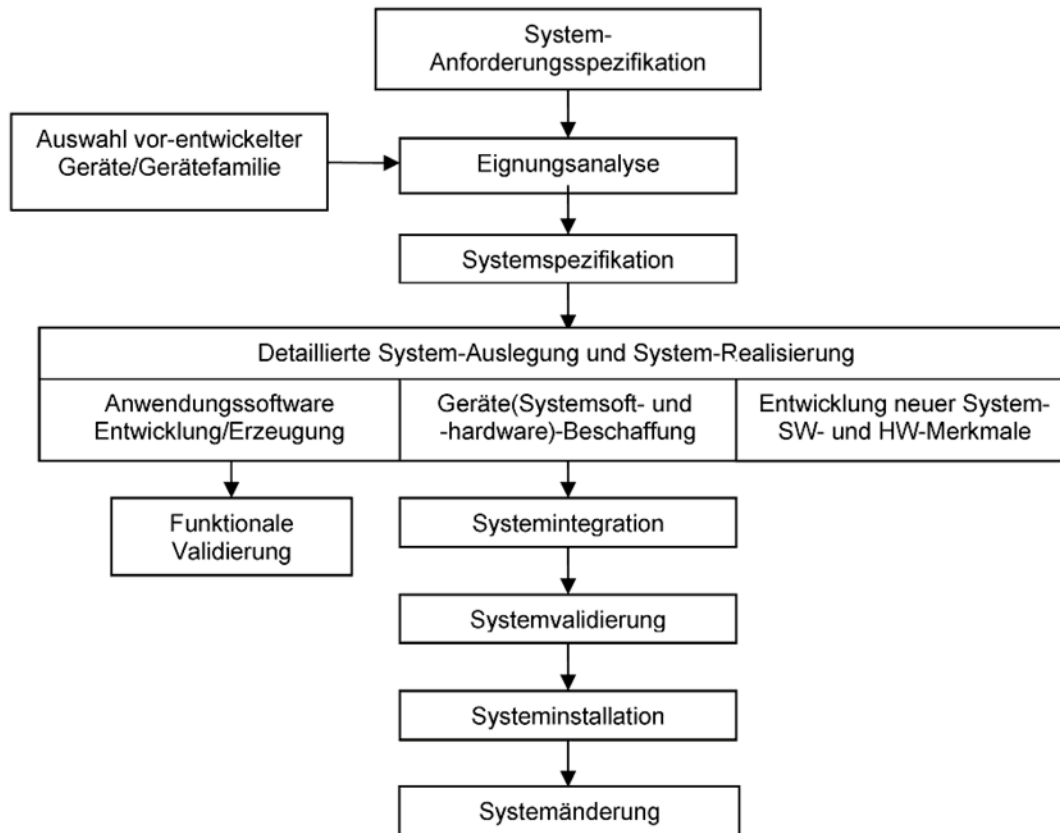


Bild 1 – System-Lebenszyklus (informativ, wie in IEC 61513 definiert)

Der System-Lebenszyklus von IEC 61513 wird in IEC 60880 (für Funktionen der Kategorie A) und in IEC 62138 (für Funktionen der Kategorien B und C) für Softwareentwicklung, in IEC 62566-1 (für Funktionen der Kategorie A) und in IEC 62566-2 (für Funktionen der Kategorien B und C) für die HPD-Entwicklung, und in IEC 60987 für die Hardwareentwicklung von rechnerbasierten Systemen der Klassen 1 und 2 ergänzt.

HPDs werden mit Rechnerwerkzeugen erstellt, die auf eine strukturierte Entwicklung nach einem Lebenszyklus abzielen, der Tätigkeiten zur Erfassung der Anforderungen, Auslegung und Realisierung, Integration und Validierung zusammen mit Nachweis- und Prüftätigkeiten umfasst.

Die in Bild 1 gezeigten Systemauslegungs- und -realisierungsphasen von IEC 61513, speziell die „Gerätebeschaffung (Systemsoftware und Hardware)“ und „Entwicklung von neuen Systemsoftware- und Hardwareeigenschaften“, sind wesentliche Teile des System-Lebenszyklus. Diese Phasen sind in Bild 2 noch erweitert, um in größerem Detail die Phasen zwischen der Anforderungsspezifikation und der Validierung von HPDs-Systemkomponenten darzustellen.

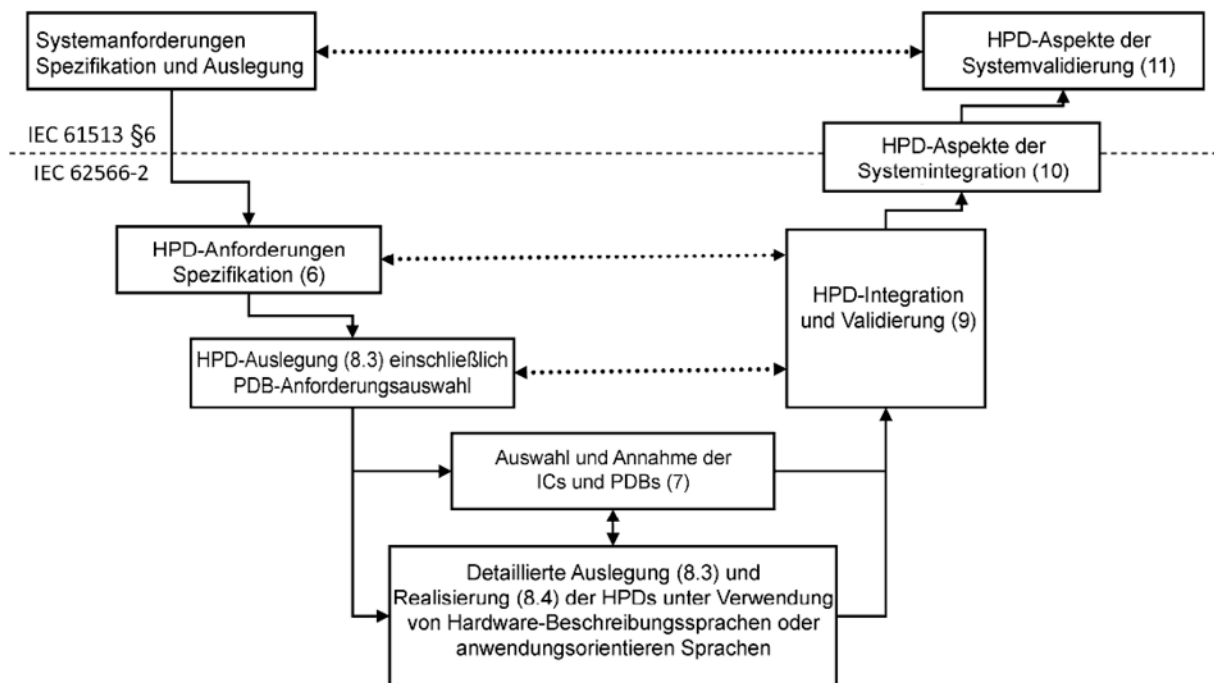


Bild 2 – HPD-Lebenszyklus^{N6)}

Bei der Auslegung werden im Allgemeinen vor-entwickelte Baugruppen wie programmierbare blanke integrierte Schaltkreise oder vor-entwickelte Blöcke (PDB) verwendet, um speziell für die Notwendigkeiten des Projekts zugeschnittene Hardware zu bauen. Die mit der Auswahl vor-entwickelter Baugruppen verbundenen Tätigkeiten werden in Abschnitt 7 angesprochen; sie können parallel mit den ersten Phasen des in Bild 2 gezeigten HPD-Lebenszyklus ausgeführt werden, vorausgesetzt, alle Abhängigkeiten sind formal behandelt und dokumentiert.

