

DIN EN 60300-3-4



ICS 03.120.10; 29.020

Einsprüche bis 2018-05-09
Vorgesehen als Ersatz für
DIN EN 60300-3-4:2008-06**Entwurf****Zuverlässigkeitsmanagement –
Teil 3-4: Anwendungsleitfaden –
Anleitung zum Festlegen von Zuverlässigkeitsanforderungen
(IEC 56/1726/CD:2017);
Text Deutsch und Englisch**

Dependability management –
Part 3-4: Application guide –
Guide to the specification of dependability requirements
(IEC 56/1726/CD:2017);
Text in German and English

Gestion de la sûreté de fonctionnement –
Partie 3-4: Guide d'application –
Spécification d'exigences de sûreté de fonctionnement
(IEC 56/1726/CD:2017);
Texte en allemand et anglaise

Anwendungswarnvermerk

Dieser Norm-Entwurf mit Erscheinungsdatum 2018-03-09 wird der Öffentlichkeit zur Prüfung und Stellungnahme vorgelegt.

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

Stellungnahmen werden erbeten

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

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

Gesamtumfang 102 Seiten

DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE

Inhalt

	Seite
Nationales Vorwort.....	5
EINLEITUNG	6
1 Anwendungsbereich	7
2 Normative Verweisungen	7
3 Begriffe	7
4 Allgemeine Betrachtungen zu Zuverlässigkeitsspezifikationen.....	8
4.1 Notwendigkeit der Zuverlässigkeit.....	8
4.2 Anforderungen und Zielsetzungen	10
4.3 Systeme.....	10
4.4 Nachweis der Erfüllung der Anforderungen	12
4.5 Vertraglich vereinbarte Zuverlässigkeit	14
4.6 Spezifikationsarten	15
4.7 Herleitung von Zuverlässigkeitsspezifikationen	16
5 Zuverlässigkeitsspezifikationen von Systemen.....	17
5.1 Systemspezifizierungs-Prozess	17
5.2 Spezifizierung der Systemzuverlässigkeit.....	18
5.3 Bestimmung der Zuverlässigkeitswerte.....	19
5.4 Verfahrensschritte zur Bestimmung der Anforderungen an die Systemzuverlässigkeit	19
6 Zuverlässigkeitsmanagement.....	22
7 Verfügbarkeit	23
7.1 Allgemeines	23
7.2 Festlegung der Verfügbarkeit	25
7.3 Verifizierung und Validierung der Verfügbarkeit.....	25
8 Funktionsfähigkeit.....	26
8.1 Allgemeines	26
8.2 Festlegung der Funktionsfähigkeit	27
8.3 Verifizierung und Validierung der Funktionsfähigkeit	29
9 Instandhaltbarkeit	30
9.1 Allgemeines	30
9.2 Festlegung der Instandhaltbarkeit.....	30
9.3 Verifizierung und Validierung der Instandhaltbarkeit.....	32
10 Unterstützbarkeit	32
10.1 Allgemeines	32
10.2 Festlegung der Unterstützbarkeit	33
10.3 Verifizierung und Validierung der Unterstützbarkeit.....	33
Anhang A (informativ) Bezugsnormen für Verifizierungs- und Validierungsverfahren	34
A.1 Zuverlässigkeitsprüfverfahren	34
A.2 Zuverlässigkeitsanalyseverfahren	35
Anhang B (informativ) Bewertung der Zuverlässigkeitsmerkmale für eine	

	Zuverlässigkeitsspezifikation: ein Haus-Sicherheitssystem.....	Seite 36
B.1	Schritt 1: Bezeichnung des Systems.....	36
B.2	Schritt 2: Beschreibung der Systemziele	36
B.3	Schritt 3: Bezeichnung der Funktionen zur Erreichung der Systemziele.....	36
B.4	Schritt 4: Beschreibung der Funktionen	36
B.5	Schritt 5: Bezeichnung der Einflussfaktoren, die sich auf die Funktionen auswirken.....	37
B.6	Schritt 6: Bewertung des technischen Ansatzes zur Umsetzung der benötigten Funktionen	38
B.7	Schritt 7: Beschreibung der Hardware, der Software und der zum Betrieb des Systems erforderlichen Steuerelemente	39
B.8	Schritt 8: Bestimmung des Betriebsprofils des Systems.....	39
B.9	Schritt 9: Beschreibung der Systemkonfigurationen im Sinne der Systemziele	40
B.10	Schritt 10: Bestimmung der Zuverlässigkeitsanforderungen	41
B.11	Schritt 11: Dokumentation der Systemzuverlässigkeits-Spezifikation	41
	Anhang C (informativ) Bewertung der Zuverlässigkeitsmerkmale	43
C.1	Beispiele für Einflussfaktoren der Systemzuverlässigkeit.....	43
C.1.1	Wirtschaftliche Beschränkungen.....	43
C.1.2	Rechtliche Beschränkungen	43
C.2	Art des Systembetriebs	43
C.3	Kritikalität des Betriebs.....	43
C.3.1	Nutzungsart	44
C.3.2	Benutzerarten.....	44
C.3.3	Abhängigkeit von interagierenden Systemen	45
C.3.4	Struktur oder Konfiguration eines Systems.....	45
C.3.5	Technische Neuheit	45
C.3.6	Erstbetrieb	46
C.3.7	Altlasten.....	46
C.3.8	Komplexität.....	46
C.3.9	Anzahl genutzter Systeme	47
C.4	Bestimmung relevanter Einflussfaktoren für die Bewertung der Systemfunktionen	47
	Anhang D (informativ) Beispiele für Funktionsfähigkeits-, Instandhaltbarkeits-, Unterstützbarkeits- und Verfügbarkeitsanforderungen.....	50
D.1	Allgemeines.....	50
D.2	Anforderungen an die Verfügbarkeit	50
D.3	Anforderungen an die Funktionsfähigkeit	50
D.4	Anforderungen an die Instandhaltbarkeit	51
D.5	Anforderungen an die Unterstützbarkeit	51
	Literaturhinweise	52
 Bilder		
	Bild 1 – Zusammenhang von Kosten und Zuverlässigkeit	9

	Seite
Bild 2 – Elemente eines Systems	10
Bild 3 – Übersicht des Systemspezifizierungs-Prozesses.....	18
Bild 4 – Verfahrensschritte zur Bestimmung der Anforderungen an die Systemzuverlässigkeit	20
Bild B.1 – Systemkonfiguration im normalen Betriebsmodus.....	40
Bild B.2 – Systemkonfiguration im Panik-Betriebsmodus.....	40
Bild B.3 – Systemkonfiguration im Sicherheits-Betriebsmodus.....	41

Tabellen

Tabelle A.1 – Verfahren für die Verifizierung und Validierung der Zuverlässigkeit durch Prüfungen	34
Tabelle A.2 – Verfahren für die Verifizierung und Validierung der Zuverlässigkeit durch Prüfungen	35
Tabelle C.1 – Beispiele für Einflussfaktoren bei jeder einflussnehmenden Bedingung	47
Tabelle C.2 – Beziehung der Systemeigenschaften zu einflussnehmenden Bedingungen	48

Nationales Vorwort

Das internationale Dokument IEC 56/1726/CD:2017 „Dependability management – Part 3-4: Application guide – Guide to the specification of dependability requirements“ (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 beigefügt. Die Nutzungsbedingungen für den deutschen Text des Norm-Entwurfes gelten gleichermaßen auch für den englischen IEC-Text.

Das internationale Dokument wurde vom TC 56 „Dependability“ der Internationalen Elektrotechnischen Kommission (IEC) erarbeitet und den nationalen Komitees zur Stellungnahme vorgelegt.

Die IEC und das Europäische Komitee für Elektrotechnische Normung (CENELEC) haben vereinbart, dass ein auf IEC-Ebene erarbeiteter Entwurf für eine Internationale Norm zeitgleich (parallel) bei IEC und CENELEC zur Umfrage (CDV-Stadium) und Abstimmung als FDIS (en: Final Draft International Standard) bzw. Schluss-Entwurf für eine Europäische Norm gestellt wird, um eine Beschleunigung und Straffung der Normungsarbeit zu erreichen. Dokumente, die bei CENELEC als Europäische Norm angenommen und ratifiziert werden, sind unverändert als Deutsche Normen zu übernehmen.

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

Für dieses Dokument ist das nationale Arbeitsgremium K 132 „Zuverlässigkeit“ der DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE (www.dke.de) zuständig.

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

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

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

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

EINLEITUNG

Für viele Systeme stellen Funktionsfähigkeit, Instandhaltbarkeit, Unterstützbarkeit und die sich daraus ergebende Verfügbarkeit wesentliche Leistungsmerkmale dar. Zusammen genommen werden diese Merkmale mit Zuverlässigkeit bezeichnet.

Für Systeme, für die Zuverlässigkeitsmerkmale wichtig sind, ist es notwendig, dass diese Merkmale in derselben Weise definiert und festgelegt werden wie andere Systemmerkmale, wie zum Beispiel technische Leistung, Maße, Gewicht usw.

Die von einem System erzielte Zuverlässigkeit, also die Leistungen des Systems hinsichtlich der Funktionsfähigkeit, der Instandhaltbarkeit, der Verfügbarkeit und der Unterstützbarkeit, hängen von den Anwendungsbedingungen des Systems und auch von dessen Aufgabenprofil ab. Falls Zuverlässigkeitsmerkmale festgelegt werden, müssen auch die Lager-, Transport-, Realisierungs- und Einsatzbedingungen festgelegt werden, denen das System ausgesetzt sein wird. Es kann wichtig sein, nicht nur die Einsatzbedingungen zu berücksichtigen, sondern auch die Instandhaltungsgrundsätze und die für das System vorgesehene Organisation der Unterstützbarkeit zu beachten.

Dabei können die Zuverlässigkeitsmerkmale sowohl quantitativ als auch qualitativ gemessen werden. Zur Beurteilung einiger der erreichten Zuverlässigkeitsmerkmale und deren Maßgrößen ist es erforderlich, statistische Verfahren zu verwenden.

Zuverlässigkeitsmerkmale können – wie andere Leistungsmerkmale auch – auf folgende drei Arten festgelegt werden:

- 1) vom Lieferanten geschriebene Spezifikationen;
- 2) vom Käufer geschriebene Spezifikationen;
- 3) vom Lieferanten und vom Käufer gemeinsam vereinbarte oder geschriebene Spezifikationen.

Diese Norm ist auf alle drei vorstehenden Spezifikationsarten anwendbar.

Zuverlässigkeitsmanagement – Teil 3-4: Anwendungsleitfaden – Anleitung zum Festlegen von Zuverlässigkeitsanforderungen

1 Anwendungsbereich

Dieser Teil der IEC 60300 leitet zur Festlegung der geforderten Zuverlässigkeitsmerkmale in Spezifikationen an und legt die Verfahren und die Kriterien ihrer Verifizierung und Validierung fest.

Diese Anleitung umfasst insbesondere die folgenden Punkte:

- Empfehlungen zur Festlegung quantitativer und qualitativer Anforderungen an die Funktionsfähigkeit, die Instandhaltbarkeit, die Verfügbarkeit und die Unterstützbarkeit;
- Empfehlungen für Käufer eines Systems zur Sicherstellung, dass die festgelegten Anforderungen von den Lieferanten erfüllt werden;
- Empfehlungen für Lieferanten, um ihnen zu helfen, den Anforderungen der Käufer zu genügen.

Andere Verpflichtungen, wie zum Beispiel Gesetze und behördliche Regulierungen, können ebenfalls Anforderungen an Systeme enthalten. Diese sollten gegebenenfalls zusätzlich zu den in Übereinstimmung mit dieser Norm abgeleiteten Spezifikationen angewendet werden.

ANMERKUNG 1 Obwohl die in den verschiedenen Teilen der Normenreihe IEC 60300 beschriebenen Verfahren sich in erster Linie an die Zuverlässigkeit von Systemen und Geräten richten, können davon viele auch auf die Produkt- oder Bauelementeebene angewendet werden. Der Begriff „System“ wird in dieser Norm durchgehend verwendet.

ANMERKUNG 2 Mit dieser Norm wird nicht beabsichtigt, eine Anleitung zum Management von Zuverlässigkeitsprogrammen oder den Tätigkeiten zu geben, die zur Erfüllung der festgelegten Anforderungen an Verfügbarkeit, Funktionsfähigkeit, Instandhaltbarkeit und Unterstützbarkeit notwendig sind. Hinweise zu dieser allgemeinen Anleitung können IEC 60300-1 entnommen werden.

ANMERKUNG 3 Sicherheits- und Umweltspezifikationen werden in dieser Anleitung nicht direkt behandelt. Jedoch könnten viele der in dieser Norm gegebenen Anleitungen auch auf Sicherheits- und Umweltspezifikationen angewendet werden.

ANMERKUNG 4 Spezifikationen zur Zuverlässigkeit von Dienstleistungen, einschließlich solcher Dienstleistungen, die im Rahmen von Partnerschaften des öffentlichen mit dem privaten Bereich beschafft werden, sind nicht Gegenstand dieser Anleitungen.

2 Normative Verweisungen

Die folgenden Dokumente, die in diesem Dokument teilweise oder als Ganzes zitiert werden, sind für die Anwendung dieses Dokuments erforderlich. Bei datierten Verweisungen gilt nur die in Bezug genommene Ausgabe. Bei undatierten Verweisungen gilt die letzte Ausgabe des in Bezug genommenen Dokuments (einschließlich aller Änderungen).

IEC 60050-192, *International Electrotechnical Vocabulary (IEV) – Chapter 192: Dependability and quality of service*.

3 Begriffe

Für die Anwendung dieses Dokuments gelten die Begriffe nach IEC 60050-192 und die folgenden Begriffe.

ANMERKUNG Die Definitionen von „Zuverlässigkeit“, „Verfügbarkeit“, „Funktionsfähigkeit“, „Instandhaltbarkeit“, „Unterstützbarkeit“, „Ausfall“, „Fehlzustand“, „Betrachtungseinheit“, „Dauer bis zum Ausfall“ und „Betriebsdauer zwischen Ausfällen“ sind in IEC 60050-192 enthalten.

3.1

Verifizierung

Bestätigung durch Bereitstellung eines objektiven Nachweises, dass festgelegte Anforderungen erfüllt worden sind

[ISO 9000:2005, Definition 3.8.4, modifiziert]

Anmerkung 1 zum Begriff: Im Zusammenhang mit dieser Norm ist Verifizierung die Tätigkeit, die in jeder Phase des relevanten Lebenszyklus durch Analyse und/oder Prüfung darlegt, dass für die speziellen Eingaben die gelieferten Elemente in jeder Hinsicht die Zielsetzungen und Anforderungen erfüllen, die für diese Phase festgelegt wurden.

