

DIN EN 60300-3-15

ICS 03.120.10; 29.020

**Zuverlässigkeitsmanagement –
Teil 3-15: Anwendungsleitfaden –
Technische Realisierung der Systemzuverlässigkeit
(IEC 60300-3-15:2009);
Deutsche Fassung EN 60300-3-15:2009**

Dependability management –
Part 3-15: Application guide –
Engineering of system dependability (IEC 60300-3-15:2009);
German version EN 60300-3-15:2009

Gestion de la sûreté de fonctionnement –
Partie 3-15: Guide d'application –
Ingénierie de la sûreté de fonctionnement des systèmes (CEI 60300-3-15:2009);
Version allemande EN 60300-3-15:2009

Gesamtumfang 63 Seiten

DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE

Beginn der Gültigkeit

Die von CENELEC am 2009-10-01 angenommene EN 60300-3-15 gilt als DIN-Norm ab 2010-05-01.

Nationales Vorwort

Vorausgegangener Norm-Entwurf: E DIN IEC 60300-3-15:2006-05.

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.

Zuverlässigkeitsmanagement –
Teil 3-15: Anwendungsleitfaden –
Technische Realisierung der Systemzuverlässigkeit
(IEC 60300-3-15:2009)

Dependability management –
Part 3-15: Application guide –
Engineering of system dependability
(IEC 60300-3-15:2009)

Gestion de la sûreté de fonctionnement –
Partie 3-15: Guide d'application –
Ingénierie de la sûreté de fonctionnement
des systèmes
(CEI 60300-3-15:2009)

Diese Europäische Norm wurde von CENELEC am 2009-10-01 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: Avenue Marnix 17, B-1000 Brüssel

© 2009 CENELEC – Alle Rechte der Verwertung, gleich in welcher Form und in welchem Verfahren, sind weltweit den Mitgliedern von CENELEC vorbehalten.

Ref. Nr. EN 60300-3-15:2009 D

Vorwort

Der Text des Schriftstücks 56/1315/FDIS, zukünftige 1. Ausgabe von IEC 60300-3-15, ausgearbeitet von dem IEC/TC 56 „Dependability“, wurde der IEC-CENELEC Parallelen Abstimmung unterworfen und von CENELEC am 2009-10-01 als EN 60300-3-15 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): 2010-07-01
- spätestes Datum, zu dem nationale Normen, die der EN entgegenstehen, zurückgezogen werden müssen (dow): 2012-10-01

Der Anhang ZA wurde von CENELEC hinzugefügt.

Anerkennungsnotiz

Der Text der Internationalen Norm IEC 60300-3-15:2009 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:

[1] IEC 61069-1	ANMERKUNG	Harmonisiert als EN 61069-1:1993 (nicht modifiziert).
[2] IEC 62347	ANMERKUNG	Harmonisiert als EN 62347:2007 (nicht modifiziert).
[7] IEC 60300-3-1	ANMERKUNG	Harmonisiert als EN 60300-3-1:2004 (nicht modifiziert).
[9] IEC 61508	ANMERKUNG	Harmonisiert in der Reihe EN 61508 (nicht modifiziert).
[10] IEC 61508-1	ANMERKUNG	Harmonisiert als EN 61508-1:2001 (nicht modifiziert).
[12] IEC 61014	ANMERKUNG	Harmonisiert als EN 61014:2003 (nicht modifiziert).
[13] IEC 61164	ANMERKUNG	Harmonisiert als EN 61164:2004 (nicht modifiziert).
[14] ISO 10007	ANMERKUNG	Harmonisiert als EN ISO 10007:1996 (nicht modifiziert).
[16] IEC 60300-3-11	ANMERKUNG	Harmonisiert als EN 60300-3-11:2009 (nicht modifiziert).
[17] IEC 60300-3-12	ANMERKUNG	Harmonisiert als EN 60300-3-12:2004 (nicht modifiziert).
[22] IEC 60721	ANMERKUNG	Harmonisiert in der Reihe EN 60721 (nicht modifiziert).
IEC 60300-3-4	ANMERKUNG	Harmonisiert als EN 60300-3-4:2008 (nicht modifiziert).
IEC 60812	ANMERKUNG	Harmonisiert als EN 60812:2006 (nicht modifiziert).
IEC 61025	ANMERKUNG	Harmonisiert als EN 61025:2007 (nicht modifiziert).