Der Lebenszyklus in Bild 2 zeigt den Entwicklungs-Lebenszyklus einer HPD, der parallel mit den anderen in Bild 1 gezeigten Komponenten (Software oder Hardware) des Systems durchgeführt werden kann, wobei schließlich alle diese Aktivitäten in den Integrations- und Validierungsphasen des Systemlebenszyklus zusammenlaufen.

Die vorgeschlagene Vorgehensweise zur Entwicklung basiert auf dem traditionellen „V-Zyklus“-Modell, wie auch diese Vorgehensweise in anderen Normen gezeigt wird und sie in IAEA SSG-39 empfohlen ist, erlaubt aber notwendige Adjustierungen in Hinblick darauf, dass einige Entwicklungsphasen mit Hilfe von Werkzeugen automatisch ablaufen können und die Entwicklung iterativ sein kann.

^{N6)} Nationale Fußnote: „Auslegung“ bedeutet „Auslegung des Inhalts“.

Oft gibt es keine klare Trennung und gut definierte Grenzen zwischen der Integration einer gegebenen Komponente und der Systemintegration. Daher wird in dieser Norm die Integration einer HPD als Teil der Systemintegration betrachtet. Ähnlich ist ihre Validierung Teil der Systemvalidierung.

Abhängig von der durch die HPD realisierten Funktion kann das zu betrachtende System oder Teilsystem reichen:

- a) von dem leittechnischen System, wenn mit der HPD die Logik einer Sicherheitsfunktion realisiert wird
- b) bis zu einem elektronischen Modul oder Schrank, wenn er eine Funktion realisiert (innerhalb des Moduls oder Schanks), die nicht in der Lage ist, die Ausgänge irgendeiner Sicherheitsfunktion im weiteren System zu beeinflussen, und wenn dies durch eine geeignete Analyse nachgewiesen wird.

Vom Standpunkt der Sicherheit ist die Situation gewöhnlich dann am kritischsten, wenn durch die HPD direkt die Logik einer Sicherheitsfunktion realisiert wird.

Folgende Tätigkeiten unterstützen den Entwicklungsprozess einer HPD:

- 1) Qualitätssicherung und Qualitätskontrolle (5.4),
- 2) Konfigurationsmanagement (5.5),
- 3) Verifizierung (5.6).

Des Weiteren gibt es Tätigkeiten, welche die Auswahl von Werkzeugen zur Unterstützung der Entwicklung (Abschnitt 15), das Herstellen der Dokumentation und die Änderung (Abschnitt 12) betreffen.

5.3 Abstufungsprinzipien

Entsprechend der Abstufung der Sicherheitsrelevanz für Funktionen der Kategorien A, B und C (siehe IEC 61226) wird eine Abstufung der für HPDs von leittechnischen Systemen der Klassen 1, 2 und 3 anwendbaren Anforderungen vorgenommen.

Die Anwendung der Anforderungen dieser Norm auf HPDs der Sicherheitsklasse 3 folgt dem grundsätzlichen Vertrauensniveau, das für HPDs eines als sicherheitstechnisch wichtig identifizierten leittechnischen Systems geeignet ist. Es gelten folgende Prinzipien:

- Verlässlichkeit der Qualitätssicherung;
- Achtsamkeit für die Sicherstellung, dass die HPD
 - soweit notwendig zu den sicherheitstechnisch wichtigen Funktionen beiträgt und sich auf diese nicht ungünstig auswirkt,
 - die Ausführungen der HPD-Anforderungsspezifikation erfüllt, die sicherheitstechnisch wichtige Randbedingungen definieren.
- Sicherstellung, dass die Operateure des leittechnischen Systems so früh wie möglich über HPD-Fehler und -Ausfälle, die sich auf sicherheitstechnisch wichtige Funktionen auswirken können, informiert werden, sodass geeignete Maßnahmen ergriffen werden können;
- dokumentierte HPD-Anforderungsspezifikationen, -Auslegungsspezifikationen, -Integrationsplan, -Prüfplan (d. h. Simulation, Funktionsprüfung), Plan zu HPD-Aspekten der Systemvalidierung und Änderungsspezifikationen.

Für HPDs der Sicherheitsklasse 2 gelten zusätzlich zu den o. g. Prinzipien für HPDs der Klasse 3 folgende in dieser Norm festgelegte Prinzipien:

- auf Prüfungen und Auslegung basierender Nachweis, dass die erforderliche sicherheitsbezogene Leistungsfähigkeit (z. B. Reaktionszeiten) unter allen spezifizierten Bedingungen eingehalten wird;
- strengere Anforderungen für die Auswahl von vor-entwickelten und nativen Blöcken;
- strengere Anforderungen für funktionale Validierung;
- strengere Anforderungen für Verifizierung, Auswahl und Verwendung von HPD-Entwicklungswerkzeugen und -sprachen;

- explizite Anforderungen für Einfachheit, Klarheit, Präzision, Verifizierbarkeit, Prüfbarkeit und Modifizierbarkeit.

Wenn die gleiche Anforderung auf beide Sicherheitsklassen anwendbar ist, kann das Ausmaß des Erfüllungsnachweises von der Sicherheitsklasse abhängen.

5.4 HPD-Qualitätssicherung

IEC 61513:2011, 6.3.2.1 enthält allgemeine Anforderungen zur Qualitätssicherung auf der Ebene eines leittechnischen Systems. In folgenden Ausführungen werden zusätzliche Anforderungen behandelt, die entweder für HPDs spezifisch oder von besonderer Bedeutung sind.

5.4.1 Die Entwicklung der HPDs muss nach einem HPD-Lebenszyklus erfolgen. Die Bereitstellung dieses HPD-Lebenszyklus muss in einem Qualitätssicherungsplan (QS-Plan) spezifiziert werden.

Dieser QS-Plan kann Teil eines System-QS-Plans oder ein separater HPD-QS-Plan sein.

5.4.2 Wenn ein separater HPD-QS-Plan verwendet wird, muss er mit dem System-QS-Plan konsistent sein. Die anwendbaren Anforderungen von **IEC 61513, 6.3.2** müssen in beiden Plänen berücksichtigt werden.

5.4.3 Der QS-Plan muss die Entwicklungsphasen des HPD-Lebenszyklus in spezifizierte Tätigkeiten unterteilen. Diese müssen die zur Erzielung der geforderten HPD-Qualität notwendigen Aktivitäten sowie die Verifizierungstätigkeiten umfassen, um die objektive Evidenz bereitzustellen, dass diese Qualität erreicht wird.

5.4.4 Die Spezifikation einer Tätigkeit muss beinhalten:

- a) ihre Ziele;
- b) ihre Beziehungen und ihr Zusammenwirken mit anderen Tätigkeiten;
- c) ihre Eingänge und Ergebnisse;
- d) die für sie relevante Organisation und Verantwortlichkeit;
- e) die zugehörigen Verifizierungsaktivitäten entsprechend **5.6** dieser Norm.

5.4.5 Erforderliche Inhalte und Eigenschaften der Eingänge und Ergebnisse sollten ebenso spezifiziert werden.

5.4.6 Der QS-Plan muss fordern, dass die Realisierung jeder Tätigkeit kompetenten Personen zugeordnet wird, die mit entsprechenden Ressourcen ausgestattet sind.

5.4.7 Der QS-Plan muss fordern, dass Änderungen in genehmigten Dokumenten von autorisierten Personen festgestellt, überprüft und genehmigt werden.

5.4.8 Der QS-Plan muss fordern, dass die verwendeten Methoden, Sprachen, Werkzeuge, Regeln und Standards festgestellt und dokumentiert sind, den betroffenen Personen bekannt sind und von ihnen beherrscht werden.

5.4.9 Der QS-Plan muss fordern, dass bei Verwendung mehrerer Methoden, Sprachen, Werkzeuge, Regeln und/oder Standards klar gemacht wird, welche für jede Aktivität zu benutzen sind.

5.4.10 Der QS-Plan muss fordern, dass die benutzten projektspezifischen Ausdrücke, Abkürzungen und Konventionen expliziert definieren werden.