Anmerkung 2 zum Begriff: Zu Tätigkeiten der Verifizierung zählen beispielsweise:

- die Bewertung der Ergebnisse (Dokumente von allen Lebenszyklusphasen), um unter Berücksichtigung der jeweiligen Eingaben für diese Phase die Übereinstimmung mit den Zielsetzungen und Anforderungen dieser Phase sicherzustellen;
- Entwicklungsbewertungen;
- Ausführung von Prüfungen an entwickelten Systemen, um sicherzustellen, dass sie gemäß ihrer Spezifikation arbeiten;
- Ausführung von Integrationsprüfungen, wobei unterschiedliche Teile eines Systems Schritt für Schritt zusammengesetzt und Prüfungen unter Umgebungsbedingungen durchgeführt werden, um sicherzustellen, dass alle Teile zusammenarbeiten.

3.2

Validierung

Bestätigung durch Bereitstellung eines objektiven Nachweises, dass die Anforderungen an eine spezifische Zweckbestimmung oder Anwendung erfüllt worden sind

[ISO 9000:2005, Definition 3.8.5, modifiziert]

Anmerkung 1 zum Begriff: Validierung ist die Tätigkeit, die darlegt, dass das betrachtete System vor und nach der Installation in jeder Hinsicht der Anforderungsspezifikation dieses Systems entspricht. Deshalb bedeutet beispielsweise der Begriff „Softwarevalidierung“ die Bestätigung durch Untersuchung und Bereitstellung eines objektiven Nachweises, dass die Software die Softwarespezifikation erfüllt.

4 Allgemeine Betrachtungen zu Zuverlässigkeitsspezifikationen

4.1 Notwendigkeit der Zuverlässigkeit

Jedes System weist ein gewisses Maß an Zuverlässigkeit auf, unabhängig davon, wie oft es ausfällt oder instand gehalten werden muss. Wenn ein System jedoch zu oft ausfällt, könnte es gerade dann nicht funktionieren, wenn es gebraucht wird, oder seine Instandhaltung könnte zu kostspielig sein. Außerdem stehen häufig ausfallende Systeme bei den Anwendern in einem schlechten Ruf und werden somit bei einer anstehenden Ersatzbeschaffung wahrscheinlich nicht wieder berücksichtigt. Andererseits kann die Entwicklung und Herstellung sehr zuverlässiger Systeme teuer sein, und es ist unter Umständen nicht möglich, ein solches System zu einem wirtschaftlichen Preis herzustellen. Man muss daher abwägen zwischen wenig zuverlässigen Systemen mit hohen Instandhaltungskosten und hoch zuverlässigen Systemen, deren Entwicklung aufwendig sein kann. Dies ist graphisch in Bild 1 dargestellt, in dem die Entwicklungs- und Betriebskosten von Systemen unterschiedlicher Zuverlässigkeit gegenübergestellt werden.

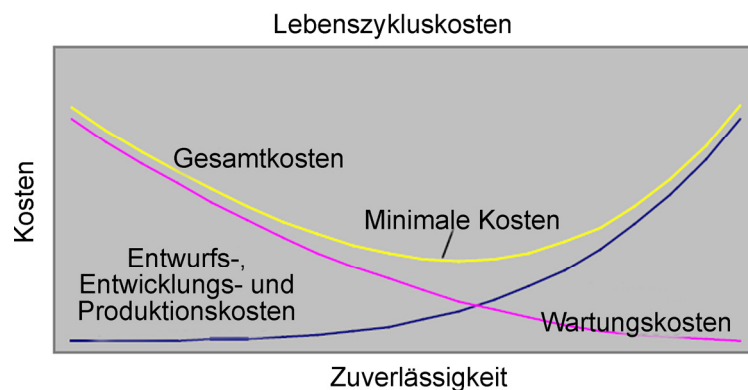


Bild 1 – Zusammenhang von Kosten und Zuverlässigkeit

In Bild 1 wird gezeigt, dass es ein Zuverlässigkeitsniveau gibt, bei dem die Gesamtkosten über die Lebensdauer eines Systems minimiert sind. Bei handelsüblichen Systemen (COTS, en: commercial off the shelf) verschiebt sich dieses Minimum, da die Entwurfs- und Entwicklungskosten auf mehrere Parteien aufgeteilt werden können. Die optimale Zuverlässigkeit eines Systems kann jedoch durch andere Faktoren beeinflusst werden, so beispielsweise durch Sicherheitsanforderungen oder Systemfunktionen, und stellt somit nicht notwendigerweise die Zuverlässigkeit dar, die den minimalen Lebenszykluskosten entspricht.

Es ist zu vermuten, dass Systeme, die von solchen Organisation produziert werden, die die Zuverlässigkeit nicht aktiv betreiben, nur Zuverlässigkeitsniveaus erreichen, die deutlich unter dem Punkt der minimalen Lebenszykluskosten liegen. Eine Investition in eine an der Zuverlässigkeit orientierte Entwicklung kann sich daher hinsichtlich der kombinierten Entwicklungs-, Realisierungs- und Betriebskosten auszahlen. IEC 60300-3-3 beschreibt Lebenszykluskosten und die Beziehungen zwischen Zuverlässigkeit und Kosten.

Zur Zuverlässigkeit gehören eine Reihe von Merkmalen, die auf unterschiedliche Weise festgelegt werden. In dieser Norm wird die Zuverlässigkeit unter den folgenden vier Überschriften betrachtet:

- Verfügbarkeit;
- Funktionsfähigkeit, ausgedrückt als eine Wahrscheinlichkeit $R(t)$ der mittleren Dauer bis zum Ausfall (MTTF, en: mean time to failure) oder die mittlere Betriebsdauer zwischen Ausfällen (MTBF, en: mean operating time between failures) sowie Parameter der Weibull- oder Exponentialverteilungen;
- Instandhaltbarkeit, hierzu gehören die mittlere Unklardauer (MDT, en: mean down time) und die mittlere Dauer bis zur Wiederherstellung (MTTR, en: mean time to restoration);
- Unterstützbarkeit.

Die zur Spezifizierung ausgewählten Zuverlässigkeitsmerkmale sollten an der Art und Aufgabe des Systems, dessen beabsichtigter Verwendung und der Kritikalität der geforderten Funktion ausgerichtet sein. Wenn zum Beispiel keine Instandhaltungsaufgaben vorgesehen sind, wird man nur Anforderungen an die Funktionsfähigkeit festlegen.

Anforderungen an die Verfügbarkeit werden allgemein dann festgelegt, wenn durch Unklarzeiten in Systemen wirtschaftliche oder andere Verluste durch erhöhte Betriebskosten oder wenn Verletzungen von Personen oder Dienstausschlag entstehen könnten. Beispiele hierfür sind Anlagen, Fertigungsstätten, medizinische Geräte, Sicherheitseinrichtungen und militärische Systeme. Die Verfügbarkeit kann anhand der Systemkonfiguration, anhand der Subsysteme einschließlich der an diese gerichteten Anforderungen zur Funktionsfähigkeit und Instandhaltbarkeit, sofern diese angegeben sind, sowie unter Berücksichtigung der Unterstützbarkeit berechnet werden.

Anforderungen an die Instandhaltbarkeit von Systemen sollten dann festgelegt werden, wenn die Instandhaltungskosten wesentlich zu den Lebenszykluskosten beitragen oder wenn die Instandhaltung für den Käufer oder Benutzer wichtig ist. Falls zutreffend, sollten auch Anforderungen an die vorbeugende und korrektive Instandhaltung (also Wartung und Instandsetzung) festgelegt werden.

ANMERKUNG Der Grad der Unterstützbarkeit ergibt sich oft aus den Anwendungsbedingungen und ist keine inhärente Anforderung an das System selbst.

In den Abschnitten 7, 8, 9 und 10 wird weiter dargelegt, wann welches Zuverlässigkeitsmerkmal am besten geeignet ist.

Die in einem System erzielte Zuverlässigkeit hängt sehr stark davon ab, wie es entwickelt, installiert und betrieben wird. Zuverlässigkeit ist daher auch im Zusammenhang mit anderen Merkmalen wie Qualität oder dem Entwicklungs- und Fertigungsprozess zu sehen. Die Zuverlässigkeitsspezifikation sollte deshalb Teil der Spezifikation für das Gesamtsystem sein, und Wechselwirkungen der verschiedenen Merkmale sollten erkannt und berücksichtigt werden.

4.2 Anforderungen und Zielsetzungen

Es ist in einer Spezifikation wichtig, zwischen förmlich festgeschriebenen Anforderungen und Zielsetzungen zu unterscheiden, da die Annahmeverfahren hierfür verschieden sind.

Eine Anforderung ist Teil einer Spezifikation, die aus Sicht des Käufers unerlässlich ist und die vom System erfüllt und vom Lieferanten nachgewiesen werden muss. Dieser Nachweis kann als Teil der vereinbarten Liefergegenstände erbracht werden, noch bevor das System in Betrieb gesetzt wird, oder auch nach Inbetriebsetzung des Systems. Dabei können für die Erfüllung dieser Anforderungen Anreize gegeben oder bei Nichterfüllung Vertragsstrafen angedroht werden.

Eine Zielsetzung ist dagegen keine Anforderung, aber sie ist aus Sicht des Käufers erstrebenswert, und ein Nachweis des Erfüllungsgrads braucht entweder nicht oder er kann nicht erbracht werden.

Für Systeme hoher Verfügbarkeit oder hoher Funktionsfähigkeit wird es möglicherweise nicht praktikabel oder kosteneffizient sein, einen formalen Nachweis des Erreichens der hohen Verfügbarkeit oder Funktionsfähigkeit zu erbringen. Der Käufer muss die Zielwerte für die nicht nachweisbare hohe Verfügbarkeit und Funktionsfähigkeit eindeutig bezeichnen sowie niedrigere Anforderungen festlegen, die nachgewiesen werden können.

4.3 Systeme

Die Zuverlässigkeit sollte in der Systemebene festgelegt werden. Zu einem System gehören die Einrichtungen (sowohl Hardware und Software) als auch das Personal, das das System betreibt und instand hält, sowie die dafür vorgesehenen Prozeduren. Außerdem gehört zum System die Umgebung, in der es betrieben wird, siehe Bild 2.

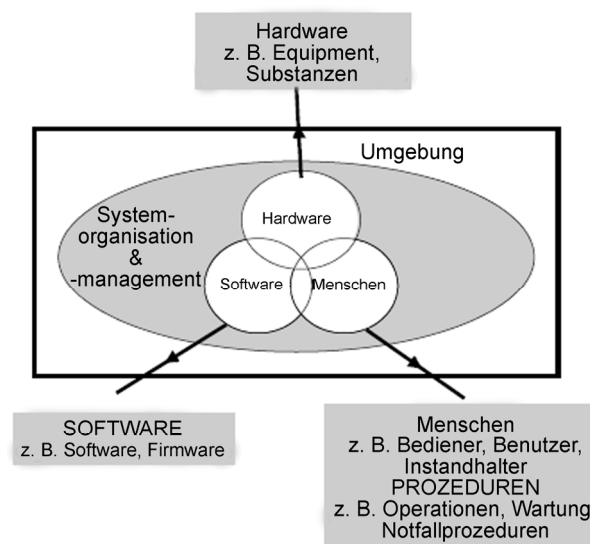


Bild 2 – Elemente eines Systems

Alle Elemente (siehe Bild 2) eines Systems sollten, soweit möglich, in die Zuverlässigkeitsspezifikation aufgenommen werden, da eine Veränderung in einem Element eine signifikante Auswirkung auf die vom

System erzielte Zuverlässigkeit haben kann. Die Zuverlässigkeitsanforderungen sollten außerdem die jeweiligen Umstände des spezifizierten Systems berücksichtigen. Zusätzlich sollten die Zuverlässigkeitsanforderungen mit dem Betriebs- oder Einsatzprofil oder den funktionalen Anforderungen an das System verbunden sein. Das System sollte in Einklang mit Abschnitt 5.4 definiert werden. Dort ist näher beschrieben, wie man ein System, seine Elemente und die Kritikalität jeder Funktion definieren kann, sodass Anforderungen an jedes Element festgelegt werden können.

BEISPIEL 1 So können verschiedene Benutzer eines Systems dieses missbrauchen oder dieses in einer aggressiveren Art anwenden. Dies kann mehr Ausfälle hervorrufen und so eine geringere Zuverlässigkeit bewirken.

BEISPIEL 2 Es kann Fälle geben, in denen Lieferant und Käufer wenig oder keine Kontrolle über spätere Instandhaltungsverfahren oder Fähigkeiten haben, beispielsweise bei einem öffentlich verkauften Kraftfahrzeug.

Die Zuverlässigkeitsspezifikation eines Systems sollte neben den Anforderungen an die Hardware auch die Spezifikation der Software und die Elemente beinhalten, die für die Menschen stehen. Die in dieser Norm gegebenen Anleitungen können in gewisser Hinsicht auch auf die Spezifizierung der Software angewendet werden. Für genauere Anleitungen wird jedoch auf IEC 62628 und die verschiedenen Teile von IEC 61508 verwiesen.

Systeme werden auf vielen unterschiedlichen Ebenen definiert und jedes System kann selbst wiederum aus anderen Systemen zusammengesetzt sein. Dabei wird dann oft von einem System von Systemen gesprochen. Dazu gehört etwa die Betrachtung der Wechselwirkung mit den Menschen, die das Subsystem benutzen, und die Art und Weise, in der sie das tun. Außerdem ist zu beachten, auf welche Weise die verschiedenen Menschen das Subsystem unterschiedlichen Belastungen aussetzen.

BEISPIEL 1 So ist beispielsweise ein Autobus ein System aus Kraftfahrzeug, einem Fahrer und den Fahr- und Lenkvorschriften. Das Kraftfahrzeug besteht aus Subsystemen, die selbst wiederum Systeme sind, zum Beispiel Motor oder Getriebe. Dabei besteht die Eingabe des Fahrers in das Getriebe in der Betätigung des Schalthebels. Die Subsysteme sind aus Komponenten und Geräten zusammengesetzt, die für sich selbst als Systeme angesehen und dementsprechend analysiert werden können.

BEISPIEL 2 Unterschiedliche Fahrer fahren das Fahrzeug auf unterschiedliche Weise und setzen das Getriebe einer mehr oder weniger großen Belastung aus.

