

DIN EN 60300-3-4

ICS 03.120.10; 29.020

Ersatz für
DIN IEC 60300-3-4:1999-04
Siehe jedoch Beginn der
Gültigkeit

**Zuverlässigkeitsmanagement –
Teil 3-4: Anwendungsleitfaden –
Anleitung zum Festlegen von Zuverlässigkeitsforderungen
(IEC 60300-3-4:2007);
Deutsche Fassung EN 60300-3-4:2008**

Dependability management –
Part 3-4: Application guide –
Guide to the specification of dependability requirements (IEC 60300-3-4:2007);
German version EN 60300-3-4:2008

Gestion de la sûreté de fonctionnement –
Partie 3-4: Guide d'application –
Spécification d'exigences de sûreté de fonctionnement (CEI 60300-3-4:2007);
Version allemande EN 60300-3-4:2008

Gesamtumfang 37 Seiten

DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE

Beginn der Gültigkeit

Die von CENELEC am 2007-12-01 angenommene EN 60300-3-4 gilt als DIN-Norm ab 2008-06-01.

Daneben darf DIN IEC 60300-3-4:1999-04 noch bis 2010-12-01 angewendet werden.

Nationales Vorwort

Vorausgegangener Norm-Entwurf: E DIN IEC 60300-3-4:2006-02.

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

Die enthaltene IEC-Publikation wurde vom TC 56 „Dependability“ erarbeitet.

Das IEC-Komitee hat entschieden, dass der Inhalt dieser Publikation bis zu dem Datum (maintenance result date) unverändert bleiben soll, das auf der IEC-Website unter „<http://webstore.iec.ch>“ zu dieser Publikation angegeben ist. Zu diesem Zeitpunkt wird entsprechend der Entscheidung des Komitees die Publikation

- bestätigt,
- zurückgezogen,
- durch eine Folgeausgabe ersetzt oder
- geändert.

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

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

Der Zusammenhang der zitierten Normen mit den entsprechenden Deutschen Normen 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.

Änderungen

Gegenüber DIN IEC 60300-3-4:1999-04 wurden folgende Änderungen vorgenommen:

- a) neuer Abschnitt 4 „Allgemeine Betrachtungen zu Zuverlässigkeitsspezifikationen“;
- b) neuer Abschnitt 5 über das „Zuverlässigkeitsmanagement“;
- c) Änderung des informativen Anhangs A: Anstelle von Beispielen für Zuverlässigkeitsanforderungen enthält Anhang A jetzt eine Auflistung von Bezugsnormen für Zuverlässigkeitsprüfverfahren.

Frühere Ausgaben

DIN IEC 60300-3-4: 1999-04

**Zuverlässigkeitsmanagement –
Teil 3-4: Anwendungsleitfaden –
Anleitung zum Festlegen von Zuverlässigkeitsforderungen
(IEC 60300-3-4:2007)**

Dependability management –
Part 3-4: Application guide –
Guide to the specification of dependability
requirements
(IEC 60300-3-4:2007)

Gestion de la sûreté de fonctionnement –
Partie 3-4: Guide d'application –
Spécification d'exigences de sûreté de
fonctionnement
(CEI 60300-3-4:2007)

Diese Europäische Norm wurde von CENELEC am 2007-12-01 angenommen. Die CENELEC-Mitglieder sind gehalten, die CEN/CENELEC-Geschäftsordnung zu erfüllen, in der die Bedingungen festgelegt sind, unter denen dieser Europäischen Norm ohne jede Änderung der Status einer nationalen Norm zu geben ist.

Auf dem letzten Stand befindliche Listen dieser nationalen Normen mit ihren bibliographischen Angaben sind beim Zentralsekretariat oder bei jedem CENELEC-Mitglied auf Anfrage erhältlich.

Diese Europäische Norm besteht in drei offiziellen Fassungen (Deutsch, Englisch, Französisch). Eine Fassung in einer anderen Sprache, die von einem CENELEC-Mitglied in eigener Verantwortung durch Übersetzung in seine Landessprache gemacht und dem Zentralsekretariat mitgeteilt worden ist, hat den gleichen Status wie die offiziellen Fassungen.