5.4.11 Der QS-Plan muss fordern, dass auftretende Fragen und Probleme verfolgt und gelöst werden.

5.4.12 Der QS-Plan muss fordern, dass Aufzeichnungen von seiner Anwendung hergestellt werden. Insbesondere ist zu fordern, dass die Resultate von Verifizierungen und Überprüfungen zusammen mit den

Zielen der Verifizierungen und Überprüfungen, den Schlussfolgerungen und den vereinbarten Lösungen aufgezeichnet werden.

5.4.13 Der QS-Plan muss fordern, dass die Ergebnisdokumentation eine Reihe von untereinander konsistenten Dokumenten bildet, in denen wechselseitig aufeinander Bezug genommen wird, um so die Rückverfolgbarkeit von der endgültigen Auslegung zu den ursprünglichen Anforderungen sicherzustellen.

5.5 Konfigurationsmanagement

In IEC 61513, 6.3.2.3 sind Anforderungen für das Konfigurationsmanagement auf leittechnischer Ebene enthalten. Im Folgenden werden zusätzlich Anforderungen behandelt, die für HPDS spezifisch oder von besonderer Bedeutung sind.

5.5.1 Das Konfigurationsmanagement für HPDs muss entsprechend den Angaben eines Konfigurationsmanagementplans oder des QS-Plans durchgeführt werden. Diese müssen mit den Vorkehrungen für das Konfigurationsmanagement der Systemebene übereinstimmen.

5.5.2 Das Konfigurationsmanagement muss folgende Punkte dokumentieren:

- a) Dokumentation der im Projekt entwickelten Module (Blöcke) sowie der PDBs;
- b) Angaben zur Identifizierung der integrierten Schaltkreise;
- c) Rechnerdateien, die zur Simulation, Verifizierung und Produktion verwendet werden,
- d) Parameter, die für automatisierte Tätigkeiten der Softwarewerkzeuge verwendet werden (siehe Abschnitt 15), wie z. B. „optimiertes Timing“, „optimierte Dichte“ für die Platzierungs- und Routingtätigkeit;
- e) Identifizierung der Versionen aller Softwarewerkzeuge (siehe Abschnitt 15) einschließlich jedes verwendeten „Software Patch“ sowie allgemeine und technologiespezifische Bibliotheken.
- f) Fehlerangaben mit Hinweisen auf festgestellte Bugs in Softwarewerkzeugen.

5.5.3 Der Konfigurationsmanagementplan muss technische Mittel für die Authentifizierung der dem Konfigurationsmanagement unterliegenden HPD-Anteile und ihrer Versionen spezifizieren.

5.5.4 Der Konfigurationsmanagementplan muss sicherstellen, dass die einer gegebenen System- oder Geräteversion angefügte HPD-Version, und die Versionen der Anteile, die miteinander die HPD-Version bilden, eindeutig identifiziert werden.

5.6 HPD-Verifizierung

Die als Teil der HPD-Entwicklung unternommenen Verifizierungstätigkeiten können in der Verantwortlichkeit des Leittechniklieferanten liegen und von Mitarbeitern durchgeführt werden, die unabhängig von den für die Entwicklung und Realisierung verantwortlichen Mitarbeitern sind.

5.6.1 Ein Verifizierungsplan muss das Ziel der HPD-Verifizierung und der Überprüfungstätigkeiten beschreiben.

5.6.2 Verifizierung und Überprüfung müssen entsprechend den dokumentierten Vorgaben erfolgen. Insbesondere müssen an Etappen des HPD-Lebenszyklus, die im Verifizierungsplan spezifiziert wurden, die Ergebnisse der im Verifizierungsplan angegebenen Tätigkeiten verifiziert werden, um zu zeigen, dass

- a) die Ergebnisse dem Konfigurationsmanagement unterliegen;
- b) die Tätigkeiten präzise angegebene Eingänge haben und ihre Ergebnisse konsistent mit den Eingängen sind;
- c) die Tätigkeiten ihre spezifizierten Ziele erfüllen, und ihre Ergebnisse die geforderten Inhalte und Eigenschaften aufweisen, und jeder abgestimmten Lösung entsprechen;
- d) die Ergebnisse klar, präzise und aktuell sind;
- e) die Ergebnisse jeder anwendbaren Regel entsprechen;
- f) die Ergebnisse die anwendbaren Anforderungen dieser Norm erfüllen.

„Präzise angegeben“ bedeutet, dass die Version eindeutig bekannt ist. „Klar“ bedeutet, dass der Benutzer eines Dokuments den Inhalt ohne besondere Anstrengung voll verstehen kann, auch wenn er vorher mit dem Projekt nicht befasst war, vorausgesetzt er hat das erforderliche Fachwissen. „Präzise“ bedeutet, dass es keine Zweideutigkeit gibt.

Das Ausmaß der Verifizierungs- und Überprüfungstätigkeiten kann von Umfang und Natur der HPD und den zu verifizierenden oder zu überprüfenden Ergebnissen abhängen, sowie von den verwendeten Methoden und Werkzeugen. Das Ausmaß der Verifizierungs- und Überprüfungstätigkeiten kann für solche Anforderungen eingeschränkter sein, die als unwichtig für die Sicherheit eingestuft werden (siehe 6.2.5) und die sicherheitstechnisch wichtigen Funktionen nicht beeinträchtigen können.

5.6.3 Die Verifizierung von Resultaten einer Aktivität muss durch kompetente Personen erfolgen, die in diese Aktivität nicht involviert waren. Das bedeutet nicht, dass eine Person als Verfasser eines bestimmten Dokuments nicht der Verifizierende eines anderen Dokuments betreffend eine andere Lebenszyklus-Aktivität sein kann.

5.6.4 Die Verifizierung der Resultate einer Aktivität sollte Vertreter der Anwender dieser Resultate mit einschließen, sowie andere Experten, wenn notwendig.

5.6.5 Die HPD-Anforderungsspezifikation, die HPD-Auslegungsspezifikation und der HPD-Validierungsplan müssen verifiziert werden.

5.6.6 Für Klasse 2 muss die Anwendung der Auslegungs- und Realisierungsregeln verifiziert werden.

5.6.7 Für Klasse 3 sollte die Anwendung der Auslegungs- und Realisierungsregeln verifiziert werden.

6 HPD-Anforderungsspezifikation

6.1 Allgemeines

Dieser Abschnitt vervollständigt und präzisiert die Anforderungen von IEC 61513, 6.2.3.4.

6.1.1 In einer HPD-Anforderungsspezifikation müssen die Anforderungen der HPDs entweder im Dokument selbst enthalten oder durch Verweise auf Anforderungen, die auf Teilsystem- oder Systemebene festgelegt wurden (z. B. das zu realisierende funktionale Verhalten), dokumentiert sein.

6.1.2 Die HPD-Anforderungsspezifikation sollte eindeutig, verifizierbar und zielorientiert sein.

6.1.3 Für Klasse 2 sollte die HPD-Anforderungsspezifikation eine Beschreibung der notwendigen zeitlichen Charakteristiken der HPD einschließen.

6.1.4 Wenn die HPD eine Sicherheitsfunktion realisiert, muss ihre Anforderungsspezifikation von den Anforderungen an das leittechnische System, das diese Sicherheitsfunktion enthält, abgeleitet werden und muss Teil der Spezifikation des Teilsystems sein, in dem die HPD verwendet wird.

6.1.5 Die HPD-Anforderungsspezifikation sollte beschreiben, was zu machen ist, und nicht, wie es zu machen ist.

Prinzipiell hat die HPD-Anforderungsspezifikation die Aufgabe, zu spezifizieren, welches Ziel die HPD zu erreichen hat, ohne jedoch festzulegen, wie das zu bewerkstelligen ist. Jedoch mögen Auslegungs- und Realisierungseinschränkungen zu spezifizieren sein, wenn dies Überlegungen bei der Auslegung des leittechnischen Systems oder der leittechnischen Architektur erforderlich machen.