IEC 61078	ANMERKUNG	Harmonisiert als EN 61078:2006 (nicht modifiziert).
IEC 61508-7	ANMERKUNG	Harmonisiert als EN 61508-7:2001 (nicht modifiziert).
IEC 61709	ANMERKUNG	Harmonisiert als EN 61709:1998 (nicht modifiziert).
IEC 62308	ANMERKUNG	Harmonisiert als EN 62308:2006 (nicht modifiziert).
ISO 13407	ANMERKUNG	Harmonisiert als EN ISO 13407:1999 (nicht modifiziert).

Inhalt

	Seite
Vorwort.....	2
Einleitung	7
1 Anwendungsbereich	8
2 Normative Verweisungen	8
3 Begriffe	8
4 Technische Realisierung der Systemzuverlässigkeit und Anwendungen	9
4.1 Allgemeines zur technischen Realisierung der Systemzuverlässigkeit	9
4.2 Systemzuverlässigkeitsmerkmale und Leistungskenngrößen	10
5 Zuverlässigkeit gestalten	11
5.1 Zuverlässigkeitsmanagement.....	11
5.2 Systemzuverlässigkeitsprojekte	11
5.3 Zuschneiden auf die Projektbedürfnisse	12
5.4 Zuverlässigkeitssicherung	12
6 Realisierung der Systemzuverlässigkeit.....	12
6.1 Prozess der Entwicklung der Zuverlässigkeit in Systemen.....	12
6.2 Erreichen der Systemzuverlässigkeit	15
6.3 Bewertung der Systemzuverlässigkeit	20
6.4 Messung der Systemzuverlässigkeit.....	23
Anhang A (informativ) Systemlebenszyklusprozesse und Anwendungen	27
A.1 Systemlebenszyklusprozesse	27
A.1.1 Beschreibung der Systemlebenszyklusprozesse.....	27
A.1.2 Prozesstätigkeiten in den Systemlebenszyklusstufen.....	28
A.2 Beispiele für Prozessanwendungen	29
A.2.1 Prozess in der Konzept-/Definitionsstufe	29
A.2.2 Prozess in der Systementwicklungsstufe.....	31
A.2.3 Prozess in der Stufe der Realisierung und Umsetzung des Systems.....	33
A.2.4 Prozess in der Stufe des Betriebs und der Instandhaltung des Systems	34
A.2.5 Prozess in der Stufe der Erweiterung des Systems.....	35
A.2.6 Prozess in der Stufe der Außerbetriebnahme/Abschaltung des Systems	35
Anhang B (informativ) Verfahren und Werkzeuge für die Entwicklung und Sicherung der Systemzuverlässigkeit.....	37
B.1 Allgemeines	37
B.2 Allgemeine Anwendungen von Verfahren und Werkzeugen für die Realisierung der Zuverlässigkeit in Systemen.....	37
B.2.1 Funktionsfähigkeits- und Instandhaltbarkeitsfall	37
B.2.2 Programme für das Zuverlässigkeitswachstum.....	37
B.2.3 Konfigurationsmanagement.....	38
B.2.4 Bayessche Netze.....	38