Ein Käufer könnte etwa eine Zuverlässigkeitsanforderung lediglich für die höchste Systemebene festlegen wollen, oder er könnte entscheiden und es für wichtig erachten, dass ein Subsystem die sich daraus ergebende Funktionsfähigkeit nicht dominiert, und daher auch Anforderungen für untere Ebenen festlegen wollen. Diese Anforderungen an untere Ebenen müssen jedoch mit den Anforderungen an die oberste Ebene im Einklang sein. Diese müssen außerdem messbar und erreichbar sein, sonst sind sie lediglich Zielsetzungen und keine Anforderungen. Daher muss beispielsweise der Beitrag eines Subsystems zur Zuverlässigkeit des Gesamtsystems geschätzt werden, bevor man die Anforderungen auf die Subsysteme aufteilen kann. Die Aufteilung auf Subsysteme der unteren Ebene verläuft nicht geradlinig, es sei denn, es handelt sich um serielle Systeme, die aus Subsystemen mit konstanter Ausfallrate bestehen. In anderen Fällen, etwa bei Systemen mit Redundanz oder bei sich zeitlich ändernder Ausfallrate, wird auf IEC 61025 und IEC 61078 verwiesen. In IEC 60300-3-1 und IEC 61703 sind weitere Anleitungen zur Analyse der Systemzuverlässigkeit enthalten.

Die Art und Beschaffenheit eines Systems hat Einfluss auf die Zuverlässigkeitsspezifikation. Dabei muss zwischen instandsetzbaren und nicht instandsetzbaren Systemen sowie Geräten zur einmaligen Benutzung unterschieden werden. Zu den instandsetzbaren Systemen gehören solche, die repariert werden können und danach wieder in den betriebsbereiten Zustand zurückkehren. Beispiele für nicht instandsetzbare Systeme sind versiegelte Einheiten, handelsübliche Einheiten, Systeme, bei denen die Reparaturkosten die Ersatzbeschaffungskosten übertreffen, wie dies beispielsweise bei vielen Konsumgütern der Fall ist, und Systeme an entlegenen Orten, an denen die Fachkenntnisse und Ersatzteile für die fragliche Zeit nicht verfügbar sind. Zu den Geräten zur einmaligen Benutzung zählen u. a. Sprengkörper, Airbags in Fahrzeugen und Schutzhelme.

Nicht instandsetzbare Systeme werden nicht repariert und müssen ersetzt werden. Die Anforderungen an die Instandhaltbarkeit und die Unterstützbarkeit werden somit grundlegend verschieden sein. So wird auch der mittlere Ausfallabstand (MTBF) für Geräte zur einmaligen Benutzung keine zutreffende Maßgröße sein. Für

diese Geräte ist die Wahrscheinlichkeit, dass das System verlässlich funktioniert, wenn es gebraucht wird (Funktionsfähigkeit), oder alternativ die Wahrscheinlichkeit vorzeitiger Aktivierung die richtige Maßgröße. Es obliegt dem Käufer, dass die Art des Systems und die resultierende Auswirkung auf die Zuverlässigkeitsanforderungen bezeichnet werden, bevor die Spezifikation geschrieben wird.

4.4 Nachweis der Erfüllung der Anforderungen

4.4.1 Allgemeines

In jeder Spezifikation gibt es zwei Elemente: die Zuverlässigkeitsanforderungen und die Art und Weise, wie der Lieferant die Erfüllung der Anforderungen dem Käufer gegenüber nachweisen soll. Dies bedeutet, dass der Lieferant dem Käufer gegenüber hinreichend nachweisen muss, dass das System seine Anforderungen erfüllt, um ihm so das nötige Vertrauen für die Bezahlung des vereinbarten Preises zu geben. Die Bereitstellung zusätzlicher Nachweise trägt zu den höheren Kosten hoch zuverlässiger Systeme bei (siehe Bild 1), aber ohne diese Maßnahmen besteht die Möglichkeit, dass das System die vereinbarten Anforderungen nicht erfüllt.

Für die Darstellung der Anforderungen gibt es zwei Hauptelemente: Verifizierung und Validierung. Diese sind in ISO 9000 festgelegt und werden sowohl im Hardware- als auch im Softwarebereich als Teil des Softwareentwicklungsprozesses oder „V-Modells“ eingesetzt (siehe IEC 61508). Sie können wie folgt erklärt werden: Verifizierung ist der Prozess der Bereitstellung eines Nachweises, dass das System in jeder Lebenszyklusphase seine Anforderungen aus den (der) vorhergehenden Phase(n) erfüllt. Validierung ist der Prozess der Bereitstellung eines Nachweises, dass das System die aktuellen Anforderungen erfüllt, die manchmal nicht so in der geschriebenen Spezifikation festgelegt sind. Beides sind unerlässliche Elemente.

Das Ausmaß der vom Käufer geforderten Verifizierung und Validierung hängt von dem vom Käufer geforderten Vertrauensbeweis ab, dass das System die festgelegten Zuverlässigkeitswerte auch erreichen wird. Falls der Käufer damit einverstanden ist, ein im Betrieb ausfallendes System instand zu setzen, könnte er einem einfacheren Nachweis und somit einem geringeren Vertrauensbeweis in die erreichte Zuverlässigkeit zustimmen. Der Grund hierfür ist, dass die Bereitstellung eines Nachweises Geld kostet und der Käufer gewillt sein könnte, das Risiko eines nicht wie festgelegt arbeitenden Systems zu tragen. Der Käufer muss bei der Festlegung der Anforderungen an die Verifizierung und Validierung abwägen, welches Risiko er einzugehen bereit ist (siehe IEC 62198 zu weitergehenden Informationen zum Projektrisikomanagement).

Um wirkungsvoll zu sein, müssen Verifizierungs- und Validierungstätigkeiten geplant werden und systematisch sein. Dazu muss der Lieferant die geplanten Tätigkeiten vorher ankündigen und die Zustimmung des Käufers hierzu einholen, dies wird häufig im Vertrag geregelt. In den Zuverlässigkeitsanforderungen sollten die verschiedenen Faktoren berücksichtigt werden, die sich wahrscheinlich auf die Kosten für die Zuverlässigkeitsverifizierung und -validierung niederschlagen. Hierzu zählen auch die erwartete Lebensdauer und die Entsorgung oder Wiederverwendung des Systems.

Bei langfristigen Beschaffungsmaßnahmen werden die Aktivitäten unter Umständen bereits viele Jahre vor dem Abschluss geplant. Je nach Vertragsbedingungen erhält der Käufer daher während der Projektausführung hierüber möglicherweise nur eine geringe Kontrolle. Ein Weg sowohl für den Käufer als auch für den Lieferanten, das Projektrisiko zu mindern, dass das System ggf. nicht das geforderte Nachweisniveau erreicht, kann eine fortschreitende Verifizierung und Validierung sein. Hierzu werden die Tätigkeiten über den gesamten Lebenszyklus hinweg geplant und die Ergebnisse dem Käufer bei Projekt-Meilensteinen mitgeteilt. Auf diese Weise kann der Käufer Vertrauen in das System gewinnen, und das Risiko eines ungenügenden Nachweises kann somit weitgehend reduziert werden.

Ein Modell, mit dem der Lieferant dem Käufer einen Nachweis bereitstellen kann, dass das System die gestellten Anforderungen erfüllt hat, ist der Zuverlässigkeitsnachweis (D-Case, en: dependability case). Der Zuverlässigkeitsnachweis führt zu einem begründeten und nachvollziehbaren Beweis, dass das System die gestellten Anforderungen erfüllt hat. Anlässlich von Projekt-Meilensteinen gibt es im D-Case-Bericht hierzu Zusammenfassungen. Mithilfe der Zuverlässigkeitsnachweise werden bei einer Reihe von Projekt-Meilensteinen üblicherweise fortschreitende Nachweise erbracht. Anleitungen und Hinweise zu Zuverlässigkeitsnachweisen können IEC 62741 entnommen werden.

4.4.2 Aktivitäten

Verifizierung und Validierung beinhalten eine Reihe von Aktivitäten, anhand derer der Nachweis erbracht werden soll, dass ein System die gestellten Zuverlässigkeitsanforderungen erfüllt. Diese Aktivitäten können mittels verschiedener Techniken erbracht werden, die alle dasselbe oder ein ähnliches Ziel haben, bei denen aber verschiedene Verfahren verwendet werden. Die Wahl des Verfahrens hängt von einer Reihe von Faktoren ab und ist in IEC 60300-3-1 näher beschrieben.

Verlangt der Käufer eine Verifizierung und Validierung, muss der Lieferant das Ziel dieser Aktivitäten und deren Beitrag hierzu bestimmen. So sollte beispielsweise in einer Spezifikation nicht die Durchführung einer Fehlzustandsbaumanalyse (FTA, en: fault tree analysis) verlangt werden, sondern eine Analyse zur Bestimmung, wie die Kombination von Ereignissen zu einem Systemausfall führen kann. Hierfür könnte auch ein Zuverlässigkeitsblockdiagramm (RBD, en: reliability block diagram) ein gleichwertiges Verfahren sein, mit dem dasselbe Ziel erreicht werden kann. Die Wahl des Verfahrens sollte im Ermessen des Lieferanten liegen, dieser hat dabei aber Faktoren, wie die Erfahrung des Analysten, verfügbare Zeit sowie erforderliche Daten und Information zu berücksichtigen. So wäre beispielsweise eine Analyse anhand eines Zuverlässigkeitsblockdiagramms durch einen erfahrenen Analysten einer schlecht ausgeführten Fehlzustandsbaumanalyse durch einen unerfahrenen Analysten vorzuziehen.

Zu den Verifizierungs- und Validierungsaktivitäten gehören:

a) Analyse:

- 1) Einhaltung von Normen, Vorschriften und Leitlinien;
- 2) Bewertung durch Fachleute, Anwendung optimaler Verfahren, Zertifizierung;
- 3) Konstruktionsberechnungen (zum Beispiel Analyse der Beanspruchung und Ermüdung anhand der Methode der finiten Elemente);
- 4) Simulation (zum Beispiel des Systemverhaltens);
- 5) Spezifische Zuverlässigkeitsanalyse.

b) Prüfungen und Nachweise:

- 1) Früheres Betriebsverhalten identischer oder ähnlicher Einheiten in identischen oder ähnlichen Anwendungen;
- 2) Spezifische Zuverlässigkeitsprüfungen, unter anderem:
 - i) Nachweisprüfungen der Funktionsfähigkeit, z. B. durch Prüfung behobener Fehler pro Zeit, Folgeprüfungen, Prüfungen des Erfolgsquotienten, beschleunigte Prüfungen oder Lebensdauerprüfungen;
 - ii) Nachweisprüfungen der Verfügbarkeit;
 - iii) Nachweisprüfungen der Instandhaltbarkeit.
- 3) Sonstige Prüfungen während der Entwicklung (z. B. Leistung, Ermüdung während der Lebensdauer, Softwaretests auf Komponenten-, Modul- oder Systemebene).

Weitere Einzelheiten zu den Verfahren der Zuverlässigkeitsverifizierung und -validierung sind in anderen Teilen der Normenreihe IEC 60300 enthalten. Eine Liste der hierfür relevanten IEC-Normen kann 0 entnommen werden.

Diese Tätigkeiten sind nicht für alle Lebenszyklusphasen gleichermaßen geeignet. Systemprüfungen können erst nach Abschluss der Entwicklung und bei Vorhandensein eines Prototyps erfolgen. Dagegen sind Analyseaktivitäten in den Entwicklungsphasen sehr wohl geeignet, die Auswirkung verschiedener Optionen auf die geschätzte Zuverlässigkeit zu ermitteln. Die Systemprüfung sollte jedoch bereits in der Entwurfsphase geplant werden, damit der Lieferant die erforderlichen Prüfungen der Subsysteme noch vor dem Zusammenbau und der Integration des Systems festlegen kann. Außerdem sollte das System für das diagnostische Prüfen eingerichtet sein, d. h., das übergeordnete System und die nachgeordneten Systeme sollten so ausgelegt sein, dass sie geprüft werden können (siehe IEC 60706-5).

Es wird darauf hingewiesen, dass alle während der Entwicklung erbrachten Nachweise lediglich eine Vorhersage der wahrscheinlichen Zuverlässigkeit liefern und dass die Analyseergebnisse wahrscheinlich weniger genau als die aus Prüfungen erhaltenen Ergebnisse sind. Daher wird der Käufer sich vermutlich

nicht bloß auf Analyseergebnisse verlassen wollen und zusätzlich eine Kombination aus Analyse und Prüftätigkeiten fordern, um so Beweise für das Erreichen der Anforderungen zu liefern. Zusätzlich müssen bei der Planung der Prüfungen die vorhandene Prüfumgebung und Prüfanwendung des Systems berücksichtigt werden. Sollte die Prüfung nahezu bei Einsatzbedingungen erfolgen, so wird dies zu einer guten Schätzung der Zuverlässigkeit führen. Solche Prüfungen werden aber lange dauern, man wird viele Prüflinge benötigen und die geringe Ausfallanzahl wird zu einer großen Unsicherheit in der Vorhersage der Zuverlässigkeit führen. Bei einer beschleunigten Prüfung kann dagegen die Prüfdauer und die Anzahl der Prüflinge reduziert werden. Die größere Ausfallanzahl wird die statistische Unsicherheit reduzieren. Jedoch wird dann die technische Unsicherheit größer werden, da die beschleunigten Prüfbedingungen zu Ausfallarten führen können, die im eigentlichen Betrieb keine Rolle spielen.

4.5 Vertraglich vereinbarte Zuverlässigkeit

Der Sinn einer Spezifikation ist es, einem Käufer eine Grundlage für den Kauf eines Systems zu geben. Solch eine Spezifikation wird üblicherweise Bestandteil des Vertrags zwischen Käufer und Lieferant sein. Daher ist es unerlässlich, dass sie so geschrieben wird, dass sie für einen Vertrag geeignet ist. Eine vertraglich vereinbarte Zuverlässigkeit kann viele Formen haben, wie etwa die Leistung von Zahlungen bei Erreichen eines Projekt-Meilensteins und erfolgreicher Erfüllung einer Nachweisprüfung bis zur Androhung von Vertragsstrafen sowie der Schaffung von Anreizen bei im Betrieb erreichter Zuverlässigkeit.

Es muss unterschieden werden zwischen den Anforderungen, anhand derer im Einzelnen dargelegt wird, wie ein System arbeiten soll, und der geschriebenen Spezifikation, die im Einzelnen darlegt, was das System enthält. Je nach Art des Systems können sich dabei unterschiedliche Komplexitätsgrade ergeben. Sowohl die Anforderungen als auch die Spezifikationen können sowohl vom Käufer als auch vom Lieferanten erarbeitet werden. Für beide können die Anleitungen in dieser Norm nützlich sein.

Bei der vertraglichen Vereinbarung der Zuverlässigkeit muss sehr sorgfältig vorgegangen werden, damit die entsprechenden Vertragsklauseln auch Sinn ergeben.