6.1.6 Für Klasse 2 sollten die zur Beschreibung der HPD-Anforderungsspezifikation verwendeten Sprachen und/oder Formate zur Klarheit und Präzision der Darstellung beitragen; sie sollten unter Berücksichtigung jener ausgewählt werden, die für die Eingänge verwendet wurden, und jener, die für Auslegung und Realisierung der HPD gewählt wurden.

Da nicht jedes Spezifikationsformat immer einen klaren, präzisen und verifizierbaren Ausdruck aller Spezifikationsnotwendigkeiten erlaubt, mögen verschiedene und ergänzende Formate in ein und derselben HPD-Anforderungsspezifikation verwendet werden.

6.1.7 Die HPD-Anforderungsspezifikation muss eine Referenz für die HPD-Auslegung, HPD-Aspekte der Systemvalidierung und mögliche HPD-Änderungen sein.

Die HPD-Anforderungsspezifikation kann unmittelbar auf die Eingangsdokumentation verweisen, um so unnötige Doppelungen zu vermeiden und das Risiko von Unstimmigkeiten zu minimieren. Sie kann auch auf andere bereits bestehende Dokumente verweisen, wie etwa die Dokumentation der nativen Blöcke und anderer vor-entwickelter Blöcke.

6.1.8 Die HPD-Anforderungsspezifikation muss ihre Rückverfolgbarkeit zu den Eingangsdokumenten ermöglichen.

6.1.9 Die Verifizierung der HPD-Anforderungsspezifikation sollte ausdrücklich überprüfen, dass diese konsistent und vollständig hinsichtlich aller Eingangsdokumente ist (siehe [Bild 2](#)).

6.1.10 Die in der HPD-Anforderungsspezifikation enthaltenen Verweisungen auf andere Dokumente müssen präzise und eindeutig sein.

6.2 Funktionale Aspekte der Anforderungsspezifikation

Dieser Abschnitt beschreibt den Inhalt der Anforderungsspezifikation, der direkt mit den funktionalen Notwendigkeiten zusammenhängt.

6.2.1 In der Anforderungsspezifikation müssen spezifiziert sein:

- a) Die von der HPD zur Verfügung zu stellenden Funktionen;
- b) die verschiedenen Betriebsarten der HPD und die entsprechenden Übergangsbedingungen, einschließlich Einschalten der Energieversorgung und Initialisierung, und, wenn zweckmäßig, die Definition der sicheren Zustände;
- c) die Schnittstellen der HPD und die Wechselwirkungen mit ihrer Umgebung (den Operateuren und verschiedenen leittechnischen Komponenten), einschließlich der Rollen, Protokolle, Formate, bit-Nummerierung, Bereiche und Beschränkungen der Ein- und Ausgänge;
- d) jegliche HPD-Parameter, die während des Betriebs von Hand geändert werden können, und ihre Rollen;
- e) die HPD-Leistungsfähigkeit, insbesondere auch (wenn zutreffend) die Antwortzeit;
- f) was die HPD nicht machen darf oder vermeiden muss (wenn zutreffend);
- g) die mit Blick auf Korrektheit und Robustheit zu beachtenden Beschränkungen bei der HPD-Auslegung und -Realisierung.

6.2.2 Für Klasse 2 sollte die HPD-Anforderungsspezifikation unnötige Funktionalität und Komplexität der HPD-Auslegung vermeiden.

Im Prinzip ist es vorzuziehen, dass die HPDs nicht mehr Fähigkeiten haben als gefordert, um so die Komplexität zu minimieren. Da jedoch die heutige industrielle Praxis auf der Verwendung vor-entwickelter Komponenten beruht, mag das Vorhandensein nicht erforderlicher Fähigkeiten gerechtfertigt sein.

6.2.3 Die HPD-Anforderungsspezifikation sollte auch die Nutzungsbedingungen beschreiben (z. B. die Abnahmeleistung), insbesondere die für die HPD schwierigsten Umgebungsbedingungen.

Hinsichtlich 6.2.1, 6.2.2 und 6.2.3 können Funktions-, Schnittstellen- und Leistungsfähigkeitsanforderungen von den für die HPD vorgesehenen Betriebsarten, Parameterwerten, Konfigurationsdaten und sonstigen Bedingungen abhängen.

6.2.4 Die HPD-Anforderungsspezifikation sollte die HPD-Qualitätsziele angeben, die für HPD-Auslegung und -Realisierung hinsichtlich Korrektheit und Robustheit zu beachten sind.

6.2.5 Die HPD-Anforderungsspezifikation muss die zu den spezifizierten Funktionen gehörende Sicherheitskategorie und die Anforderungen festlegen.

6.3 Fehlerentdeckung und Fehlertoleranz

6.3.1 Die HPD-Anforderungsspezifikation muss festlegen, welchen Beitrag die HPD zu leisten hat, um sicherzustellen, dass die Operateure rechtzeitig über Fehler oder Ausfälle von Funktionen sicherheitstechnisch wichtiger leittechnischer Systeme informiert werden. Die den Operateuren zur Verfügung gestellte Information muss sie in die Lage versetzen, geeignete Maßnahmen zu ergreifen.

6.3.2 Die HPD-Anforderungsspezifikation muss die Vorgehensweise spezifizieren, die bei Entdeckung von Fehlern oder Ausfällen erforderlich ist. Wenn periodische Tests des leittechnischen Systems gefordert werden, muss die HPD-Anforderungsspezifikation ebenso die Vorgehensweise bei der Durchführung solcher Tests festlegen.

Das kann beispielsweise Einschränkungen einschließen,

- a) um die Fähigkeit der HPD und des leittechnischen Systems zu verbessern, Fehler (etwa durch SEU) zu tolerieren, Fehler und Ausfälle zu entdecken und zu melden, spezielle Betriebsarten anzunehmen und so Ausfälle zu kompensieren;
- b) um Vertrauen zu gewinnen, dass Operateurfehler und Ausfälle anderer Systeme oder Geräte, mit denen die HPD in Wechselwirkung steht oder gemeinsam Ressourcen nutzt, nicht zu unakzeptablen Auswirkungen führen.

6.4 Anforderungserfassung unter Benutzung von ESL-Werkzeugen

6.4.1 Allgemeines

In dieser Norm wird keine spezifische Methode zur Festlegung der HPD-Anforderungen vorgeschrieben. Wenn sie unter Verwendung von Werkzeugen auf der Elektroniksystemebene (ESL, siehe [Anhang A](#)) festgelegt werden, gelten die Anforderungen in 6.4.2 und 6.4.3 für diese Werkzeuge und ihre Nutzung.

Da Sprachen für Anforderungsspezifikationen den Implementierungssprachen ähnlich sein können, mag es im Fall der ESL weniger praktisch sein, 6.1.5 zu erfüllen (Trennung zwischen „was zu machen ist“ (die Anforderung) und „wie es zu machen ist“ (die Auslegung). Es mögen Vorkehrungen notwendig sein, um 6.1.5 zu erfüllen, z. B. Kommentare zur Spezifikation von Eingängen, Ausgängen und Algorithmen.

6.4.2 Anforderungen an den Formalismus von Werkzeugen, die auf ESL-Ebene verwendet werden

6.4.2.1 Wenn die HPD-Anforderungen unter Verwendung eines ESL-Werkzeugs festgelegt werden, ist Folgendes zu beachten:

- a) Dieses Werkzeug muss einen Formalismus mit strenger Semantik und Klarheit anbieten (Standardisierung der Struktur und Präsentation, Modularität, gute Kommentare);
- b) der vom ESL-Werkzeug verwendete Formalismus muss für alle Beteiligten verständlich sein;
- c) wenn das Werkzeug flexible Mechanismen zur Re-Definition von Funktionen und Operateuren anbietet, sollten die aktuellen Eigenschaften jedes gegebenen Elements allen beteiligten Beteiligten klar sein.