B.3	Hardwarespezifische Anwendungen von Verfahren und Werkzeugen zur Realisierung der Zuverlässigkeit in Systemen	38
B.3.1	Steigerung der Funktionsfähigkeit.....	38
B.3.2	Steigerung der Instandhaltbarkeit	39
B.3.3	Steigerung der Instandhaltung und Logistikunterstützung	40
B.4	Softwarespezifische Anwendungen von Verfahren und Werkzeugen zur Realisierung der Zuverlässigkeit in Systemen	40
B.4.1	Objektorientierte Methodik	40
B.4.2	Strukturierte Methodik	40
B.4.3	Entwurf durch funktionale Zerlegung	41
B.4.4	Analyse von Fehlaussagen	41
B.4.5	Delphi-Technik	41
B.4.6	Rechnergestützte Softwareentwicklung	42
B.4.7	Software-Entwicklungsumgebungen	42
B.4.8	Reifegradmodelle	42
Anhang C (informativ)	Anleitung zur Beachtung der Systemanwendungsumgebungen	44
C.1	Verständnis der Systemanwendungsumgebungen	44
C.2	Prozess der Festlegung von Umgebungsanforderungen	44
C.3	Systemumgebungsbedingungen.....	45
C.3.1	Klassifizierung der Systemumgebungsbedingungen	45
C.3.2	Elektromagnetische Bedingungen	46
C.3.3	Klimatische Bedingungen.....	46
C.3.4	Mechanische Bedingungen.....	46
C.4	Durch Systemeinsatzbedingungen beeinflusste Konstruktionsmerkmale	46
C.5	Bei der Entwicklung zu beachtende Systemmerkmale	47
C.5.1	Allgemeines	47
C.5.2	Bei der Entwicklung zu beachtende EMV-Belange.....	47
C.5.3	Bei der Entwicklung zu beachtende thermische Belange	48
C.5.4	Bei der Entwicklung zu beachtende Qualitätsbelange	48
C.5.5	Bei der Entwicklung zu beachtende Zuverlässigkeitsbelange	48
C.5.6	Bei der Entwicklung zu beachtende Umweltverträglichkeitsbelange	48
Anhang D (informativ)	Prüflisten für die Entwicklung der Systemzuverlässigkeit	50
D.1	Prüflisten für das Projektmanagement der Systemzuverlässigkeit.....	50
D.1.1	Allgemeines	50
D.1.2	Prüflisten für die Markterkundung	50
D.1.3	Prüflisten für die Systementwicklung	51
D.1.4	Prüflisten für die Produktrealisierung	51
D.1.5	Prüflisten für die Systemabnahme	52
D.1.6	Prüflisten für den Regelbetrieb.....	52
D.1.7	Prüflisten für Erweiterungen.....	52

	Seite
D.1.8 Prüflisten für Außerbetriebnahme	53
D.2 Prüflisten für Hardware, Software und menschliche Einflüsse.....	53
D.2.1 Allgemeines	53
D.2.2 Prüflisten für Hardwareentwicklung.....	53
D.2.3 Prüflisten für Softwareentwicklung	54
D.2.4 Prüflisten zur Berücksichtigung menschlicher Einflüsse	54
D.2.5 Prüfliste für Umweltverträglichkeit	55
D.3 Prüflisten für die Verwendung handelsüblicher Produkte in Systemen	56
D.3.1 Allgemeines	56
D.3.2 Prüflisten für die Ermittlung der Anforderungen	56
D.3.3 Prüflisten für die Beurteilung des dokumentierten Verhaltens	56
D.3.4 Prüflisten für Produktsicherung	57
Literaturhinweise.....	58
 Bilder	
Bild 1 – Übersicht über einen Systemlebenszyklus.....	13
Bild 2 – Beispiel eines Prozessmodells	14
Bild A.1 – Übersicht über Systemlebenszyklusprozesse.....	27
Bild C.1 – Prozess der Festlegung von Umgebungsanforderungen	45
Bild C.2 – Abbildung von Systemanwendungsumgebungen auf Beanspruchungen	46
Bild C.3 – Abbildung von Systemanwendungsumgebungen auf Entwurfsattribute	47

Einleitung

Aktuell verwendete Systeme nehmen laufend an Komplexität zu. Systemzuverlässigkeit ist zu einem wichtigen Leistungsmerkmal geworden und hat Auswirkungen auf Geschäftsstrategien sowohl beim Erwerb als auch beim wirtschaftlichen Betrieb eines Systems während dessen gesamter Lebensdauer. Die Gesamtzuverlässigkeit eines Systems ist das zusammengefasste Ergebnis komplexer Wechselwirkungen einzelner Systemelemente, der Einsatzumgebung, der Mensch-Maschine-Schnittstellen, der bereitgestellten Unterstützungsdienste und anderer Einflussfaktoren.