BEISPIEL Ein Vertrag über ein Gerät zur einmaligen Benutzung mit einer Klausel, in der eine Funktionsfähigkeit von 99,5 % gefordert wird. Im Vertrag wird darüber hinaus ein vollständiger Zuverlässigkeitsnachweis mit 80 % Vertrauensniveau gefordert. Hierfür wären mindestens 322 Prüfungen erforderlich, dies wären sechs Mal mehr Einheiten als der beabsichtigte Kauf von 50 Einheiten gewesen. Da das System als ein Gerät zur einmaligen Benutzung konstruiert worden war, stellte dies eine eindeutig unrealistische Forderung dar. Der Käufer musste somit einen anderen Weg suchen, auf dem die geforderte Verifizierung und Validierung zu erreichen war. Als solcher kämen entweder niedrigere nachweisliche Zuverlässigkeitsziele oder Analysen, Simulationen oder Prüfungen von Subsystemen in Betracht.

Die Wahl der vertraglich festzulegenden Verifizierungs- und Validierungsaktivitäten hängt von dem vom Käufer akzeptierten Projektrisiko ab. Falls der Käufer bereit ist, das Risiko eines ausfallenden Systems in Kauf zu nehmen, das dann vom Lieferanten wieder instand gesetzt wird, könnten Vertragsstrafen bei ungenügender Leistung und Anreize bei Übererfüllung der Anforderungen die beste Methode sein. Ist der Käufer dagegen nicht gewillt, das Risiko eines nicht verfügbaren Systems einzugehen, so könnten förmliche Zuverlässigkeits- oder Verfügbarkeits-Nachweisprüfungen nötig sein. Besondere Sorgfalt sollte bei seltenen Ereignissen walten, da diese kaum durch Prüfungen ausgeschlossen werden können.

Die Vorteile der genannten Vorgehensweisen sind:

- a) Vertragsstrafen bei ungenügender Leistung werden den Lieferanten veranlassen, der Zuverlässigkeit seine ganze Aufmerksamkeit zu widmen und so zu höheren Zuverlässigkeitswerten zu gelangen als auf anderen Wegen;
- b) Nachweisprüfungen sind teuer und zeitaufwendig, und stellen unter Umständen kurz vor der geplanten Inbetriebnahme nur dar, dass das System die Zuverlässigkeitsanforderungen nicht erfüllt;
- c) die Aufforderung an den Lieferanten, die Instandhaltung zu übernehmen, erfordert einen viel längeren Vertrag, beispielsweise eine Instandhaltungsvereinbarung zu fixen Kosten mit den damit einhergehenden Schwierigkeiten. Aber damit liegt das Risiko einer ungenügenden Systemzuverlässigkeit beim Lieferanten, während der Käufer gegebenenfalls mit Folgeschäden aus der ungenügenden Systemzuverlässigkeit rechnen muss.

Wenn die Zuverlässigkeit vertraglich per Spezifikation geregelt werden soll, dann muss diese Spezifikation vollständig ausformuliert werden, damit unterschiedliche Auffassungen nach Vertragsabschluss vermieden werden. Beispiele für die in einen Vertrag aufzunehmenden spezifizierenden Elemente sind:

- Präzise und eindeutig festgelegte Kriterien für die Bewertung der Verfügbarkeit, der Funktionsfähigkeit, der Instandhaltbarkeit und der Unterstützbarkeit;
- Pflichten und Verantwortlichkeiten des Käufers, des Lieferanten und ggf. von Dritten;
- Beschreibung des zu betrachtenden Systems, der Geräte und Baugruppen, für die die Anforderungen gelten;
- Beabsichtigte Systemfunktionen;
- Verschiedene Betriebs- und Umgebungsbedingungen, bei denen das System verwendet wird, einschließlich, soweit zutreffend, der anteilig in jeder Bedingung verbrachten Zeit;
- Definition von Ausfällen und Ausfallkriterien, also beispielsweise, ob es sich um einen vollständigen Systemausfall handelt, nach dem überhaupt keine Funktion mehr verfügbar ist, oder um einen Ausfall wesentlicher Funktionen, einen Teilausfall oder um eine Leistungsver schlechterung;
- Art und Weise der Installation und der Nutzung des Systems;
- Qualifikationen und Verantwortlichkeiten des für den Betrieb und die Instandhaltung der Hardware, der Software und der Pflege der Dokumentation zuständigen Personals;
- Anzuwendende Instandhaltungsgrundsätze und zugehörige Verfahren und logistische Vorkehrungen;
- Angedachte Verfahren zur Verifizierung und Validierung der Übereinstimmung mit den Anforderungen, einschließlich Annahme- und Rückweisungskriterien;
- Akzeptable Datenquellen für Analyseverfahren.

Um die Zahl der Ausfälle und die Systemunklarzeit gering zu halten, müssen Lieferant und Käufer in allen Phasen des Systemlebenszyklus zusammenarbeiten. Dadurch entstehen bei beiden Vertragspartnern verschiedene Verpflichtungen, die festgelegt werden sollten. Ein formales Zuverlässigkeits- und Instandhaltbarkeits-Managementprogramm (siehe IEC 60300-1) kann dabei helfen, diese Tätigkeiten zu bezeichnen und festzulegen.

Wo möglich, sollte festgelegt werden, dass Käufer bzw. Händler ihre Verantwortlichkeit anerkennen, die im Betrieb erfahrene Zuverlässigkeit zu berichten und diese Erkenntnisse (ob gut oder schlecht) ihren Lieferanten zurückzumelden.

4.6 Spezifikationsarten

Die Art des zu beschaffenden Systems hat grundlegende Wirkung auf die Art und Weise, in der die Spezifikation geschrieben wird. Es sind hauptsächlich drei Arten zu unterscheiden:

- Vom Lieferanten geschriebene Spezifikationen:
Dies ist meistens bei Systemen der Fall, die bestimmte Zuverlässigkeitsmerkmale erfüllen müssen, wie zum Beispiel die Funktionsfähigkeit, um vom Markt angenommen zu werden.
- Vom Käufer geschriebene Spezifikationen:
Dies ist meistens für genormte Systeme der Fall, die bestimmte Zuverlässigkeitsmerkmale erfüllen müssen, um den Ansprüchen des Käufers zu genügen.
- Vom Lieferanten und vom Käufer gemeinsam vereinbarte oder geschriebene Spezifikationen:
Dies ist üblicherweise bei Systemen der Fall, die speziell für den Kunden hergestellt werden, oder bei Änderungen an bestehenden Konstruktionen.

Bei nach Kundenwünschen hergestellten Systemen legt der Käufer fest, was er benötigt, und der Lieferant konzipiert, entwickelt und fertigt ein System einzig und allein, um diese Spezifikationen zu erfüllen. Wenn der Lieferant jedoch angibt, welche Systeme verfügbar sind, und der Käufer ein System daraus auswählt, das am besten seinen Anforderungen entspricht, spricht man von handelsüblichen oder marktüblichen Produkten (COTS, en: commercial off the shelf). In diesem Fall gibt es keine Änderungen am handelsüblichen System. In der Praxis bestehen die großen Beschaffungen meistens aus einer Kombination von nach

Kundenwünschen hergestellten und handelsüblichen Elementen, und die Spezifikation wird zwischen Käufer und Lieferant vereinbart.

Beispiele von nach Kundenwünschen hergestellten Systemen sind militärische Beschaffungen von Kampfpanzern (dabei werden viele Subsysteme lediglich in Militärfahrzeugen verwendet) oder die Errichtung von Kernkraftwerken. Beispiele handelsüblicher Systeme sind Haushaltswaschmaschinen oder IT-Systeme für das Büro.

Bei nach Kundenwünschen hergestellten Systemen spezifiziert der Käufer Ausmaß und Art der vom Lieferanten bereitzustellenden Verifizierung und Validierung, mit denen dieser die Erfüllung der Anforderungen nachweisen kann. Zu dieser Verifizierung und Validierung gehören Prüfungen und analytische Beweise. Da das System jedoch einzig und allein für den Käufer gebaut wird, kann außer nach erfolgter Auslieferung kein Beweis aus der Anwendung des Systems unter Einsatzbedingungen beigebracht werden. Der Lieferant berücksichtigt dann die Kosten der Verifizierung und Validierung in seiner Preiskalkulation, und der Käufer kann den erforderlichen Nachweis in Abhängigkeit des von ihm annehmbaren Geschäftsrisikos festlegen. Allerdings weiß der Käufer auch, dass das System für ihn entworfen und entwickelt wird, um seine Anforderungen zu erfüllen.

Bei einem handelsüblichen System gibt der Lieferant an, was verfügbar ist, und kann allgemeine Angaben zur erreichbaren Zuverlässigkeit des Systems machen. Dazu können auch Betriebsdaten aus früheren Anwendungen zählen. Für die Verifizierung und Validierung gibt es dabei allerdings nur wenig Gelegenheit, und viele Lieferanten werden kaum geneigt sein, aus ihrer Sicht kommerziell relevante Daten offenzulegen.

In Folge der geringeren Entwicklungsaufwendungen und der eingeschränkten Verifizierungs- und Validierungsaktivitäten sind die Kosten für handelsübliche Systeme viel niedriger als bei nach Kundenwünschen hergestellten Systemen. Aus diesem Grund geben neuerdings viele Käufer an, dass sie ihre Anforderungen mit handelsüblichen Systemen erfüllt sehen möchten. Dabei nehmen sie in Kauf, dass ihre Anforderungen nicht ganz genau erfüllt werden.

Wenn der Käufer jedoch irgendwelche Änderungen des handelsüblichen Systems fordert, wird es nicht mehr handelsüblich sein, da die Änderungen erhebliche Auswirkungen auf die erreichte Zuverlässigkeit haben können. Der Käufer muss daher sorgfältig darauf achten, dass er das handelsübliche System unverändert erhält und dass der bereitgestellte Nachweis für dieses System zutreffend und angemessen ist. Sollten Änderungen gewünscht werden, so müssen deren Auswirkungen auf die erreichte Zuverlässigkeit im Einzelnen berücksichtigt werden. Der Käufer muss dann gegebenenfalls eine zusätzliche Verifizierung und Validierung fordern und bezahlen.

4.7 Herleitung von Zuverlässigkeitsspezifikationen

Soweit möglich, sollten sämtliche Anforderungen an die Funktionsfähigkeit, die Instandhaltbarkeit und die Verfügbarkeit quantitativ festgelegt werden. Es könnte jedoch angebracht sein, Anforderungen in der Spezifikation auch qualitativ festzulegen. Quantitative Anforderungen ergeben nur dann Sinn, wenn sie während des Verifizierungs- und Validierungsprozesses gemessen werden können. Wenn die Anforderungen während des Nachweisprozesses nicht gemessen werden können, so handelt es sich um Zielsetzungen. Zur Erbringung des Nachweises sollten damit qualitative Vorgaben als Grundlage herangezogen werden.

Die Anforderungen müssen erreichbar sein. Eine Zuverlässigkeit von 100 % mag zwar wünschenswert sein, lässt sich aber nicht erreichen. Hohe Anforderungen an die Zuverlässigkeit können unangemessen hohe Kosten mit sich bringen. Der Käufer muss daher beurteilen, welche Werte der verschiedenen Zuverlässigkeitsmaßgrößen vernünftig sind. In diese Beurteilung können früher gesammelte Erfahrungen mit ähnlichen Systemen, die gewünschte Leistung und eventuell zu erwartende Verbesserungen mit einfließen. Aktuelle Systeme werden immer komplexer und können die gewünschte Funktionalität nicht mehr erreichen. Viele dieser Systeme haben die Grenze wirtschaftlich vertretbarer Aufwendungen für die Zuverlässigkeit erreicht.

Daten aus früher gesammelten Betriebserfahrungen sind aus mehreren Quellen verfügbar, zum Beispiel:

- a) Aufzeichnungen des Lieferanten über Instandhaltung und Wartung des Systems;
- b) Herstellerdaten zu Subsystemen und Komponenten;
- c) allgemeine Datenquellen und Datenbücher.

Spezifikationen zu Sicherheits- und Umgebungsbedingungen sind zwar nicht unmittelbar in dieser Anleitung enthalten, aber viele Hinweise aus dieser Norm lassen sich auch auf Sicherheits- und Umgebungsbedingungen anwenden. Falls sich also Zuverlässigkeitsanforderungen auch auf die Sicherheit und die Umgebung beziehen, sollten die betreffenden Sicherheits- und Umgebungsanforderungen in die Zuverlässigkeitsanforderungen aufgenommen oder in diesen referenziert werden.

5 Zuverlässigkeitsspezifikationen von Systemen

5.1 Systemspezifizierungs-Prozess

Beim Systemspezifizierungs-Prozess wird davon ausgegangen, dass Eingaben zur Marktsituation für die Systemdefinition vorliegen und die damit im Zusammenhang stehenden Bedingungen für die Erreichung des Systemziels bereitgestellt wurden. Zu Beginn des Prozesses steht die Bezeichnung des Systems und die Entwicklung der notwendigen Anforderungen. Dies führt dann zur funktionsbezogenen Spezifizierung der Zuverlässigkeit.

Bild 3 zeigt eine Übersicht des Systemspezifizierungs-Prozesses. Es bezeichnet die Abfolge der Prozessaktivitäten sowie die Ergebnisse der Systemzuverlässigkeitsaktivitäten im Systemspezifizierungs-Prozess. Die Prozessaktivitäten der *Systembezeichnung* anhand der Definition der Anforderungen beruhen auf dem Bedarf der Benutzer und auf den Beschränkungen der Systemanwendungen. Die Prozessaktivitäten der *Anforderungsanalyse* übertragen die Sicht der Benutzer auf Systemanwendungen auf eine technische Sicht zur Systementwicklung. Anhand der Prozessaktivitäten des *Strukturentwurfs* wird eine Lösung erstellt, welche durch Bezeichnung der erforderlichen Funktionen die Systemanforderungen bei bestimmten Betriebsszenarien erfüllt. Die Prozessaktivitäten im Bereich *Funktionsentwurf und -bewertung* bestimmen die praktischen Maßnahmen zur Umsetzung der Funktionen, damit der Entwurfsvergleich und die Optimierung ermöglicht werden. Die Prozessaktivitäten der *Systementwurfsdokumentation* stellen die Systemdaten für den Systementwurf bereit, einschließlich der Zuverlässigkeitsdaten. Der detaillierte Prozess für die technische Zuverlässigkeit von Systemen ist in IEC 60300-3-15 beschrieben.