CENELEC-Mitglieder sind die nationalen elektrotechnischen Komitees von Belgien, Bulgarien, Dänemark, Deutschland, Estland, Finnland, Frankreich, Griechenland, Irland, Island, Italien, Lettland, Litauen, Luxemburg, Malta, den Niederlanden, Norwegen, Österreich, Polen, Portugal, Rumänien, Schweden, der Schweiz, der Slowakei, Slowenien, Spanien, der Tschechischen Republik, Ungarn, dem Vereinigten Königreich und Zypern.

CENELEC

Europäisches Komitee für Elektrotechnische Normung
European Committee for Electrotechnical Standardization
Comité Européen de Normalisation Electrotechnique

Zentralsekretariat: rue de Stassart 35, B-1050 Brüssel

© 2008 CENELEC – Alle Rechte der Verwertung, gleich in welcher Form und in welchem Verfahren, sind weltweit den Mitgliedern von CENELEC vorbehalten.

Ref. Nr. EN 60300-3-4:2008 D

Vorwort

Der Text des Schriftstücks 56/1212/FDIS, zukünftige 2. Ausgabe von IEC 60300-3-4, ausgearbeitet von dem IEC/TC 56 „Dependability“, wurde der IEC-CENELEC Parallelen Abstimmung unterworfen und von CENELEC am 2007-12-01 als EN 60300-3-4 angenommen.

Nachstehende Daten wurden festgelegt:

- spätestes Datum, zu dem die EN auf nationaler Ebene durch Veröffentlichung einer identischen nationalen Norm oder durch Anerkennung übernommen werden muss (dop): 2008-09-01
- spätestes Datum, zu dem nationale Normen, die der EN entgegenstehen, zurückgezogen werden müssen (dow): 2010-12-01

Der Anhang ZA wurde von CENELEC hinzugefügt.

Anerkennungsnotiz

Der Text der Internationalen Norm IEC 60300-3-4:2007 wurde von CENELEC ohne irgendeine Abänderung als Europäische Norm angenommen.

In der offiziellen Fassung sind unter „Literaturhinweise“ zu den aufgelisteten Normen die nachstehenden Anmerkungen einzutragen:

IEC 60812	ANMERKUNG	Harmonisiert als EN 60812:2006 (nicht modifiziert).
IEC 61165	ANMERKUNG	Harmonisiert als EN 61165:2006 (nicht modifiziert).
IEC 61508-1	ANMERKUNG	Harmonisiert als EN 61508-1:2001 (nicht modifiziert).
IEC 61508-2	ANMERKUNG	Harmonisiert als EN 61508-2:2001 (nicht modifiziert).
IEC 61508-3	ANMERKUNG	Harmonisiert als EN 61508-3:2001 (nicht modifiziert).
IEC 61508-4	ANMERKUNG	Harmonisiert als EN 61508-4:2001 (nicht modifiziert).
IEC 61508-5	ANMERKUNG	Harmonisiert als EN 61508-5:2001 (nicht modifiziert).
IEC 61508-6	ANMERKUNG	Harmonisiert als EN 61508-6:2001 (nicht modifiziert).
IEC 61508-7	ANMERKUNG	Harmonisiert als EN 61508-7:2001 (nicht modifiziert).
IEC 61709	ANMERKUNG	Harmonisiert als EN 61709:1998 (nicht modifiziert).