6.4.2.2 Die auf ESL-Ebene benutzten Sprachen sollten eine ausreichende Berücksichtigung der Systemarchitektur erlauben, z. B. die Zuordnung von Funktionen zu Komponenten ermöglichen, und alle Auslegungsmerkmale zur Fehlertoleranz unterstützen.

6.4.3 Schnittstellen mit Auslegungswerkzeugen

Die Semantik der für die Formulierung der Anforderungsspezifikation auf ESL-Ebene verwendeten Sprachen kann sich von der Semantik der bei der Auslegung verwendeten HDL-Sprachen unterscheiden. Beispiele von möglicherweise auftretenden Diskrepanzen liegen in der Interpretation von Parallelismus, Management von Overflows oder der Kodierung von Typen und Zustandsmaschinen.

In dieser Norm werden die PDBs in zwei Kategorie unterteilt, Softcore-PDBs und Hardcore-PDBs. Erstere sind PDBs, die von dem Ziel-IC unabhängig sind und in jede HPD-Auslegung integriert werden können, entweder in Form von HDL-Quellcode oder als synthetisierte RTL-Beschreibung. Hardcore-PDBs werden in Form von Hardware mit dem gewählten IC zur Verfügung gestellt und können bei der HPD-Auslegung nicht modifiziert werden.

Da vor-entwickelte Komponenten Merkmale aufweisen können, die für die HPD nicht erforderlich sind, kann die Ausarbeitung spezifischer Anwendungsvorschriften empfohlen werden, um ihre Benutzung auf das Notwendige und Sichere zu beschränken.

Obwohl die Auswahl- und Annahmeprozesse für ICs und PDBs in diesem Abschnitt seriell abgehandelt werden, heißt das nicht, dass Auswahl und Annahme des IC (7.2) vor Auswahl und Annahme der PDBs (7.3) stattfinden müssen. In manchen Fällen kann die notwendige Verwendung einer speziellen PDB die Auswahl der möglichen ICs einschränken. In anderen Fällen kann die notwendige Verwendung eines speziellen IC die Auswahl von PDBs beschränken, die in der HPD-Auslegung einsetzbar sind. Die Auswahl geeigneter ICs und PDBs ist daher in einem iterativen Prozess durchzuführen, beginnend mit der HPD-Anforderungsspezifikation und anfänglichen Auslegungsentscheidungen nach den Anforderungen in 8.3.

IEC 61513, 6.2.3.2 enthält allgemeine Anforderungen für die Auswahl bereits bestehender Komponenten (nicht notwendigerweise HPD-Komponenten). Im Folgenden werden zusätzliche Anforderungen behandelt, die spezifisch oder von besonderer Wichtigkeit für HPDs sind.

7.2 Annahmeprozess für programmierbare integrierte Schaltkreise und eingeschlossene native Blöcke

7.2.1 Allgemeines

Die allgemein empfohlene Vorgehensweise für Auswahl und Annahme von blanken programmierbaren ICs und ihren eingeschlossenen nativen Blöcken ist in Bild 3 angegeben.

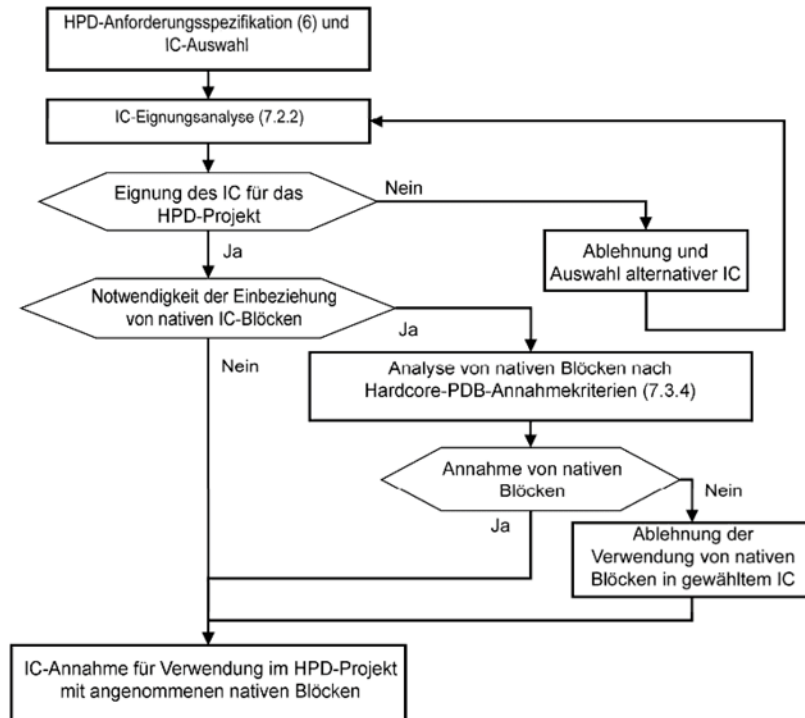


Bild 3 – Empfohlener Auswahl- und Annahmeprozess für blanke integrierte Schaltkreise und eingeschlossene native Blöcke

7.2.2 IC-Eignungsanalyse

7.2.2.1 Der ausgewählte IC muss einer Eignungsanalyse in Hinblick auf die Anforderungen der HPD unterzogen werden

7.2.2.2 Die Eignungsanalyse muss folgende Eigenschaften des ausgewählten IC berücksichtigen:

- IC-Technologie (PAL, CPLD, FPGA usw.);
- Konfigurationstechnologie (antifuse, flash, SRAM usw.);
- Anzahl logischer Elemente und Eignung der internen Architektur;
- Anzahl der Eingangs-/Ausgangspins;
- maximale Betriebsfrequenz;
- Bereich der Betriebstemperatur;
- Herstellungs-Anforderungen (RoHS usw.);
- Hardware-Zuverlässigkeit und Dauer der Beibehaltung einer programmierten Konfiguration;
- Eignung der Entwicklungswerkzeuge hinsichtlich der Anforderungen in [Abschnitt 15](#) dieser Norm.

7.2.2.3 Wenn der ausgewählte IC für die gegebene Anwendung nicht geeignet ist, muss er abgelehnt und eine alternative Lösung gefunden werden.

7.2.3 Annahme nativer Blöcke in gewähltem IC

7.2.3.1 Wenn einer oder mehrere native Blöcke der gewählten IC in der Auslegung des HPD einzusetzen sind, muss jeder davon für die Verwendung nach [7.3](#) angenommen sein.

Die Ablehnung der Verwendung eines nativen Blocks in einem gegebenen IC bedeutet nicht die Ablehnung des IC selbst.

7.2.4 Dokumentation der IC-Annahme

7.2.4.1 Die Eignungsanalyse des gewählten IC und die Annahme der in den gewählten IC eingeschlossenen nativen Blöcken muss dokumentiert werden.

7.3 Annahmeprozess für PDBs

7.3.1 Allgemeines

Die allgemein empfohlene Vorgehensweise für die Auswahl und Annahme von PDBs ist in Bild 4 gezeigt.