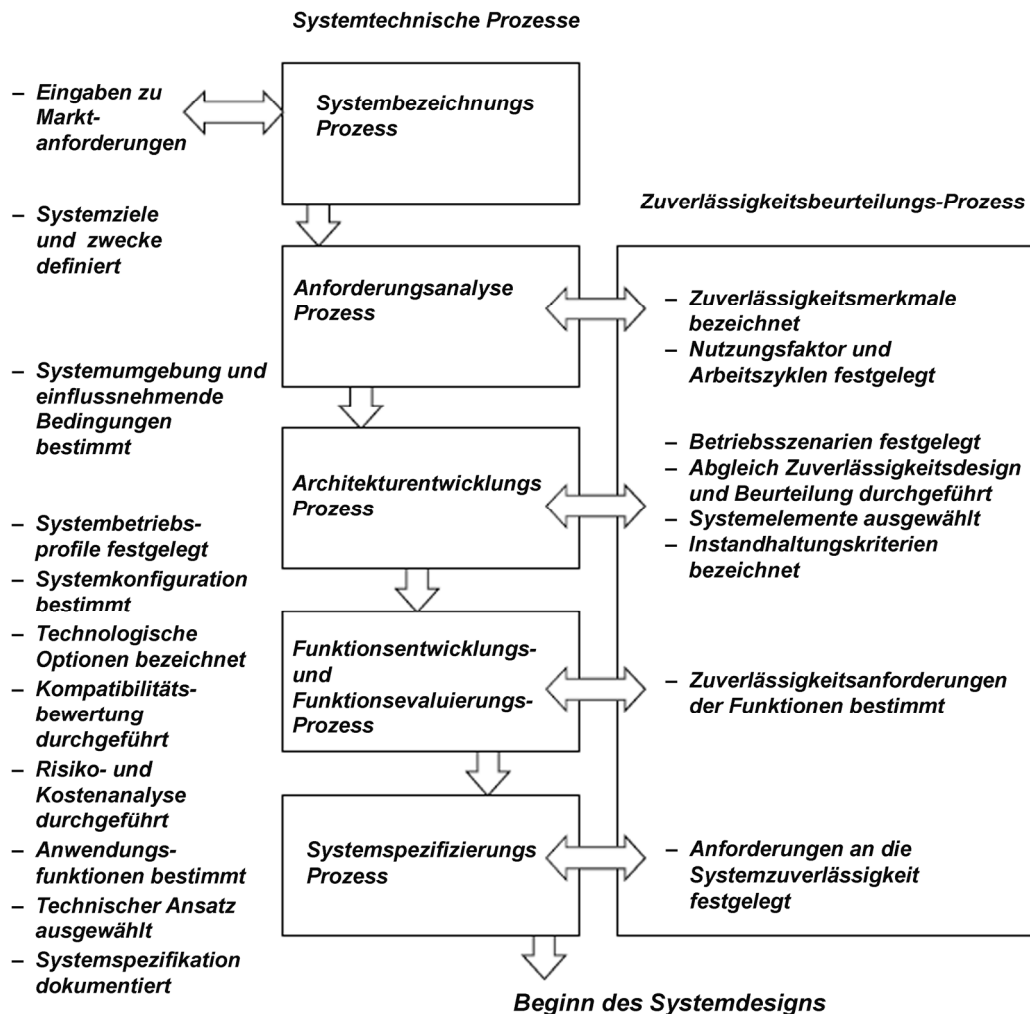


Bild 3 – Übersicht des Systemspezifizierungs-Prozesses

5.2 Spezifizierung der Systemzuverlässigkeit

Im Sinne der Bemühungen um den Systementwurf sollte die Spezifizierung der Systemzuverlässigkeit ein fester Bestandteil des Systemspezifizierungs-Prozesses darstellen. Die Zuverlässigkeitsaktivitäten sollten zeitgleich mit dem systemtechnischen Prozess durchgeführt werden, damit eine zeitnahe Koordination und Zusammenarbeit gewährleistet sind.

Die Spezifikation der Systemzuverlässigkeit ist die Zuordnung von Zuverlässigkeitsanforderungen zu jeder relevanten zuverlässigkeitsbezogenen Funktion des Systems. Je nach Systemkonfiguration, Betriebsmodus und anwendbaren einflussnehmenden Bedingungen kann die Zuverlässigkeitsspezifikation unterschiedlich ausfallen. Die Spezifikation stellt ein Gerüst aus Zuverlässigkeitsanforderungen der relevanten Systemfunktionen und entsprechende Merkmale für die Einleitung des Systementwurfs bereit.

Im Hinblick auf das System selbst bezeichnen die Systemanforderungen die Leistung des Systems und die Systemspezifikationen dessen Inhalte. Die Anforderungen sind wesentliche Voraussetzungen, die sich in den Vereinbarungen eines Vertrags wiederfinden müssen. Eine Spezifikation stellt eine präzise Aussage über die Anforderungen dar. Neben weiteren Zwecken gilt eine Spezifikation allgemein als Grundlage für das eindeutige Verständnis der Anforderung durch die Vertragsparteien. Anforderungen sind die Grundlage des Vertragszwecks bei Geschäftsvereinbarungen.

Bild 3 zeigt außerdem die Beziehungen der verschiedenen Prozessaktivitäten bei der Systemspezifikation, einschließlich der im Rahmen der Zuverlässigkeitsbewertung festgelegten Werte für Zuverlässigkeitsanforderungen.

5.3 Bestimmung der Zuverlässigkeitswerte

Zuverlässigkeit ist ein umfassender Begriff für die Verfügbarkeitsleistung und ihre Einflussfaktoren Funktionsfähigkeit, Instandhaltbarkeit und Unterstützbarkeit. Der Begriff Zuverlässigkeit ist ein qualitativer Begriff für allgemeine Beschreibungen. Er ist nicht als einzelne Maßgröße quantifizierbar. Zur Charakterisierung der Zuverlässigkeit werden quantitative Maßgrößen verwendet und der Verfügbarkeit, der Funktionsfähigkeit, der Instandhaltbarkeit und der Unterstützbarkeit zugewiesen. Die Bestimmung der Werte für die Zuverlässigkeitsanforderungen kann anhand der Quantifizierung der anwendbaren Maßgrößen auf die relevanten Zuverlässigkeitsmerkmale erfolgen. Die folgenden Beispiele verdeutlichen die Interpretierbarkeit von Zuverlässigkeitswerten als quantitative Werte oder numerische Formate:

- Verfügbarkeit: Prozentsatz der Nutzungsdauer für die Zeit der Systemleistung bei angefordertem Betrieb, Ausfallhäufigkeit und Ausfalldauer;
- Funktionsfähigkeit: mittlere Betriebsdauer zwischen zwei Fehlern, ausfallfreie Betriebsdauer, Ausfallwahrscheinlichkeit;
- Instandhaltbarkeit: mittlere Reparaturzeit, Wiederherstellungszeit;
- Unterstützbarkeit: logistische Verzögerung, Umlaufzeit für die Ersatzteilbereitstellung.

Bei neu entwickelten Systemen oder Systemfunktionen werden die Zielwerte für die Zuverlässigkeit üblicherweise anhand von Marktdaten, Wettbewerbsanalysen, Kundenanforderungen, Datenbanken zu technischen Anwendungen und Analysen von Feldleistungsdaten bestimmt. Bei älteren Systemen werden die Zielwerte für die Zuverlässigkeit unter Umständen mithilfe von Feldleistungserfahrungen ermittelt.

5.4 Verfahrensschritte zur Bestimmung der Anforderungen an die Systemzuverlässigkeit

5.4.1 Allgemeines

Bild 4 zeigt die Verfahrensschritte zur Bestimmung der Anforderungen an die Systemzuverlässigkeit. Die folgenden Abschnitte beschreiben den Zweck und den Prozess jedes Schritts und gibt Hinweise zum Verfahren. 0 enthält ein Beispiel für die Entwicklung einer Systemzuverlässigkeits-Spezifikation.

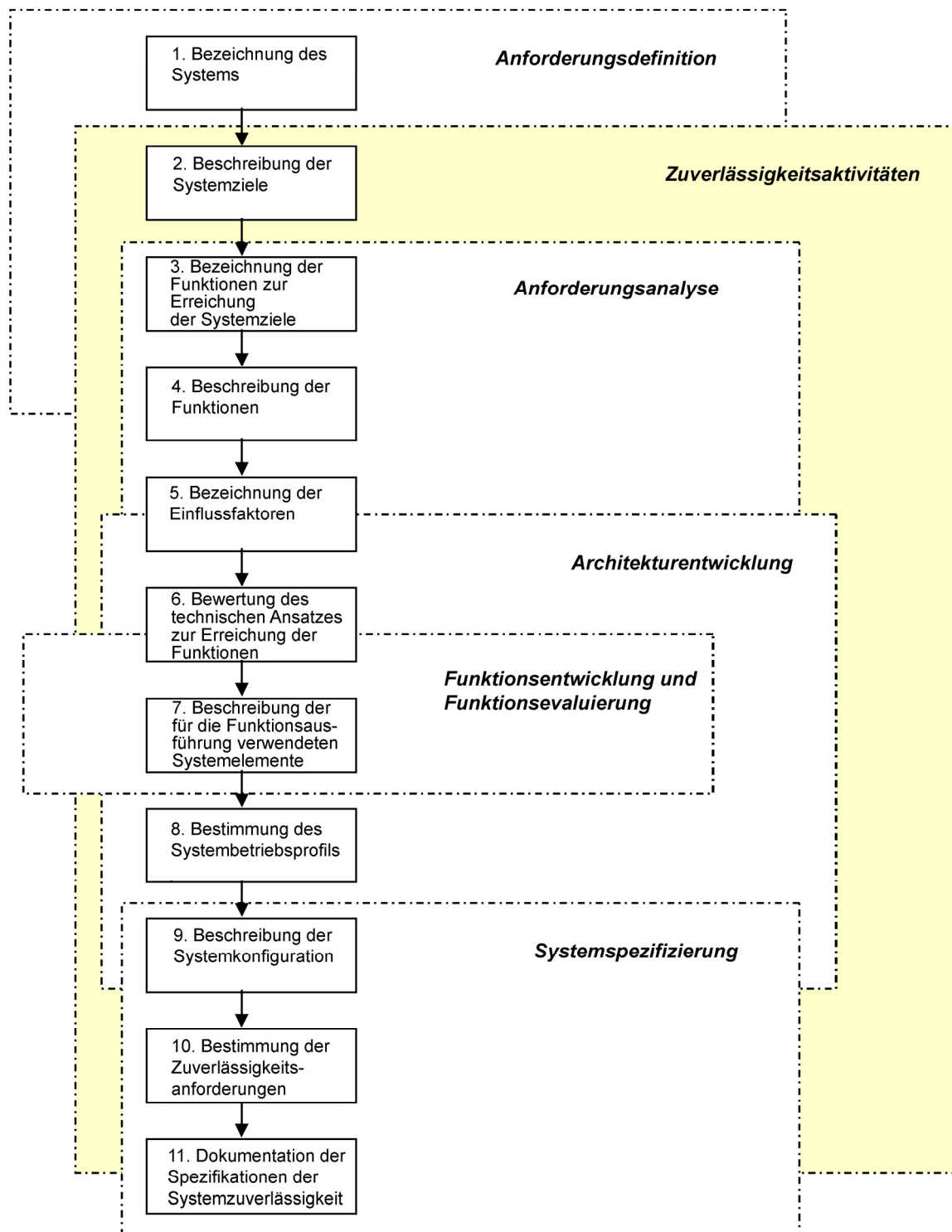


Bild 4 – Verfahrensschritte zur Bestimmung der Anforderungen an die Systemzuverlässigkeit

5.4.2 Bezeichnung des Systems

Das zu berücksichtigende System sollte bezeichnet werden. Die Systembezeichnung sollte den Namen, den Standort des Betriebs oder Einsatzes und den primären Anwendungszweck beinhalten.

5.4.3 Beschreibung der Systemziele

Der Zweck des Systems im Hinblick auf seine primäre Anwendung sollte angegeben werden. Außerdem sollten die zu erreichenden Betriebsziele beschrieben werden.

5.4.4 Bezeichnung der Funktionen zur Erreichung der Systemziele

Die zur Erreichung der Systemleistung erforderlichen Schlüsselfunktionen sollten bezeichnet werden. Im Hinblick auf die Systemanforderungen sollte der Zweck jeder Funktion angegeben werden. Ggf. sollten die Beziehungen dieser Funktionen untereinander festgelegt werden.

5.4.5 Beschreibung der Funktionen

Jede aus Sicht des Systems erforderliche bezeichnete Funktion sollte beschrieben werden, um einen Anwendungsbereich und eine Zielsetzung für die Bewertung der durchführbaren Realisierung dieser Funktion zu erhalten.

5.4.6 Bezeichnung der einflussnehmenden Bedingungen

Die auf jede Funktion einwirkenden Einflussfaktoren sollten bezeichnet werden, damit ihre Einflüsse auf die Systemleistung bewertet werden kann. Unter Verwendung von 0 als Leitlinie können die wesentlichen Einflussfaktoren aus der Matrix der auf die notwendigen Funktionen einwirkenden Beziehungen bezeichnet werden.

5.4.7 Bewertung des technischen Ansatzes zur Umsetzung der Funktionen

Der technische Ansatz zur Umsetzung der Funktionen sollte bewertet werden. Dabei geht es um die Bewertung der praktischen Maßnahmen, mit denen die Funktionen innerhalb der festgelegten Grenzwerte erreicht werden können. Der technische Ansatz befasst sich mit der Entwicklung und Aufrechterhaltung der im Sinne eines nachhaltigen Betriebs benötigten Funktionen unter den vorliegenden Kosten- und Zeitbeschränkungen.

5.4.8 Beschreibung der für die Funktionsausführung verwendeten Systemelemente

Die aus Hardware, Software und menschlicher Eingriffnahme in die Funktionen des Systembetriebs bestehenden Systemelemente sollten beschrieben werden. Dies sollte im Rahmen des technischen Systementwicklungs- und Systementwurf-Prozesses geschehen, um die praktikablen und kosteneffizienten Ergebnisse der Auswahl und des Erwerbs dieser Funktionen bestimmen zu können.

5.4.9 Bestimmung des Systembetriebsprofils

Das Betriebsprofil des System sollte bestimmt werden, um die unterschiedlichen Betriebsszenarien und die Aufgabenabläufe festzulegen, die unter den angegebenen Bedingungen zur Erreichung der Systemleistung erforderlich sind.

5.4.10 Beschreibung der Systemkonfiguration

Die mit jedem Betriebsszenario des Systembetriebsprofils einhergehende Systemkonfiguration sollte beschrieben werden. Die Beziehungen der einzelnen in einer Konfiguration vorgesehenen Funktionen sollte festgelegt werden, um den Systementwurfsvergleich und die entsprechende Beurteilung durchführen zu können. Sofern mehrere Systeme bei bestimmten Betriebsszenarien miteinander interagieren, sollten sie bezeichnet und ihre Grenzen und Schnittstellen bei der Systembewertung festgelegt werden.

5.4.11 Bestimmung der Zuverlässigkeitsanforderungen

Die Zuverlässigkeitsanforderungen der Systemfunktionen sollten anhand einer Bewertung des Systembetriebsszenarios und der Anforderungen an die spezifischen, im Evaluierungsprozess bezeichneten Funktionen festgelegt werden. Jedes mit einer der Schlüsselfunktionen im Zusammenhang stehendes Zuverlässigkeitsmerkmal sollte in einer qualitativen Bewertungsaussage in der spezifischen Ereignisabfolge des Betriebsprofils aufgeschlüsselt werden. Soweit möglich sollte auch ein quantitativer Wert zugewiesen werden. Dieser Charakterisierungsprozess stellt die Grundlage für die Erfassung der Zuverlässigkeitsspezifikation der Systemfunktionen zur Erfüllung der Zuverlässigkeitsziele dar.