Inhalt

	Seite
Vorwort	2
Einleitung	5
1 Anwendungsbereich	5
2 Normative Verweisungen	6
3 Begriffe	7
4 Allgemeine Betrachtungen zu Zuverlässigkeitsspezifikationen	8
4.1 Zuverlässigkeit gestalten	8
4.2 Anforderungen und Zielsetzungen	9
4.3 Systeme	10
4.4 Nachweis der Erfüllung der Anforderungen	11
4.5 Vertraglich vereinbarte Zuverlässigkeit	13
4.6 Spezifikationsarten	15
4.7 Herleitung von Zuverlässigkeitsspezifikationen	16
5 Zuverlässigkeitsmanagement	16
6 Verfügbarkeit	17
6.1 Allgemeines	17
6.2 Festlegung der Verfügbarkeit	18
6.3 Verifizierung und Validierung der Verfügbarkeit	19
7 Funktionsfähigkeit	20
7.1 Allgemeines	20
7.2 Festlegung der Funktionsfähigkeit	20
7.3 Verifizierung und Validierung der Funktionsfähigkeit	22
8 Instandhaltbarkeit	24
8.1 Allgemeines	24
8.2 Festlegung der Instandhaltbarkeit	24
8.3 Verifizierung und Validierung der Instandhaltbarkeit	25
9 Instandhaltungsbereitschaft	26
9.1 Allgemeines	26
9.2 Festlegen der Instandhaltungsunterstützung	26
9.3 Verifizierung und Validierung der Instandhaltungsunterstützung	27
Anhang A (informativ) Bezugsnormen für Verifizierungs- und Validierungsverfahren	28
A.1 Zuverlässigkeitsprüfverfahren	28
A.2 Zuverlässigkeitsanalyseverfahren	29
Anhang B (informativ) Beispiele für Anforderungen an die Zuverlässigkeit	30
B.1 Allgemeines	30
B.2 Anforderungen an die Verfügbarkeit	30
B.3 Anforderungen an die Funktionsfähigkeit	30
B.4 Anforderungen an die Instandhaltbarkeit	31

	Seite
B.5 Anforderungen an die Instandhaltungsbereitschaft.....	31
Literaturhinweise.....	32
Anhang ZA (normativ) Normative Verweisungen auf internationale Publikationen mit ihren entsprechenden europäischen Publikationen	34

Einleitung

Für viele Systeme stellen Funktionsfähigkeit, Instandhaltbarkeit und Verfügbarkeit wesentliche Leistungsmerkmale dar. Zusammen mit der Instandhaltungsbereitschaft 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, Abmessungen, Masse usw.

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

Zur Beurteilung 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 Käufer gemeinsam vereinbarte oder geschriebene Spezifikationen.

Diese Norm ist auf alle drei vorstehenden Spezifikationsarten anwendbar.

Diese Norm ergänzt IEC 62347, in der die Definition von Systemen und deren Bestandteile so behandelt wird, dass damit die Zuverlässigkeitsanforderungen eines jeden Elementes unter Verwendung dieser Norm festgelegt werden können. Der Zweck der Norm IEC 62347 ist die Ermittlung der Systemanforderungen nach Funktionen aus systemtechnischer Sicht. Sie beschreibt eine Vorgehensweise, wie man die Systemanwendungen aus Sicht eines Käufers in eine technische Sicht zur Systementwicklung übersetzen kann. IEC 62347 betont den Architektur- und Funktionsentwurf als Grundlage für die Realisierung der Funktionen durch geeignete Auswahl von Hardware, Software und menschlichen Elementen, um somit die geforderte Systemzuverlässigkeit entsprechend den Käuferbedürfnissen zu erzielen.

1 Anwendungsbereich

Dieser Teil der IEC 60300 leitet zur Festlegung der geforderten Zuverlässigkeitsmerkmale in Spezifikationen an, zusammen mit Festlegungen für die Verfahren und die Kriterien ihrer Verifizierung und Validierung.

Diese Anleitung umfasst insbesondere das Folgende:

- Empfehlungen zur Festlegung quantitativer und qualitativer Anforderungen an die Funktionsfähigkeit, Instandhaltbarkeit, Verfügbarkeit und Instandhaltungsbereitschaft, also an die Zuverlässigkeit;
- 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 Unterlagen, 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 Produkte, Einheiten oder auf die Bauelementeebene angewendet werden. Der Begriff „System“ wird durchgehend in dieser Norm verwendet.

ANMERKUNG 2 Mit dieser Norm ist nicht beabsichtigt, Anleitung zum Management von Zuverlässigkeitsprogrammen oder den Tätigkeiten zu geben, die zur Erfüllung der festgelegten Anforderungen an Verfügbarkeit, Funktionsfähigkeit, Instandhaltbarkeit und Instandhaltungsbereitschaft (also an die Zuverlässigkeit) notwendig sind. Für solche allgemeine Anleitungen wird auf andere Normen verwiesen.