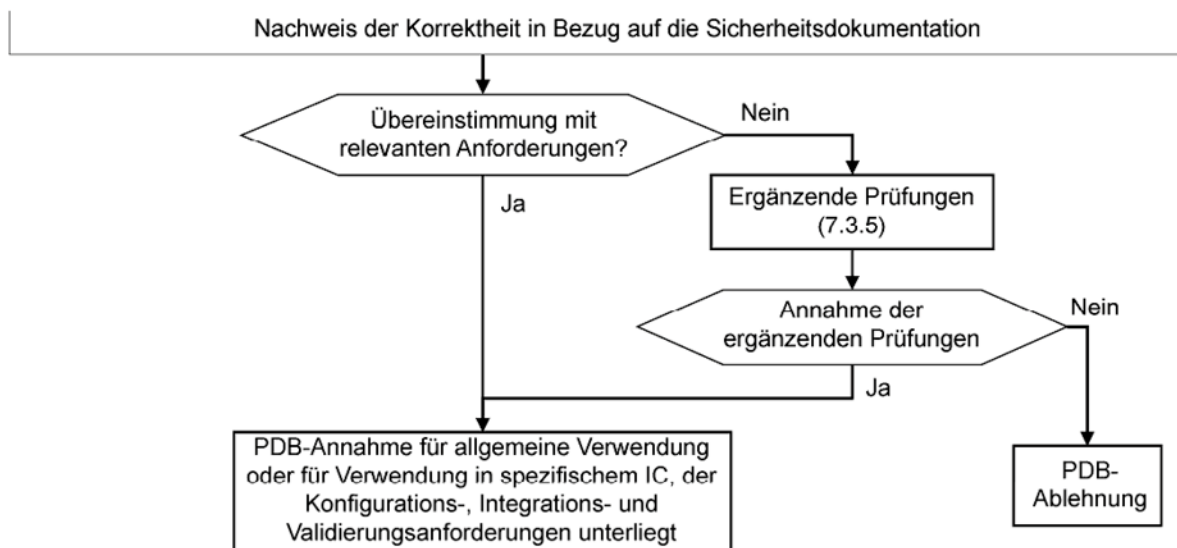


Bild 4 – Empfohlener Auswahl- und Annahmeprozess für PDBs

7.3.2 Funktionale Eignung von PDBs

Das Ziel dieses Abschnitts besteht darin, die Eignung von PDBs hinsichtlich der PDB-Anforderungen sicherzustellen.

7.3.2.1 Die Dokumentation zur Sicherheit von PDBs muss bezüglich der Systemauslegungsspezifikation und der PDB-Anforderungsspezifikation beurteilt werden. Unstimmigkeiten müssen geklärt werden.

7.3.2.2 *Für Klasse 2 sollten die Funktionen festgestellt werden, die zur Unterstützung der PDB-Anforderungsspezifikation nicht notwendig sind. Es sollte eine Begründung dargelegt werden, dass diese Funktionen keine nachteilige Auswirkung auf die Sicherheit haben.*

7.3.3 Dokumentation zur Sicherheit von PDBs

7.3.3.1 Die PDB-Dokumentation muss detailliert zeigen, wie bei der Auslegung die PDBs in Übereinstimmung mit ihren Spezifikationen und Auslegungsscharakteristiken zu verwenden sind.

In dieser Norm wird das entsprechende Dokument (oder der entsprechende Dokumentensatz) Sicherheitsdokumentation genannt. Wenn der PDB Teil eines Geräts oder einer Gerätefamilie ist, kann diese Dokumentation Teil der Sicherheitsdokumentation des Geräts oder der Gerätefamilie sein.

Die Sicherheitsdokumentation umfasst im Allgemeinen mehr als die von der Lieferfirma des PDB zur Verfügung gestellte Benutzerdokumentation. Sie kann beispielsweise Information über die PDB-Auslegung, zusätzliche Tests, Messungen und/oder Analysen und Betriebserfahrung einschließen.

7.3.3.2 Die Sicherheitsdokumentation muss Beschreibungen enthalten von

- a) vorgesehenen Funktionen;
- b) externen Schnittstellen;
- c) Rolle, Typen, Formaten, Bereichen und Beschränkungen der Eingänge und Ausgänge, Ausnahmereingungen, Parametern und Konfigurationsdaten, soweit zutreffend;
- d) verschiedenen Betriebsarten und den entsprechenden Übergangsbedingungen;
- e) jeglichen zu beachtenden Beschränkungen bei der Verwendung des PDB.

7.3.3.3 *Für Klasse 2 sollten, wo anwendbar, diese Beschränkungen*

- 1) *hinreichendes Vertrauen in die Korrektheit des PDB und der Systemauslegung geben;*
- 2) *die Fähigkeit des PDB und des leittechnischen Systems verbessern, einen Ausfall zu entdecken, zu melden und zu tolerieren, spezifizierte Betriebsarten anzunehmen und so den Ausfall zu kompensieren;*
- 3) *hinreichendes Vertrauen geben, dass Operateurfehler und Ausfälle anderer Systeme oder Geräte, mit denen der PDB in Wechselwirkung steht oder Ressourcen teilt, zu definierten Betriebsarten führen;*
- 4) *sicherstellen, dass im PDB-Umfeld alle notwendigen Ressourcen unter allen Verwendungsbedingungen des leittechnischen Systems zur Verfügung stehen.*

7.3.3.4 *Für Klasse 2 sollte, wenn zutreffend, die Sicherheitsdokumentation auch Information zur Leistungsfähigkeit der Funktionen geben (z. B. Antwortzeit).*

Die von der PDB bereitgestellten Funktionen, einschließlich jener bezüglich der Systemschnittstellen, können in Abhängigkeit von den Betriebsbedingungen der Anlage variieren.

7.3.3.5 *Für Klasse 2 muss die Sicherheitsdokumentation auch Information enthalten betreffend*

- *die durchgeführte Selbstüberwachung, die Toleranzfähigkeit und die Ausfallarten;*
- *die Anforderungen des PDB bezüglich der Umgebung (z. B. hinsichtlich Hardware oder anderer HPD-Komponenten);*

- *die Wechselwirkungen und Schnittstellen des PDB mit der Hardware, im notwendigen Maße die volle Beschreibung der sicheren funktionalen Leistungsfähigkeit des Systems.*

7.3.3.6 *Für Klasse 2 muss die Sicherheitsdokumentation des PDB Information bereitstellen, die korrekte Vorhersagen bezüglich der hauptsächlichen sicherheitssignifikanten Elemente der Systemleistungsfähigkeit ermöglicht, vor allem auch der maximalen Antwortzeiten.*

Eine derartige Information kann in Form von Daten, Formeln und/oder Modellen gegeben werden. Wenn die HPD einen großen Bereich von Funktionen, Schnittstellen und Konfigurationsmöglichkeiten anbietet, kann es schwierig werden, ein hinreichendes Vertrauen in die Korrektheit der Information zu erreichen, ohne detailliertes Wissen zur Auslegung und Realisierung des PDB verfügbar zu haben.

7.3.4 Nachweis der Korrektheit von PDBs in Hinblick auf die Sicherheitsdokumentation

7.3.4.1 Allgemeines

7.3.4.1.1 Eine dokumentierte Analyse jedes in der HPD verwendeten PDBs muss zeigen, dass er die ihm zugeordneten Anforderungen erfüllt.

7.3.4.1.2 Es muss ein Nachweis für die Korrektheit der PDBs hinsichtlich ihrer Sicherheitsdokumentation erbracht werden.

7.3.4.1.3 Softcore-PDBs, die in Form einer RTL-Beschreibung bereitgestellt werden, sollten entweder durch Überprüfung der Auslegungsdokumentation (7.3.4.2) oder durch Zertifizierung (7.3.4.4) ausgewählt und bestätigt werden.

7.3.4.1.4 Softcore-PDBs, die in Form synthetisierter RTL bereitgestellt werden, sollten entweder durch Überprüfung der Betriebserfahrung (7.3.4.3) oder durch Zertifizierung (7.3.4.4) ausgewählt und bestätigt werden.

7.3.4.1.5 Hardcore-PDBs sollten entweder durch Überprüfung der Betriebserfahrung (7.3.4.3) oder durch Zertifizierung (7.3.4.4) ausgewählt und bestätigt werden.

7.3.4.1.6 Native Blöcke sollten durch denselben Prozess wie Hardcore-PDBs bestätigt werden.

7.3.4.1.7 Wenn ein vollständiger Nachweis der Korrektheit von PDBs nicht erbracht werden kann, sei es durch eine Überprüfung der Auslegungsdokumentation, Überprüfung der Betriebserfahrung oder Zertifizierung, oder durch eine Kombination dieser Methoden, muss ergänzendes Prüfen nach 7.3.5 dieser Norm erfolgen.