5.4.12 Dokumentation der Systemzuverlässigkeits-Spezifikation

Die Systemzuverlässigkeits-Spezifikation und die relevanten erfassten Daten sollten dokumentiert werden. Die Zuverlässigkeitsanforderungen sollten Bestandteil der Systemspezifikation werden. Die Zuverlässigkeitsdaten sollten für die künftige Nutzung aufgezeichnet werden, damit sie im Sinne der Erreichung der allgemeinen Systemanforderungen als Eingabe für den Entwurf der betreffenden Funktionen dienen können. Die Inhalte der Dokumentation dienen darüber hinaus als Unterstützungsdaten für die Entwicklungsbewertung und die Produktrealisierung sowie für Systemverifizierungen und Modifikationen.

Als Bestandteil der Systemspezifikation sollte die Dokumentation der Systemzuverlässigkeits-Spezifikation die folgenden Angaben umfassen:

- Systembezeichnung;
- Systemziele;
- Systemfunktionen;
- Systembetriebsprofil;
- Systeminstandhaltbarkeit und Zugangsanforderungen für die Instandhaltung;
- Systemkonfiguration;
- Zuverlässigkeitsanforderungen jeder Funktion;
- Aussage zur Systemzuverlässigkeit.

6 Zuverlässigkeitsmanagement

Diese Norm behandelt die Festlegung der Zuverlässigkeitsanforderungen. Dabei wird mindestens ein Zuverlässigkeitselement spezifiziert, also Verfügbarkeit, Funktionsfähigkeit, Instandhaltbarkeit bzw. Unterstützbarkeit. Diese Maßgrößen sind inhärente Systemeigenschaften, und durch Verifizierung und Validierung kann der Grad ihrer wahrscheinlichen Erfüllung nachgewiesen werden. Durch andere Faktoren können jedoch die erreichbaren Werte dieser Maßgrößen beträchtlich unter die inhärent möglichen Werte gedrückt werden. In diesem Zusammenhang sind die Fertigungsqualität und die Instandhaltung des Systems als wesentlichste Faktoren zu nennen, die zu neuen Fehlzuständen im System führen können. Es ist daher unerlässlich, dass die Zuverlässigkeit während des Systemlebenszyklus aktiv geleitet und gelenkt wird. Dies erstreckt sich sowohl auf den Beschaffungsprozess als auch auf die Nutzung. Die betreffenden Managementaktivitäten sind je nach Phase verschieden. Wenn die Zuverlässigkeit nicht korrekt geleitet und gelenkt wird, steigt die Wahrscheinlichkeit, dass die Anforderungen an die Funktionsfähigkeit oder an die Verfügbarkeit nicht erreicht werden.

IEC 60300-1 und IEC 61160 enthalten detaillierte Angaben zu Aktivitäten und Verfahren für das Zuverlässigkeitsmanagement.

ANMERKUNG Es wird darauf hingewiesen, dass IEC 61160:2005 nicht alle Entwicklungsbewertungen berücksichtigt. IEC 62960 „Dependability reviews during the life cycle“ (Zuverlässigkeitsbewertungen während des Lebenszyklus – Entwurf) befasst sich mit Zuverlässigkeitsbewertungen während des gesamten Lebenszyklus.

Ein Systemlebenszyklus umfasst die folgenden Phasen:

- Konzeption;
- Entwicklung;
- Realisierung;
- Umsetzung;
- Erweiterung;
- Außerbetriebsetzung.

Jede Lebenszyklusphase weist ihre eigenen Zielsetzungen auf, die im Systementwurf-Prozess zu erreichen sind, wie beispielsweise die Einschränkung des Zugangs zu Instandhaltungsfunktionen während der Nutzung oder wiederverwendbare Teile zur Erleichterung der Außerbetriebsetzung. Für jede Phase sind außerdem

unterschiedliche interne Verfahren und Arbeitsanweisungen erforderlich sowie verschiedene vertragliche Bedingungen, die zu erfüllen sind. Mit der Definition der Systemanforderungen und der Entwicklung der Systemlösungen während der Konzeptions- und der Entwicklungsphase ergeben sich in nachfolgenden Phasen unter Umständen Änderungen bei der Systemnutzung. Entscheidungen zur Systemarchitektur und Auswahl bestimmter Technologien beim Systementwurf können sich auf die Realisierung, die Systemintegration und die Erweiterungsarbeiten auswirken und den Prozess der Außerbetriebsetzung beschränken.

Während der Konzeptions- und Entwicklungsphase des Systemlebenszyklus konzentriert sich die Zielsetzung des Entwurfs auf die Realisierung der Funktionen, mit denen die Systemleistung während der Nutzung erreicht werden soll. Die Zuverlässigkeitsanforderungen der Systemfunktion können erst dann bestimmt werden, wenn die Funktionen im Rahmen des Systementwurf-Prozesses bezeichnet wurden. Bei den meisten Systemen mit einem allgemeinen Betriebsmuster wird für alle Funktionen die Einhaltung bestimmter Zuverlässigkeitsanforderungen gefordert, damit der Betrieb des Systems aufrecht erhalten werden kann. Das bedeutet, dass während des Betriebs alle Systemfunktionen benötigt werden, um die beabsichtigte Systemleistung jederzeit entweder dauerhaft oder unmittelbar auf Abruf gewährleisten zu können.

Bei bestimmten Betriebsvorgängen werden die Zuverlässigkeitsanforderungen unter Umständen nur von einer Untergruppe der Systemfunktionen gefordert, damit eine erfolgreiche Systemleistung während dieses Betriebs erreicht werden kann.

BEISPIEL Die Verfügbarkeit der Fahrwerksfunktionen eines Luftfahrzeugs bei Start und Landung.

Das Anwendungsverfahren zur Angabe der Systemzuverlässigkeit umfasst die Unterscheidung zwischen den Funktionen, die sich auf die Systemzuverlässigkeit auswirken, und denen, die dies nicht tun.

Zur Entwicklung der Anforderungen für die Angabe der Systemzuverlässigkeit ist eine Beschreibung des Betriebsprofils erforderlich. Erreicht wird dies durch eine Bewertung der zuverlässigkeitsbezogenen Funktionen, zu denen eine Analyse der einflussnehmenden Bedingungen zählt, die sich auf die ausgewählten Zuverlässigkeitsmerkmale auswirken.

Der Systemlebenszyklus kann eine signifikante Auswirkung auf die vom System erreichte Zuverlässigkeit haben. So können etwa schlechte Handhabung oder ausgedehnte Lagerperioden die Funktionsfähigkeit eines Systems beträchtlich verschlechtern. Auch kann sich die Funktionsfähigkeit über die Lebenszeit verändern. Viele Systeme zeigen dabei aufgrund verschleißender Bauelemente oder Subsysteme eine sich ändernde Ausfallrate. Die sich mit der Anwendung eines Systems verändernde Funktionsfähigkeit bedeutet für viele Systeme, dass es ein Fehler ist, eine konstante Ausfallrate anzunehmen. Demzufolge müssen andere Wahrscheinlichkeitsverteilungen mit komplexeren mathematischen Verfahren zur Vorhersage der Zuverlässigkeit verwendet werden. IEC 61649, IEC 61703 und IEC 61710 enthalten hierzu weitere Anleitungen.

Änderungen der Systemnutzung sind ein weiterer Faktor mit Auswirkungen auf die Zuverlässigkeit und müssen daher im Rahmen des Zuverlässigkeitslebenszyklus auf jeden Fall überwacht, geleitet und gelenkt werden.

BEISPIEL So wird beispielsweise ein Fahrzeug, das üblicherweise auf der Straße fährt, mit großer Wahrscheinlichkeit häufiger ausfallen, wenn es im Gelände gefahren wird, da dort härtere Beanspruchungen und Belastungen auf das Fahrzeug einwirken.

7 Verfügbarkeit

7.1 Allgemeines

7.1.1 Wahl der Zuverlässigkeitsmerkmale

Bei einigen Systemen, insbesondere bei solchen mit höherer Komplexität, müssen Funktionsfähigkeit und Instandhaltung gemeinsam betrachtet werden. Bei solchen Systemen könnte es daher angebracht sein, auf Systemebene anstelle von getrennten Anforderungen an die Funktionsfähigkeit und an die Instandhaltbarkeit eher Anforderungen an die Verfügbarkeit zu stellen. Der Käufer sollte auf jeden Fall festlegen, welche Maßgröße für die Verfügbarkeit spezifiziert werden soll, da ansonsten die Gefahr besteht, dass die

erforderliche Verfügbarkeit nicht erreicht wird. Die gebräuchlichste Maßgröße ist die stationäre Verfügbarkeit, es kann jedoch auch die mittlere Verfügbarkeit geeignet sein.

BEISPIEL 1 Im Eisenbahnsektor wollen Zugbetreiber einen bestimmten Prozentsatz der Züge für Spitzenzeiten oder für Zeiten mit erheblichen Verspätungen bereithalten.

BEISPIEL 2 In der Telekommunikationsbranche benötigen die Betreiber eine bestimmte Anzahl von Kommunikationskanälen verfügbar, damit das System insgesamt verfügbar bleibt, auch wenn einige Leitungen unter Umständen nicht zur Verfügung stehen.

Übliche Definitionen für Verfügbarkeit sind:

- Die stationäre Verfügbarkeit ist „der Mittelwert der momentanen Verfügbarkeit unter stationären Bedingungen während eines gegebenen Zeitintervalls“. Damit diese Definition der Verfügbarkeit zutrifft, müssen stationäre Bedingungen herrschen. Da bei solchen Bedingungen mathematisch einfacher vorgegangen werden kann, wird manchmal die stationäre Verfügbarkeit spezifiziert, obwohl dem so nicht ist.
- Momentane Verfügbarkeit ist „die Wahrscheinlichkeit, eine Einheit zu einem gegebenen Zeitpunkt in einem Zustand anzutreffen, in dem sie eine geforderte Funktion unter gegebenen Bedingungen erfüllen kann, vorausgesetzt, dass die erforderlichen äußeren Mittel bereitgestellt sind“. Solch eine Anforderung wird vermutlich in einer Zuverlässigkeitsspezifikation eher nicht festgelegt werden.
- Mittlere Verfügbarkeit ist „der Mittelwert der momentanen Verfügbarkeit während eines gegebenen Zeitintervalls (t_1, t_2)“. Diese Maßgröße ist eher für Spezifikationen geeignet und hat in Bereichen Bedeutung, in denen die Verfügbarkeit in unterschiedlichen Zeitintervallen etwa aufgrund unterschiedlicher Betriebsbedingungen variieren kann.

Es gibt noch weitere Definitionen für die Verfügbarkeit, wie etwa die betriebliche Verfügbarkeit (mit Berücksichtigung logistischer Verzugsdauern) und die asymptotische Verfügbarkeit (siehe IEC 60050-192).

7.1.2 Beziehung zwischen Verfügbarkeit, Funktionsfähigkeit und Instandhaltbarkeit

Verfügbarkeit, Funktionsfähigkeit und Instandhaltbarkeit sind keine voneinander unabhängigen Maßgrößen, sondern sind bei einem reparierbaren System durch folgende Beziehung miteinander verbunden:

$$\text{Stationäre Verfügbarkeit} = \frac{\text{MUT}}{\text{MUT} + \text{MDT}}$$

Dabei ist

MUT = mittlere Klardauer;

MDT = mittlere Unklardauer.

Bei konstanter Ausfallrate und konstanter Reparaturrate, und nur in diesem Fall, sind die asymptotische Verfügbarkeit und die stationäre Verfügbarkeit identisch und werden dann oft mit „Verfügbarkeit“ bezeichnet. Diese mathematische Beziehung gilt nur bei diesen sehr speziellen Bedingungen, die aber häufig nicht zutreffen. Daher sollte diese Formel nur für eine erste Schätzung verwendet werden, und danach sollten detailliertere und genauere Bewertungen der Verfügbarkeit durchgeführt werden.

Es sollten nicht alle drei Zuverlässigkeitsmaßgrößen gleichzeitig festgelegt werden, da dadurch die Systemzuverlässigkeit eingeschränkt würde. Üblicherweise werden jedoch zwei dieser drei Maßgrößen festgelegt, um so ein betrieblich akzeptables Gleichgewicht zwischen Klardauer und Unklardauer zu sichern. Durch hohe mittlere Klardauern bei langen Unklardauern oder alternativ durch niedrige mittlere Klardauern bei kurzen Unklardauern kann dieselbe Verfügbarkeit erreicht werden. Beispielsweise können Betriebssysteme von Arbeitsplatzrechnern (PC) oft ausfallen, benötigen aber für eine allgemeine hohe Verfügbarkeit nur wenig Zeit zum Wiederhochfahren. Dies ist aus Anwendersicht frustrierend, aber unter Umständen annehmbarer als ein bei gleicher Verfügbarkeit nur selten ausfallender Rechner, der dann danach allerdings für Tage nicht mehr nutzbar ist. Für Telekommunikationsnetze wäre allerdings eine niedrige Funktionsfähigkeit bei kurzen Unklardauern nicht akzeptabel, da dann für die Datenübertragung keine genügend lange unterbrechungsfreie Zeit zur Verfügung stünde.

7.2 Festlegung der Verfügbarkeit

7.2.1 Quantitative Anforderungen

Bei der Festlegung der Verfügbarkeit muss genau definiert werden, was darunter zu verstehen ist, also welche Verfügbarkeitsart spezifiziert wird, welche Zeiten in der Unklardauer enthalten sind, wie logistische Verzugsdauern behandelt werden und zu welchem Anteil.

Anforderungen an die Verfügbarkeit werden als Dezimalzahl kleiner eins oder als ein in Prozent angegebenes Verhältnis ausgedrückt, zum Beispiel als das Verhältnis von mittlerer Klardauer zur Beobachtungsdauer. Anforderungen an die Verfügbarkeit beziehen sich sowohl auf die Versagenshäufigkeit als auch auf die Unklardauer. Falls die mittlere Verfügbarkeit festgelegt wird, muss neben weiteren zeitlich relevanten Daten auch die Zeitperiode angegeben werden, über die sie zu messen ist.

BEISPIEL Wenn beispielsweise die mittlere Verfügbarkeit von Nahverkehrszügen festgelegt werden soll, so könnte man dafür die mittlere Verfügbarkeit pro Stunde annehmen, etwa montags bis freitags von 7 Uhr bis 10 Uhr und von 17 Uhr bis 20 Uhr.