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 für die Zuverlässigkeit einer Dienstleistung werden in dieser Anleitung nicht behandelt. Dies betrifft auch Dienstleistungen, die im Rahmen von Partnerschaften des öffentlichen mit dem privaten Bereich beschafft werden.

2 Normative Verweisungen

Die folgenden zitierten Dokumente 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 60050-191, *International Electrotechnical Vocabulary (IEV) – Chapter 191: Dependability and quality of service*

IEC 60300-1, *Dependability management – Part 1: Dependability management systems*

IEC 60300-2, *Dependability management – Part 2: Guidelines for dependability management*

IEC 60300-3-1, *Dependability management – Part 3-1: Application guide – Analysis techniques for dependability – Guide on methodology*

IEC 60300-3-2, *Dependability management – Part 3-2: Application guide – Collection of dependability data from the field*

IEC 60300-3-3, *Dependability management – Part 3-3: Application guide – Life cycle costing*

IEC 60300-3-5, *Dependability management – Part 3-5: Application guide – Reliability test conditions and statistical test principles*

IEC 60300-3-10, *Dependability management – Part 3-10: Application guide – Maintainability*

IEC 60300-3-12, *Dependability management – Part 3-12: Application guide – Integrated logistic support*

IEC 60300-3-14, *Dependability management – Part 3-14: Application guide – Maintenance and maintenance support*

IEC 60605-4, *Equipment reliability testing – Part 4: Statistical procedures for exponential distribution – Point estimates, confidence intervals, prediction intervals and tolerance intervals*

IEC 60605-6, *Equipment reliability testing – Part 6: Tests for the validity and estimation of the constant failure rate and constant failure intensity*

IEC 60706-2, *Maintainability of equipment – Part 2: Maintainability requirements and studies during the design and development phase*

IEC 60706-3, *Maintainability of equipment – Part 3: Verification and collection, analysis and presentation of data*

IEC 60706-5, *Maintainability of equipment – Part 5: Diagnostic testing*

IEC 61014, *Programmes for reliability growth*

IEC 61025, *Fault tree analysis (FTA)*

IEC 61070, *Compliance test procedures for steady-state availability*

IEC 61078, *Analysis techniques for dependability – Reliability block diagram and Boolean methods*

IEC 61123, *Reliability testing – Compliance test plans for success ratio*

IEC 61124, *Reliability testing – Compliance tests for constant failure rate and constant failure intensity*

IEC 61160, *Design review*

IEC 61164, *Reliability growth – Statistical test and estimation methods*

IEC 61508 (alle Teile), *Functional safety of electrical/electronic/programmable electronic safety-related systems*

IEC 61649, *Goodness-of-fit tests, confidence intervals and lower confidence limits for Weibull distributed data*

IEC 61703, *Mathematical expressions for reliability, availability, maintainability and maintenance support terms*

IEC 61710, *Power law model – Goodness-of-fit tests and estimation methods*

IEC 61713, *Software dependability through the software life cycle processes – Application guide*

IEC 62198, *Project risk management – Application guidelines*

IEC 62308, *Equipment Reliability – Reliability assessment methods*

IEC 62347, *Guidance on system dependability specifications*

3 Begriffe

Für die Anwendung dieses Dokuments gelten die Begriffe nach IEC 60050-191 und die folgenden Begriffe.

ANMERKUNG Die Definitionen von „Zuverlässigkeit“, „Verfügbarkeit“, „Funktionsfähigkeit“, „Instandhaltbarkeit“, „Instandhaltungsbereitschaft“, „Ausfall“, „Fehlzustand“, „Betrachtungseinheit“, „Dauer bis zum Ausfall“ und „Betriebsdauer zwischen Ausfällen“ sind in IEC 60050-191 enthalten.