7.3.4.2 Überprüfung der Auslegungsdokumentation

Eine Überprüfung der Auslegungsdokumentation kann verwendet werden, um den Nachweis der Korrektheit von PDBs zu unterstützen, und zwar unter folgenden Bedingungen:

7.3.4.2.1 Die Überprüfung der Auslegungsdokumentation sollte zeigen, dass der PDB den Anforderungen entspricht, die ihm entsprechend der Sicherheitsdokumentation zugewiesen sind.

7.3.4.2.2 *Für Klasse 2 muss die Analyse der Dokumentation zeigen, dass alle in der HPD nicht verwendeten Funktionen und Betriebsarten des vor-entwickelten Blocks die verwendeten nicht beeinträchtigen.*

7.3.4.3 Überprüfung der Betriebserfahrung

Betriebserfahrung kann verwendet werden, um den Nachweis der Korrektheit von PDBs zu unterstützen, und zwar unter folgenden Bedingungen:

7.3.4.3.1 Wenn die Betriebserfahrung benutzt wird, dann

- a) muss die Analyse der Betriebserfahrung zeigen, dass
 - 1) ihr Umfang den Zuverlässigkeitsanforderungen entspricht,
 - 2) sie unter Betriebsbedingungen gewonnen wurde, die jenen des einzusetzenden PDB entsprechen,
 - 3) der tatsächliche Einsatz des PDB in dem Detaillierungsgrad verfolgt wurde, der generell in dieser Norm für die Dokumentation verlangt wird;
- b) *für Klasse 2 müssen die Mittel und Prozeduren zur Erfassung der Betriebserfahrung sicherstellen, dass jeder im analysierten Betrieb aufgetretene PDB-Ausfall so detailliert aufgezeichnet wird, um durch eine technische Analyse soweit wie möglich seine Ursache feststellen zu können;*
- c) *für Klasse 2 müssen Ausfälle, die während des Betriebs des ausgewählten PDB aufgezeichnet wurden, bei der HPD-Auslegung berücksichtigt werden;*
- d) die Betriebserfahrung – und wenn nötig die ergänzenden Tests – müssen zeigen, dass der PDB seine Anforderungen erfüllt;
- e) *für Klasse 2 muss durch eine technische Analyse nachgewiesen werden, dass alle Wechselwirkungen des PDB mit seiner Umgebung in den Wechselwirkungen enthalten sind, die durch die Betriebserfahrung abgedeckt werden;*
- f) *für Klasse 2 muss die in Betracht gezogene Betriebserfahrung genau den festgestellten Versionen des PDB entsprechen, und wenn der PDB speziell zu einem Gerät gehört, der festgestellten Version in diesem Gerät;*
- g) *für Klasse 2 sollte sich die Betriebserfahrung auf die spezielle Version der in der HPD verwendeten vorentwickelten Teile beziehen, anderenfalls muss der Unterschied zwischen den Versionen analysiert und gezeigt werden, dass die Betriebserfahrung für die gewünschte Version relevant ist.*

7.3.4.4 Zertifizierung der PDBs

Die durch Zertifizierung von PDBs erzielte Evidenz kann den Nachweis der Korrektheit von PDBs unter folgenden Bedingungen unterstützen:

7.3.4.4.1 Der für die Zertifizierung der PDBs verwendete Sicherheitsstandard muss den PDB-Entwicklungsprozess explizit ansprechen.

7.3.4.4.2 Die in Betracht gezogene Zertifizierung muss dokumentiert sein.

7.3.4.4.3 Die präzise Identifizierung des zertifizierten PDB muss dokumentiert sein. Wenn sie Teil der Zertifizierung eines größeren Produkts war (z. B. als Teil eines Geräts oder einer Gerätefamilie), muss die genaue Identifizierung dieses Produkts ebenfalls dokumentiert werden.

7.3.4.4.4 Für Klasse 2 muss die Evidenz, die Zertifizierung unterstützt, überprüfbar sein, insbesondere:

- a) die Bedingungen (z. B. die Gebrauchsbedingungen und die Annahmen) der Zertifizierung;
- b) die für die Zertifizierung verwendeten Methoden und Werkzeuge;
- c) die erzielten Ergebnisse (z. B. die zertifizierten Eigenschaften und/oder Messungen)

7.3.4.4.5 Für Klasse 2 muss die Relevanz dieser Bedingungen und Resultate für die Korrektheit und für das leittechnische System begründet werden.

7.3.4.4.6 Für Klasse 2 sollte die Effektivität der für die Zertifizierung verwendeten Methoden und Werkzeuge begründet werden.

7.3.4.4.7 Für Klasse 2 muss die Zertifizierungsstelle festgelegt werden; sie muss für die zertifizierten Eigenschaften und/oder Messungen kompetent sein.

7.3.4.4.8 Für Klasse 2 sollte die Version des zertifizierten PDB dieselbe sein wie die für das leittechnische System verwendete; anderenfalls müssen die Unterschiede zwischen den Versionen analysiert werden, um zu zeigen, dass die Zertifizierung für die gewünschte Version gültig ist.

7.3.5 Ergänzende Prüfungen

In Fällen, in denen die Begründung der PDB-Korrektheit gemäß Überprüfung der Auslegungsdokumentation, Betriebserfahrung oder Zertifizierung oder einer Kombination dieser Methoden nicht erzielt werden kann, mögen ergänzende Prüfungen verwendet werden, um diese Begründung zu unterstützen. Solche ergänzenden Prüfungen können auch notwendig werden, wenn der PDB besonders komplex ist, wie etwa für integrierte Mikroprozessorkerne.

Ergänzende Prüfungen können unter folgenden Bedingungen verwendet werden:

7.3.5.1.1 Die während der Entwicklung einer HPD an einem PDB durchgeführten ergänzenden Prüfungen müssen nach den Anforderungen von 9.1 dieser Norm ablaufen.

7.3.5.1.2 Die ergänzenden Prüfungen müssen den Nachweis erbringen, dass sich der PDB im Rahmen der HPD-Gebrauchsbedingungen wie in der Sicherheitsdokumentation spezifiziert darstellt und verhält.

7.3.5.1.3 Die Gebrauchsbedingungen können Aspekte wie die Konfiguration des PDB (speziell die Einstellung der Parameter und Konfiguration der Daten), die Verwendung der Funktionen und Schnittstellen sowie die Hardwareumgebung betreffen.

7.3.5.1.4 Für Klasse 2 sollten die zur Auslegung der ergänzenden Prüfungen verwendeten Regeln dokumentiert und begründet werden.

7.3.5.1.5 Die Dokumentation der ergänzenden Prüfungen muss enthalten:

- a) die betroffene Version und die Konfiguration des PDB;
- b) eine Beschreibung der durchgeführten Prüfungen und, wenn relevant, der Umgebungsbedingungen, um eine Wiederholung dieser Prüfungen unter identischen Bedingungen zu erlauben;
- c) die gemachten Annahmen und die Evidenz ihrer Gültigkeit;
- d) die erzielten Resultate und die Evidenz ihrer Korrektheit;
- e) die erreichten Schlussfolgerungen und die vereinbarten Lösungen.

7.3.5.1.6 Wenn ergänzende Prüfungen zur Begründung benötigt werden und die Ergebnisse nicht den o. g. Anforderungen entsprechen, muss der PDB abgelehnt werden.

7.3.6 Verwendungsregeln

Die Verwendung von Funktionen oder Betriebsarten, die zur Realisierung der HPD erforderlich sind, können durch Regeln eingeschränkt werden, um Auslegungseigenschaften wie Sicherheit oder Testbarkeit zu verbessern.

7.3.6.1 Wenn die vor-entwickelte Einheit Funktionen, Konfigurationen oder Betriebsarten umfasst, deren Realisierung in der HPD nicht erforderlich ist, sollten Regeln aufgestellt werden, um die Verwendung solcher Funktionen und Betriebsarten zu verhindern.