Bei der Festlegung quantitativer Verfügbarkeitsanforderungen werden üblicherweise die Unklarzeiten kumuliert, die sich innerhalb eines bestimmten Zeitintervalls ereignen (zum Beispiel eines Monats oder eines Jahres). Falls Teile der Systemunklarzeit nicht vom Lieferanten zu verantworten sind (zum Beispiel logistische oder administrative Verzugsdauern), so sollte dies in der Spezifikation vermerkt und die Werte der jeweiligen Dauern angegeben werden. In IEC 60050-192, Bild 2, sind die verschiedenen Instandhaltungsdauern erläutert. Alternativ darf eine inhärente Verfügbarkeit festgelegt werden, indem man solche Dauern ausschließt.

Anhang D, Absatz D.2 führt Beispiele für quantitative Anforderungen an die Verfügbarkeit auf.

7.2.2 Qualitative Anforderungen

Qualitative Verfügbarkeitsanforderungen könnten aus einer Kombination von qualitativen Anforderungen an die Funktionsfähigkeit und die Instandhaltbarkeit zusammengesetzt sein, auf jeden Fall ist aber der Vorgabe quantitativer Verfügbarkeitsanforderungen der Vorzug zu geben, wo immer dies möglich ist. Qualitative Verfügbarkeitsanforderungen könnten dort die quantitativen Anforderungen ergänzen, wo die quantitativen Anforderungen nicht alle Gesichtspunkte der Spezifikation abdecken können. Ein Beispiel hierfür ist der Fall, wenn die Unklarzeit bei bestimmten Betriebsbedingungen kritisch ist. Jedoch müssen weiterhin die Art der Verfügbarkeit und die in der Unklarzeit berücksichtigten Zeiten in der Spezifikation festgelegt werden.

7.3 Verifizierung und Validierung der Verfügbarkeit

7.3.1 Allgemeines

Die Spezifikation sollte die Notwendigkeit der Verifizierung und Validierung der geforderten Verfügbarkeit enthalten. Der Nachweis der erreichten Verfügbarkeit wird oft indirekt durch einen kombinierten Nachweis der Funktionsfähigkeit und der Instandhaltbarkeit bewiesen, seltener durch einen direkten Nachweis.

7.3.2 Verifizierung und Validierung durch Prüfung

Wenn die Verifizierung und Validierung durch eine Prüfung erfolgen soll, dürfen die in IEC 61070 genormten Prüfverfahren zum Nachweis einer stationären Verfügbarkeit verwendet werden. Wenn jedoch eine sehr hohe Verfügbarkeit (zum Beispiel $> 0,999$) gefordert wird, so muss beachtet werden, dass es hierbei sehr schwierig ist, einen sinnvollen Prüfplan zu erstellen. Eine Bewertung, Verifizierung und Validierung der Verfügbarkeit der Subsysteme kann hier hilfreich sein. Dies kann durch Beobachtung in der System- und Subsystemebene zusammen mit einem Modell der Systemverfügbarkeit erreicht werden. Dabei muss die Brauchbarkeit der Verfahren bewiesen werden, die zur Verifizierung und Validierung der geforderten hohen Verfügbarkeit benutzt werden.

Bei der Verifizierung während der Anwendung eines Systems sollte vorab ein detailliertes Datenerfassungsprogramm (siehe IEC 60300-3-2) vereinbart werden. Dabei sollten unter anderem die Unklarzeiten berücksichtigt werden, die durch Ausfälle der Geräte, Versagen der Software oder durch die

angewendeten Instandhaltungsverfahren entstehen. Die Durchführung der Prüfung sollte überwacht und analysiert werden, um den erforderlichen Nachweis erbringen zu können.

Falls mehr als eine Einheit vom selben Systemtyp als Prüflinge verwendet werden, sollte die Anzahl dieser Einheiten und die Beobachtungsdauer mit berücksichtigt werden. Es sollte außerdem eine Vorgehensweise vereinbart werden, nach der im Fall der Nichterfüllung der Vorgaben eine Nachbesserung vereinbart und durchgeführt und die Prüfung anschließend fortgesetzt wird. Bei der Verwendung von mehr als einem Prüfling sollte sorgfältig vorgegangen werden, da 100 Stunden eines Prüflings statistisch gesehen nur dann einer Stunde von 100 Prüflingen entsprechen, wenn eine Reihe von Faktoren berücksichtigt werden und gewisse Annahmen auch zutreffen. Zu diesen Annahmen gehören eine konstante Ausfallrate, das Ausbleiben von Früh- oder Abnutzungsausfällen und der Vertrauensgrad, dass die verwendeten Prüflinge für das System repräsentativ sind.

7.3.3 Verifizierung und Validierung durch Analyse

Ist die Verifizierung und Validierung durch Analyseverfahren zu erbringen, so können die genormten Vorhersagetechniken mit den detaillierten Analyseverfahren nach IEC 62308 und IEC 61709 angewendet werden.

Zahlenwerte für die Berechnungen müssen allgemein anerkannten Datenquellen entnommen werden oder aus Erfahrungen mit ähnlichen, bereits im Betrieb befindlichen Geräten, aus Prüfungen im Labor oder aus der Integration von Hardware und Software stammen. Die Daten sollten zwischen dem Lieferanten und dem Käufer vereinbart werden, die Datenquelle sollte dokumentiert sein.

8 Funktionsfähigkeit

8.1 Allgemeines

Bei einigen Systemen muss die Funktionsfähigkeit des Systems direkt betrachtet werden. Funktionsfähigkeit ist dabei häufig ein allgemeiner Begriff, der sowohl die eigentliche Definition als auch die Maßgrößen der Ausfallwahrscheinlichkeit bezeichnet. Bei solchen Systemen könnte es angebracht sein, für die Systemebene die Funktionsfähigkeit und die Instandhaltbarkeit getrennt festzulegen. Funktionsfähigkeit ist per Definition die Fähigkeit eines Systems, eine geforderte Funktion unter gegebenen Bedingungen für ein gegebenes Zeitintervall ohne einen Ausfall erfüllen zu können. Sie wird in den meisten Fällen richtigerweise durch die Wahrscheinlichkeit beschrieben, dass das System seine geforderte Aufgabe vollständig ausführen kann. In vielen Spezifikationen wird die geforderte Funktionsfähigkeit jedoch durch alternative Größen ausgedrückt, wie der mittleren Dauer bis zum Ausfall oder der mittleren Betriebsdauer zwischen zwei Ausfällen.

Beispiele für technische Bereiche, in denen die Funktionsfähigkeit das wichtigste Zuverlässigkeitsmerkmal ist, sind die Luftfahrt und die Automobilindustrie. In der Luftfahrt ist es unerlässlich, dass ein einmal gestarteter Flugzeug seinen Flug ohne einen Komplettausfall vollendet, beim Automobil will der Fahrer sein Ziel erreichen und erst dort gegebenenfalls das Fahrzeug warten.

Beispiele, bei denen die Dauer bis zum Ausfall die geforderte Maßgröße für die Funktionsfähigkeit sein kann, sind Glühlampen, die für eine bestimmte Lebensdauer konstruiert wurden. Zu den Beispielen, bei denen die Dauer zwischen Ausfällen das Maß sind, gehören Maschinen, die dauernd in Betrieb sind und bei denen die Dauer bis zum Ausfall bekannt sein muss, um die Instandhaltungsmaßnahmen planen zu können.

Der Käufer muss sorgfältig darauf achten, dass für die Funktionsfähigkeit eine geeignete Maßgröße spezifiziert wird und dass die statistischen Auswirkungen der Anforderung verstanden werden.

BEISPIEL Wenn zum Beispiel eine Funktionsfähigkeit von 99 % für ein Jahr festgelegt wird, so mag dies sinnvoll erscheinen. Jedoch entspricht dies bei konstanter Ausfallrate einer mittleren Betriebsdauer zwischen Ausfällen (MTBF) von 871 613 h (oder von mehr als 99 Jahren).

Die MTBF wird häufig als eine überholte Maßgröße für die Funktionsfähigkeit angesehen, die Änderungen durch eine sich wandelnde Systemnutzung unterliegt. Es wird daher empfohlen, an ihrer Stelle die Verfügbarkeit, die Funktionsfähigkeit oder die Ausfallwahrscheinlichkeit anzugeben. Bei nicht konstanten Ausfallraten können die Parameter der Weibull-Verteilung oder anderer zutreffender Verteilungen für die

Spezifikation verwendet werden (siehe IEC 61649). Bei nicht konstanter Ausfalldichte kann das Potenzgesetzmodell (siehe IEC 61164 und IEC 61710) herangezogen werden.

8.2 Festlegung der Funktionsfähigkeit

8.2.1 Quantitative Anforderungen

Quantitative Anforderungen an die Funktionsfähigkeit sind vorzuziehen und sollten vor Entwicklungsbeginn festgelegt werden. Wie bei statistischen Betrachtungen üblich, sollte bei der Festlegung von quantitativen Anforderungen auch das Vertrauen spezifiziert werden, mit dem die Anforderungen nachzuweisen oder anzugeben sind (siehe IEC 60605-4).

Der das System bestimmende Ausfallmechanismus muss frühzeitig in Betracht gezogen werden, da sich daraus ableitet, welche der Zuverlässigkeitsmaßgrößen geeignet und zutreffend sind. Sie unterliegen zudem einem Verschleiß, so dass die Annahme einer konstanten Ausfallrate nicht zutreffend ist. Elektrische Haushaltsglühlampen fallen in erster Linie entsprechend der Ein/Ausschalthäufigkeit und weniger entsprechend ihrer Brenndauer aus. Somit sind die Anzahl der Betätigungen oder die geleisteten Betriebsstunden die geeigneten Maßgrößen, und das System wird auf eine bestimmte Betriebsdauer hin konstruiert. Die Berücksichtigung redundanter Elemente ist ein weiterer Faktor bei der Wahl der Funktionsfähigkeitsmaßgröße.

BEISPIEL So fallen beispielsweise Fahrzeugmotoren entsprechend der Kilometerleistung des Fahrzeugs und weniger entsprechend ihrem Alter aus, so dass die gefahrenen Kilometer die geeignete Maßgröße sind.

Für jedes System müssen die geforderten Funktionsfähigkeitsmerkmale und die zugehörigen Maßgrößen ausgewählt und festgelegt und ihnen jeweils quantitative Anforderungen zugewiesen werden. Bei der Festlegung quantitativer Anforderungen an ein System sollten folgende Angaben gemacht werden:

- Anwendung oder Einsatzprofil des Systems;
- Ausfallkriterien oder Definition eines Ausfalls, d. h., die Angabe, was bei einem bestimmten System bei der beabsichtigten Anwendung einen Ausfall darstellt;

ANMERKUNG Ein Ausfall kann auf verschiedene Arten über die sich ergebenden Folgen definiert werden. Dies kann beispielsweise der Ausfall einer Dienstleistung oder die Notwendigkeit zur Instandsetzung sein (siehe auch 0).

- Betriebsbedingungen;
- Umgebungsbedingungen;
- die zum Nachweis der Übereinstimmung mit den Anforderungen beabsichtigten Verfahren.

Ohne solche Angaben wäre die Festlegung einer Maßgröße wie $R(t)$, $F(t)$, MTTF, MTBF, Anzahl der Ausfälle in einem Zeitintervall oder von Parametern der Weibull- oder Potenzgesetzverteilung bedeutungslos.

Bei der Wahl des Werts der festzulegenden Maßgröße zur Beschreibung der Funktionsfähigkeit sollten die folgenden Faktoren beachtet werden:

- durch den Stand der Technik erzwungene Einschränkungen sowie Art und Komplexität des Systems;
- Erfahrungen des Käufers mit dem Betrieb und der Instandhaltung dieser Art von System;
- Durchführbarkeit der Verifizierung der festgelegten Anforderungen;
- die Zuverlässigkeitswerte der Einheiten, Bauelemente usw., aus denen das System gefertigt werden kann;
- die Kosten für Entwicklung, Fertigung sowie Verifizierung und Validierung des Systems mit einem vorgegebenen Maß für die Funktionsfähigkeit.

Falls sich bei der Entwicklung eines Projekts herausstellt, dass die zugrunde liegenden Annahmen nicht gelten, so müssen die Funktionsfähigkeitsanforderungen unter Umständen neu überdacht und geändert werden. Falls die Spezifikation geändert werden muss, so sollte dies für beide involvierte Parteien einvernehmlich geschehen.

Die quantitativen Anforderungen sollten eindeutig und in einer Form festgelegt werden, die einen Vergleich mit später erhaltenen Ergebnissen zulässt.

Falls der Nachweis der quantitativen Anforderungen durch Prüfung erbracht werden soll, sollte auch das geforderte Vertrauensniveau oder der zu verwendende Prüfplan festgelegt werden. Falls ein Prüfplan festgelegt wird, sollten darin eine Aussage zur Prüfdauer sowie Annahme- und Rückweiskriterien enthalten sein.

Es gibt mehrere Arten von Nachweisprüfungen. Allerdings sollte normalerweise Folgeprüfplänen (siehe IEC 61123 und IEC 61124) der Vorzug gegenüber Prüfungen mit fester Ablaufzeit oder fester Anzahl von Prüflingen gegeben werden, da die erstgenannten Prüfungen effizienter sind. Wenn die Maßgröße der Funktionsfähigkeit bekannt ist oder sich im Laufe der Zeit wahrscheinlich ändert, so sollte die Zuverlässigkeit beispielsweise auf folgende Weise angegeben werden:

- Weibull-Parameter bei nicht reparierbaren Systemen (siehe IEC 61649);
- Potenzgesetz-Parameter bei reparierbaren Systemen (IEC 61164 und IEC 61710);
- mittlere Ausfalldichte über eine gegebene Zeit.

IEC 60300-3-5 enthält Informationen zu statistischen Verteilungen. Anhang D, Absatz D.3 führt Beispiele für quantitative Anforderungen an die Funktionsfähigkeit auf.

8.2.2 Qualitative Anforderungen

Qualitative Anforderungen an die Funktionsfähigkeit können vorgegeben werden sowohl durch

- Kriterien zum Entwurf des Systems als auch durch
- Maßnahmen zur Verbesserung der Zuverlässigkeit, die während der einzelnen Phasen des Systemlebenszyklus durchzuführen sind.