3.1

Verifizierung

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

[ISO 9000:2005, 3.8.4, modifiziert]

ANMERKUNG 1 In 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 Zu den Beispielen für Tätigkeiten der Verifizierung gehören:

- die Bewertung der Ergebnisse (Dokumente aus allen Phasen des Lebenszyklus), um unter Berücksichtigung der jeweiligen Eingaben der Phase die Übereinstimmung mit den Zielsetzungen und Anforderungen der 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 für einen spezifischen beabsichtigten Gebrauch oder eine spezifische beabsichtigte Anwendung erfüllt worden sind

[ISO 9000:2005, 3.8.5, modifiziert]

ANMERKUNG Validierung ist die Tätigkeit, die darlegt, dass das betrachtete System vor und nach der Installation in jeder Hinsicht der Anforderungsspezifikation des Systems entspricht. Deshalb bedeutet beispielsweise Software-Validierung die Bestätigung durch Untersuchung und Bereitstellung eines objektiven Nachweises, dass die Software die Softwarespezifikation erfüllt.

4 Allgemeine Betrachtungen zu Zuverlässigkeitsspezifikationen

4.1 Zuverlässigkeit gestalten

Jedes System hat eine gewisse Zuverlässigkeit, gleichgültig, 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 könnte nicht möglich sein, solch ein 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 sind.

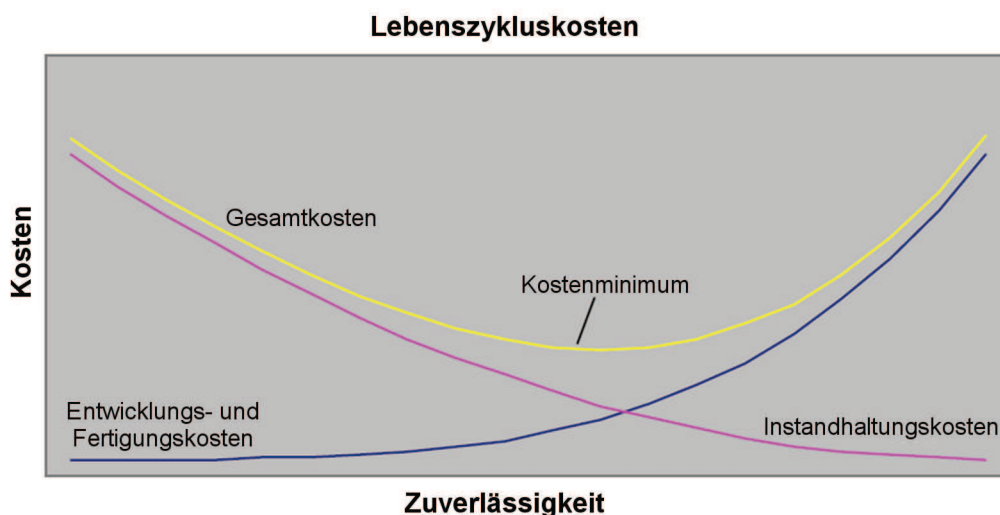


Bild 1 – Zusammenhang von Kosten und Zuverlässigkeit

In Bild 1 wird gezeigt, dass es ein Zuverlässigkeitsniveau gibt, bei dem die Gesamtkosten über die Lebensdauer eines Systems minimiert sind. Bei handelsüblichen Systemen (en: commercial off the shelf, COTS) verschiebt sich dieses Minimum, da sich mehrere Parteien die Entwicklungskosten teilen. Die optimale Zuverlässigkeit eines Systems kann jedoch durch andere Faktoren beeinflusst werden, so beispielsweise

durch Sicherheitsanforderungen oder Systemfunktionen, und somit nicht notwendigerweise diejenige Zuverlässigkeit sein, 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 links des Punktes der minimalen Lebenszykluskosten liegen. Eine Investition in eine an der Zuverlässigkeit orientierte Entwicklung kann sich daher hinsichtlich der kombinierten Entwicklungs-, Fertigungs- 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 Weisen festgelegt werden. In dieser Norm wird die Zuverlässigkeit unter den folgenden vier Überschriften betrachtet:

- Verfügbarkeit (A);
- Funktionsfähigkeit ($R(t)$), hierzu gehören die mittlere Dauer bis zum Ausfall (MTTF) oder die mittlere Betriebsdauer zwischen Ausfällen (MTBF) sowie Parameter der Weibull- oder Exponentialverteilungen;
- Instandhaltbarkeit, hierzu gehören die mittlere Unklardauer (MDT) und die mittlere Dauer bis zur Wiederherstellung (MTTR);
- Instandhaltungsbereitschaft.