7.3.6.2 Wenn Verwendungsregeln eingeführt werden,

- a) müssen sie dokumentiert sein,
- b) muss der Verifizierungsplan sicherstellen, dass ihre Erfüllung während des Projekts verifiziert wird.

7.3.7 Änderung für die Annahme

Im Allgemeinen sind Änderungen von PDBs im Zuge der HPD-Auslegung nur für PDBs in der Form von HDL-Quellcode möglich.

7.3.7.1 Wenn Änderungen des PDB zur Erzielung der Annahmefähigkeit notwendig sind, sollten sie spezifiziert, entwickelt, realisiert und verifiziert werden.

7.3.7.2 Diese Änderungen müssen in Übereinstimmung mit den Anforderungen dieser Norm betreffend Projektstruktur und Management, Qualität, Anforderungsspezifikation, Auslegung, Realisierung und Verifizierung durchgeführt werden.

7.3.8 Änderung nach der Annahme

7.3.8.1 Nach jeder Auslegungsänderung des PDB muss wieder eine Annahmeprozedur durchgeführt werden.

7.3.9 Dokumentation der PDB-Annahme

7.3.9.1 Die Annahmedokumentation des PDB muss dem Konfigurationsmanagement unterliegen.

7.3.9.2 Die Dokumentation muss einschließen oder verweisen auf

- a) die Anforderungsspezifikation der HPD,
- b) alle Dokumente, die während der Analyse des PDB herausgegeben oder verlangt wurden,
- c) alle Dokumente, die während der Änderung des PDB herausgegeben wurden.

7.3.9.3 Die Dokumentation muss jede für den richtigen Gebrauch des PDB notwendige Information einschließen und die Randbedingungen seiner ursprünglichen Spezifikation, seiner Gebrauchsanweisungen und Änderungen berücksichtigen.

7.3.9.4 Die Dokumentation muss beschreiben, ob der PDB Gegenstand einer generischen, für die Verwendung in jedem IC gültigen Annahme ist, oder ob die Annahme nur für die Verwendung des PDB in dem HPD-Projekt gilt.

8 HPD-Auslegung und -Realisierung

8.1 Allgemeines

In diesem Abschnitt sind auf guter Auslegungspraxis beruhende Anforderungen und Empfehlungen zusammengestellt, um entsprechende Sicherheitsmerkmale wie Fehlerfreiheit (so gut wie möglich) und Zugänglichkeit für die Verifizierung schaffen zu können.

Obwohl seriell dargestellt, folgt die Auslegungs- und Realisierungsphase in diesem Abschnitt nicht notwendigerweise direkt dem Realisierungs- und Annahmeprozess für vor-entwickelte Einheiten wie in [Abschnitt 7](#) beschrieben. Zum Zweck der Wiederverwendbarkeit mögen die ICs und PDBs schon bei Beginn der anfänglichen Auslegungsphase ausgewählt worden sein. In anderen Fällen können Auswahl und Annahme der ICs und PDBs von den anfänglichen Auslegungsentscheidungen abhängen und können daher erst nach Beginn der anfänglichen Auslegungsphase stattfinden. In allen Fällen ist die HPD-Auslegungsphase ([Abschnitt 8](#)) und der Auswahl- und Abnahmeprozess für vor-entwickelte Einheiten ([Abschnitt 7](#)) im ganzen als iterativer Prozess zu betrachten.

8.1.1 Die HPD-Auslegungs- und -Realisierungsphasen müssen dokumentiert werden.

Das entsprechende Dokument oder die Dokumentenreihe setzt sich aus der HPD-Auslegungsspezifikation ([8.3.6](#)) und der HPD-Realisierungsdokumentation ([8.4.7](#)) zusammen.

8.2 Hardware-Beschreibungssprachen (HDL) und zugehörige Werkzeuge

Wenn auch die Benutzung spezifischer Sprachen und Werkzeuge nicht gefordert werden kann, mögen folgende Ausführungen als gemeinsame grundlegende Regeln für Sprachen und Werkzeuge betrachtet werden, die für Auslegung und Realisierung von HPDs für Systeme der Klasse 2 und Klasse 3 benutzt werden.

8.2.1 Für Auslegung und Realisierung sollten Hardware-Beschreibungssprachen (HDL) und Werkzeuge für Simulation, Synthese, Platzierung und Routing^{N7)} verwendet werden.

ANMERKUNG Wenn entsprechend ausgelegt und angewendet, verbessern diese Werkzeuge wesentliche Aspekte wie z. B. die Verständlichkeit von Beschreibungen, die Handhabung elektrischer und zeitlicher Randbedingungen, die Verifizierung, adäquate Abdeckungskriterien und die Dokumentation.

8.2.2 Auch wenn 8.2.1 nicht erfüllt ist, muss jegliche in dieser Norm geforderte Dokumentation, Analyse oder Verifizierung verfügbar gemacht werden.

8.2.3 Die verwendete Sprache

- a) muss strikten (wohldefinierten) Semantik- und Syntaxregeln folgen;
- b) muss eine vollständig und klardefinierte und dokumentierte Syntax haben;
- c) sollte mit einer anerkannten Norm übereinstimmen (z. B. mit IEEE 1076 für VHDL, IEEE 1364 für Verilog oder IEEE 1800 für SystemVerilog).

8.3 Auslegung

8.3.1 Allgemeines

Beginnend mit der HPD-Anforderungsspezifikation zielt die Auslegung am Beginn darauf ab, die wichtigsten Auswahlmöglichkeiten festzulegen, wie z. B. das Aufteilen der Module (anwendungsspezifisch oder vor-entwickelt), sowie das Festlegen der benötigten mikroelektronischen Technologien (einschließlich ihrer nativen Blöcke) und PDBs. Dann wird unter Nutzung von HDLs eine RTL-Beschreibung aufgebaut. Die folgenden Anforderungen dienen der Erstellung einer klaren und verifizierbaren Auslegung.

8.3.1.1 Die Eingänge für den HPD-Auslegungsprozess müssen die HPD-Anforderungsspezifikation einschließen.

Sie können auch andere Dokumente einschließen, wie etwa projektspezifische Randbedingungen und/oder einschlägige Regeln und Normen.

8.3.1.2 Die anfängliche Entwicklungsphase muss enthalten:

- a) eine Beschreibung der gesamten Organisation des HPD;
- b) die Festlegung der zu verwendenden ICs (Auswahl und Abnahme der ICs müssen auf der HPD-Anforderungsspezifikation beruhen und sind nach 7.2. dieser Norm auszuführen);
- c) eine Beschreibung des gesamten Betriebs der HPD unter den Bedingungen und Betriebsarten wie in der HPD-Anforderungsspezifikation festgelegt;
- d) die Anforderungsspezifikation für jedes in der Auslegung vorgesehene Modul, einschließlich PDBs (die zu dieser Zeit erstellte PDB-Anforderungsspezifikation ist für die Auswahl und Abnahme der PDBs nach den Anforderungen in 7.3 dieser Norm zu verwenden);
- e) eine Beschreibung (auf hoher Ebene) der Simulationsprüfanlagen für die HPD-Tests nach Abschnitt 9 dieser Norm.

8.3.1.3 Zur gesamten Organisation sollte Information bereitgestellt werden betreffend

- i) Beschreibungen und Konfigurationen der RTL-Module, die im Rahmen des HPD-Projekts entwickelt wurden;
- ii) wichtige interne und externe Schnittstellen, einschließlich Kommunikationsschnittstellen und Links zwischen HPD-Komponenten und PDBs.

^{N7)} Nationale Fußnote: „route“ bedeutet Bestimmen bzw. Festlegen der Verbindungen auf dem Chip. Als eingeführter Fachausdruck wird im Folgenden stets „route“ oder „Routing“ verwendet.