Entwurfskriterien an ein System, zum Beispiel Anforderungen an die Konstruktion, an die Leistung und an den Betrieb, stehen meist für sich alleine. Sie könnten aber auch quantitative Anforderungen an die Funktionsfähigkeit ergänzen. Durch sie können indirekt Vorgaben zur Funktionsfähigkeit des Systems, zu dessen Installation und zur Überwachung seiner Leistungsmerkmale festgelegt werden. Beispiele hierfür sind:

- ausschließendes Fehlzustandskriterium, d. h., das System muss so beschaffen sein, dass kein Fehlzustand alleine zu einem kritischen Zustand des Systems führen kann;
- kumulierendes Fehlzustandskriterium, d. h., das System muss so beschaffen sein, dass kein unerkannter Fehlzustand in Kombination mit weiteren Fehlzuständen zu einem Systemausfall führen kann;
- Pfadtrennung, d. h., die Unabhängigkeit redundanter Subsysteme muss durch getrennte Pfade für Verkabelung, Rohrleitungen, Signalisierungskanäle, Energieversorgung und andere Versorgungsleitungen aufrechterhalten werden;
- Überwachung kritischer Funktionen, d. h., es muss dafür gesorgt werden, dass kritische Funktionen dauernd oder in Intervallen automatisch oder manuell geprüft werden, um einen festgelegten Wert der Funktionsfähigkeit sicherzustellen.

Zusätzlich zur Festlegung quantitativer Anforderungen an die Funktionsfähigkeit kann es häufig angebracht sein, eine Abfolge von Maßnahmen zur Verbesserung der Zuverlässigkeit (und Instandhaltbarkeit) vorzugeben, die während der einzelnen Phasen des Systemlebenszyklus umzusetzen sind. Solche qualitativen Vorgaben können sich auf Hardware, auf Software oder auf logistische Mittel beziehen. Diese Maßnahmen sind besonders dann wichtig, wenn die Funktionsfähigkeit des Systems durch die quantitativen Vorgaben nicht ausreichend genau beschrieben ist. Sie sollten zwischen Käufer und Lieferant einvernehmlich festgelegt werden. Dies bezieht sich sowohl auf die technischen Sachverhalte als auch auf die zeitliche Planung und auf die Kosten solcher Maßnahmen. Solche qualitativen Vorgaben sollten mittels eines Zuverlässigkeitsprogrammplans nach IEC 60300-1 formal aufgestellt und die notwendigen Aufgaben entsprechend diesem Plan durchgeführt werden.

Der Zuverlässigkeitsprogrammplan sollte auf die Art des Systems und auf die festgelegten Anforderungen zugeschnitten sein. Üblicherweise enthält er die folgenden Aufgaben:

- die anzuwendenden Analyseverfahren;
- ein Zuverlässigkeitswachstumsprogramm, sofern erforderlich (siehe IEC 61014);
- Angaben zur Verifizierung der Konformität in Bezug auf die Anforderungen (siehe IEC 60300-3-5) oder jeder anderen qualitativen oder quantitativen Maßgröße, mit der der Grad der Konformität mit den Anforderungen angegeben werden kann;
- Kriterien zur Bauelementeauswahl und Hinweise zum Qualitätsnachweis;
- „Worst case“-Analysen.

8.3 Verifizierung und Validierung der Funktionsfähigkeit

8.3.1 Allgemeines

In der Spezifikation sollten die Verfahren angegeben werden, mit denen die Erfüllung der Anforderungen nachgewiesen werden kann.

Die Funktionsfähigkeit kann entweder durch eine Analyse während der Entwicklung und vor der Fertigung verifiziert und validiert werden oder durch Prüfungen im Labor, durch Erprobungen nach der Fertigung oder durch eine Bewertung des Betriebsverhaltens nach der Auslieferung. Andere Tätigkeiten während des Entwicklungsprozesses können eine zusätzliche Verifizierung und Validierung erbringen. Beispiele hierfür sind Entwurfsanalysen (wie etwa Belastungsanalysen), Leistungsprüfungen, Softwaretests und Betriebssimulationen. Aus allen Quellen können Hinweise für eine Verifizierung und Validierung erfasst werden und so die eigentliche Zuverlässigkeitsverifizierung und -validierung ergänzen.

8.3.2 Verifizierung und Validierung durch Prüfung

Die bevorzugten Verfahren der Verifizierung und Validierung der Funktionsfähigkeit durch Prüfung werden üblicherweise im gegenseitigen Einvernehmen von Käufer und Lieferant ausgewählt. Zu diesen Verfahren zählen:

- Erfassung und Auswertung von Ausfalldaten von im Betrieb befindlichen Systemen, d. h. in der tatsächlichen Anwendung (siehe IEC 60300-3-2 und IEC 60605-6). Um gültig zu sein, müssen jedoch ausreichend Daten erfasst werden, und falls ein hohes Nachweismaß gefordert wird, können diese Daten für den Beschaffungsprozess zu spät vorliegen.
- Prüfungen an Systemen in der Anwendung oder im Labor unter Verwendung der Verfahren zum Nachweis oder zur Bestimmung nach IEC 60300-3-5, IEC 61123, IEC 61124, IEC 61649 oder IEC 61710. Falls Laborprüfungen spezifiziert werden, müssen die damit einhergehenden Kosten und die benötigte Zeit beachtet werden.

Prüfungen sollten derart gestaltet werden, dass sie die erwartete betriebliche Anwendung und die dabei herrschenden Umweltbedingungen und Belastungen, denen das System ausgesetzt sein wird, widerspiegeln. Andernfalls wird das Prüfergebnis nicht die künftig vom System erreichte Zuverlässigkeit reflektieren.

Es sollten präzise Kriterien festgelegt werden, damit Ausfälle der Geräte, Versagen der Software usw. in relevante und nicht relevante Ereignisse eingeteilt werden können. Diese Klassenbildung ist die Grundlage für Annahme- und Rückweiskriterien, deren klare und genaue Festlegung vor Prüfbeginn unerlässlich ist. Die Klassen sollten vorzugsweise früh im Lebenszyklus gebildet werden, damit es keinen Argwohn geben kann, ob die Ergebnisse etwa so angepasst wurden, dass sie das gewünschte Ergebnis erbringen. Es kann andererseits jedoch möglich sein, dass nicht alle Prüfkriterien rechtzeitig festgelegt werden können und dies erst später im Lebenszyklus oder der Produktentwicklung möglich sein wird.

Die Verifizierung und Validierung der Funktionsfähigkeit muss getrennt für instand zu setzende und für nicht instand zu setzende Systeme erfolgen.

IEC 61123 enthält Einzelheiten zu Prüfungen, die durchgeführt werden können, falls der Erfolgsquotient als Maß für die Funktionsfähigkeit verwendet wird. IEC 61124 beschreibt Prüfpläne, falls Ausfallrate und Ausfalldichte zeitlich konstant sind. Die Annahme einer konstanten Ausfallrate oder konstanten Ausfalldichte sollte jedoch validiert werden, da das Ergebnis einer Prüfung nichtig sein kann, wenn die Annahme falsch verwendet wird (siehe IEC 60605-6).

8.3.3 Verifizierung und Validierung durch Analyse

Die Funktionsfähigkeit eines Systems kann rechnerisch vor der Auslieferung durch eine Funktionsfähigkeitsanalyse verifiziert und validiert werden. Für einige Bereiche (beispielsweise bei Systemen mit sehr hoher Funktionsfähigkeit) kann dies der einzig gangbare Weg sein. Analysen können schon lange durchgeführt werden, bevor ein Nachweis der Funktionsfähigkeit während der Anwendung (Validierung) oder durch Prüfung im Labor möglich sein wird. Dieses Verfahren kann jedoch nur durch Analyse bestimmen, ob das auszuliefernde System die in der Systemspezifikation genannten Anforderungen erfüllt. Die erzielte Funktionsfähigkeit wird dabei nicht direkt gemessen.

Zu Beispielen für analytische Verfahren bei der Funktionsfähigkeitsverifizierung und -validierung eines Systems mit Hardware- und Softwarekomponenten zählen:

- Zuverlässigkeitsblockdiagramme;
- Fehlerbaumanalysen;
- Zustandsdiagramme;
- Fehlermöglichkeits- und Einflussanalysen.

Siehe 0 mit Normen, die Anleitungen zu den verschiedenen Analysemethoden enthalten.

Die Geräte eines Systems sollten daraufhin analysiert werden, ob die Ausfallraten aller Subsysteme, Teile und elektronischen Bauelemente sowie der anderen Komponenten richtig bestimmt sind und dass die erwarteten Anwendungen und betrieblichen Beanspruchungen richtig und begründbar berücksichtigt wurden. Hierzu können elektrische, thermische oder andere Messungen notwendig sein.

Die Software eines Systems sollte in ähnlicher Weise auf mögliche Versagensarten untersucht und deren qualitative Auswirkung auf die Funktionsfähigkeit des Systems bewertet werden.

Daten und Zahlenwerte für solche Berechnungen können beispielsweise durch Erfahrungen mit ähnlichen, bereits in der Anwendung befindlichen Geräten, aus Prüfungen im Labor, aus der Integration von Hardware und Software erhalten oder sie können anerkannten Datenquellen entnommen werden. Falls der Käufer beabsichtigt, eine bestimmte Datenquelle (zum Beispiel ein bestimmtes Handbuch mit Ausfallraten) vorzuschreiben, so sollte dies zwischen dem Lieferanten und dem Käufer vereinbart werden. Die Vorgabe einer bestimmten Datenquelle entbindet den Lieferanten jedoch nicht von seiner Verpflichtung, die geforderte Zuverlässigkeit zu erreichen. Auf jeden Fall sollten die Datenquelle genannt und die Annahmen und Schätzungen dokumentiert werden.

9 Instandhaltbarkeit

9.1 Allgemeines

Instandhaltbarkeit ist eine wichtige Maßgröße für die Zuverlässigkeit aller Arten instandsetzbarer Systeme. Sie steht für die Fähigkeit eines Systems, in einem Zustand bewahrt oder wieder in ihn zurückversetzt werden zu können, in dem es seine geforderte Funktion ausführen kann. Ein Beispiel sind Aktualisierungen von Softwareprojekten in der Mitte ihrer Lebensdauer, wenn die bis dahin erreichte Verfügbarkeit zu niedrig ist und korrigiert werden soll, oder abseits gelegene Einsatzorte, an denen Systeme schwierig instand zu halten sind. Allgemein ist zu beachten, dass für Systeme die Instandhaltbarkeit einen bedeutenden Einfluss auf die erreichte Zuverlässigkeit haben kann, falls diese falsch spezifiziert wurde. Dies gilt insbesondere für Systeme ohne Redundanz. Instandhaltbarkeit wird allgemein in IEC 60300-3-10 behandelt.

9.2 Festlegung der Instandhaltbarkeit

9.2.1 Quantitative Anforderungen

Einzelheiten zur Spezifizierung und vertraglichen Ausgestaltung der Instandhaltbarkeit können IEC 60706-2 entnommen werden. Es könnte nötig sein, die Anforderungen an die korrektive und die vorbeugende Instandhaltung getrennt festzulegen, da die hierfür jeweils erforderliche Unterstützbarkeit sehr unterschiedlich sein kann.

Falls quantitative Anforderungen spezifiziert werden, muss die Dauer festgelegt werden, während der sich ein System aufgrund der Instandhaltungsebene oder der Unterstützbarkeit in einem Nichtbetriebszustand befindet. Für diese Dauer sind geeignete Maßgrößen zu verwenden, wie zum Beispiel der Mittelwert oder das Quantil der Reparaturdauer, bzw. der Mittelwert oder das Quantil der logistischen Verzugsdauer. Quantitative Anforderungen können auch abhängig von der benötigten Zeit oder der zurückzulegenden Entfernung angegeben werden, beispielsweise die Instandhaltungskosten je Betriebsstunde.

Eine vollständige Festlegung der Instandhaltbarkeitsanforderungen sollte fünf weite Bereiche abdecken:

- die Instandhaltbarkeit, die durch die Konstruktion des Systems erreicht werden soll;
- die Einschränkungen für die Systemnutzung, die sich auf die Instandhaltung auswirken;
- die vom Lieferanten zu erfüllenden Vorgaben des Instandhaltbarkeitsprogramms, die sicherstellen sollen, dass das ausgelieferte System die geforderten Instandhaltbarkeitsmerkmale hat;
- die Anforderungen an die Zugänglichkeit zur Instandhaltung;
- die Bereitstellung eines Unterstützbarkeitsplans.

Bei der Festlegung der Anforderungen an die Instandhaltbarkeit müssen folgende Punkte angegeben werden:

- die verschiedenen Betriebs- und Umgebungsbedingungen, unter denen das Gerät eingesetzt wird;
- die Qualifikationen und Zuständigkeiten sowie die körperliche Konstitution des für den Betrieb und die Instandhaltung des Geräts verantwortlichen Personals;
- die anzuwendenden Instandhaltungsgrundsätze und die zugehörigen Verfahren und logistischen Vorkehrungen (z. B. präventive Instandhaltung oder diagnostische Prüfung);
- verfügbare Werkzeuge und gegebenenfalls erforderliche Spezialwerkzeuge;
- bereitzustellende Ersatzteile und deren Berechnung und Bevorratung.

Die Festlegung der Instandhaltbarkeit sollte die Forderungen und die Verfahren zu ihrer Erfüllung im Einzelnen darlegen. Sie sollte weiterhin genaue Definitionen der in der Spezifikation verwendeten Begriffe enthalten und, falls zutreffend, auf Begriffsnormen wie IEC 60050-192 verweisen.

Die Instandhaltbarkeitsanforderungen können in der Spezifikation entweder als Zielsetzung oder in Form fest vorgegebener Anforderungen festgelegt werden, die mit vorgeschriebenen Verfahren verifiziert werden müssen. Zielsetzungen oder Anforderungen können entweder in quantitativer oder in qualitativer Form festgelegt sein.

Die Festlegungen zur Instandhaltbarkeit enthalten üblicherweise die verschiedenen während des Betriebs durchzuführenden und zu erreichenden Instandhaltungsaufgaben. Da die Instandhaltbarkeit als Systemmerkmal die Instandhaltungs- und Bereitschaftskosten beeinflusst und auch die Instandhaltungsdauern in den verschiedenen Instandhaltungsebenen beeinflussen kann, sollten auf allen Instandhaltungsebenen die Anforderungen an die Ziele, für die die Instandhaltungsgrundsätze gelten, in die Festlegungen aufgenommen werden.

Weitergehende Anleitungen zur Festlegung von Instandhaltbarkeitsanforderungen in Spezifikationen und Verträgen sind in IEC 60706-2 enthalten.

Anhang D, Absatz D.4 führt Beispiele für quantitative Anforderungen an die Instandhaltbarkeit auf.

9.2.2 Qualitative Anforderungen

Sollten die Anforderungen an die Instandhaltbarkeit nicht quantifiziert werden können, sollten ersatzweise qualitative Anforderungen verwendet werden. Jedoch dürfen, wie bei allen anderen Zuverlässigkeitsmerkmalen auch, sowohl quantitative als auch qualitative Anforderungen festgelegt werden. Dies könnte beispielsweise der spezifizierte Grad sein, zu dem ein System die spezifischen Bedingungen und die auf die Instandhaltung bezogenen Einschränkungen einhält.