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 Instandhaltungsbereitschaft 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 wichtig ist. Falls zutreffend, sollten auch Anforderungen an die vorbeugende und korrektive Instandhaltung (also Wartung und Instandsetzung) festgelegt werden.

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

In den Abschnitten 6, 7, 8 und 9 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 erbracht werden, noch bevor das System in Dienst gestellt wird als Teil der vereinbarten Liefergegenstände oder auch nach Indienststellung 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 braucht entweder nicht oder kann nicht erbracht werden.

Für Systeme hoher Verfügbarkeit oder hoher Funktionsfähigkeit wird es möglicherweise nicht praktikabel sein, einen formalen Nachweis des Erreichens der hohen Verfügbarkeit oder Funktionsfähigkeit zu erbringen. Der Käufer muss die Zielwerte für die hohe Verfügbarkeit und Funktionsfähigkeit, die nicht nachgewiesen werden können, vorgeben sowie niedrigere Anforderungen, die nachgewiesen werden können, festlegen; dabei muss klar gesagt werden, was wofür gilt.

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.

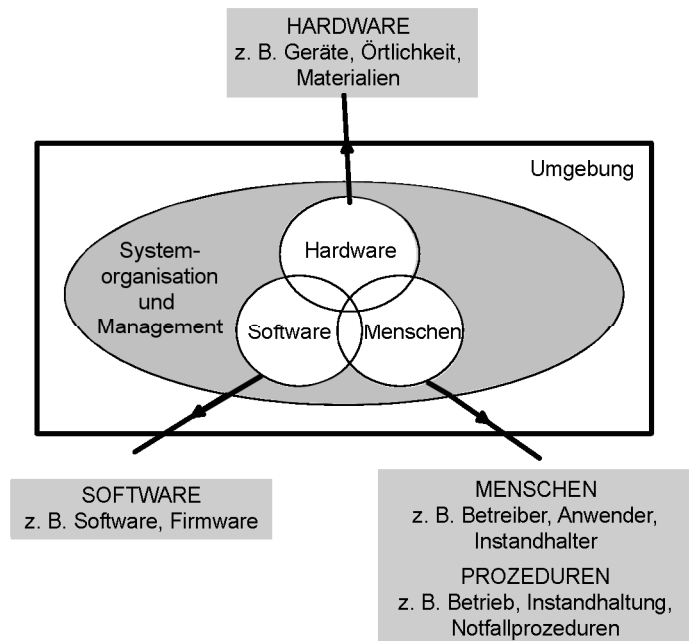


Bild 2 – Elemente eines Systems

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. Beispielsweise können verschiedene Betreiber eines Systems dieses missbrauchen oder dieses in einer aggressiveren Art anwenden und dadurch mehr Ausfälle hervorrufen und so eine geringere Zuverlässigkeit bewirken. Es kann jedoch Fälle geben, in denen Lieferant und Käufer wenig oder keine Kontrolle über spätere Instandhaltungsverfahren oder Fähigkeiten haben, beispielsweise ein öffentlich verkauftes Kraftfahrzeug. Die Zuverlässigkeitsanforderungen sollten 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 IEC 62347 definiert werden, dort ist näher beschrieben, wie man ein System, seine Elemente und die Kritikalität^{N1)} jeder Funktion definieren kann, so dass Anforderungen an jedes Element festgelegt werden können.

Die Zuverlässigkeitsspezifikation eines Systems sollte neben den Anforderungen an die Hardware auch die Spezifikation der Software und die Elemente, die für die Menschen stehen, beinhalten. Die in dieser Norm gegebenen Anleitungen können in gewisser Hinsicht auch auf die Spezifizierung der Software angewendet

^{N1)} Nationale Fußnote: Kritikalität ist ein Maß für die Schwere der Folgen eines Ausfalls.