In diesem Teil von IEC 60300 wird zur technischen Realisierung eines Gesamtsystems so angeleitet, dass das System die gesetzten Zuverlässigkeitsziele erreichen kann. Die in dieser Norm beschriebene technische Vorgehensweise stellt das aktuelle wissenschaftliche Fachwissen und die zugehörigen technischen Disziplinen dar, mit denen die geforderte Zuverlässigkeit in dem zu realisierenden System verwirklicht werden kann.

Die bei der Realisierung der Systemzuverlässigkeit zu beachtenden wichtigsten vier Punkte sind

- Prozess,
- Erfüllung,
- Bewertung und
- Messung.

Die technischen Disziplinen sind technische Prozesse, die für die jeweiligen Stufen des Systemlebenszyklus geeignet und anwendbar sind. In diesem Teil von IEC 60300 beschriebene einzelne technische Prozesse werden durch eine Abfolge zugehöriger Prozesstätigkeiten ergänzt, damit die Zielsetzungen jeder einzelnen Stufe im Systemlebenszyklus erreicht werden können.

Dieser Teil von IEC 60300 ist anwendbar auf allgemeine, aus den Elementen Hardware, Software und Menschen bestehende Systeme, in denen diese Elemente miteinander in Wechselwirkung stehen, um so die geforderte Systemfunktion zu erbringen. In vielen Fällen kann eine bestimmte Funktion durch handelsübliche Produkte realisiert werden. Ein System kann mit anderen Systemen verbunden sein und so ein Netzwerk bilden. Die Grenzen, die ein Produkt von einem System und ein System von einem Netzwerk abgrenzen, können durch die Definition der Anwendung einer Einheit beschrieben werden. Beispielsweise kann das Produkt digitaler Zeitgeber zum Synchronisieren des Betriebs eines Rechners verwendet werden; der Rechner als ein System kann in einem Büro mit anderen Rechnern verbunden sein, die zusammen ein lokales Netzwerk zur gegenseitigen Kommunikation bilden. Die Anwendungsumgebung kann für alle Arten von Systemen vorgegeben werden. Beispiele solchermaßen beschriebener Systeme sind Steuerungssysteme zur Stromerzeugung, fehlertolerante Rechensysteme und Systeme zur Bereitstellung von Unterstützungsdiensten.

Es wird zur technischen Realisierung der Zuverlässigkeit allgemeiner Systeme angeleitet. Systeme für Spezialanwendungen werden nicht behandelt. Die Mehrzahl der in Betrieb befindlichen Systeme ist während ihres Lebenszyklus aus wirtschaftlichen und praktischen Gründen instandsetzbar. Nicht instandsetzbare Systeme wie beispielsweise Fernmeldesatelliten, fern abgesetzte Mess- und Überwachungsgeräte oder Geräte zur einmaligen Verwendung werden als anwendungsspezifische Systeme erachtet. Für solche Systeme müssen die spezifische Anwendungsumgebung, die betrieblichen Bedingungen und zusätzliche Angaben zu einzigartigen, zur Erfüllung ihrer betrieblichen Zielsetzung notwendigen Leistungsmerkmalen, eigens ermittelt werden. Nicht instandsetzbare Subsysteme und Bauelemente werden als Wegwerf-Einheiten behandelt. Die Auswahl der für die technische Realisierung der Zuverlässigkeit in einem spezifischen System anzuwendenden Prozesse geschieht beim Projektzuschnitt und über den Zuverlässigkeitsmanagementprozess.

Dieser Teil von IEC 60300 gehört zu den Rahmennormen über die Systemaspekte der Zuverlässigkeit, die die Normen IEC 60300-1 und IEC 60300-2 zum Zuverlässigkeitsmanagement ergänzen. Bezüge zu Projektmanagementtätigkeiten bei Systemen werden hergestellt. Dazu gehören die Ermittlung und Benennung von für Systeme relevanten Zuverlässigkeitselementen und Aufgaben sowie Anleitungen zu Zuverlässigkeitsmanagementbewertungen und der Zuschnitt von Zuverlässigkeitsprojekten.

1 Anwendungsbereich

In diesem Teil von IEC 60300 wird zur technischen Realisierung der Systemzuverlässigkeit angeleitet und ein Prozess beschrieben, wie die Systemzuverlässigkeit während des Lebenszyklus realisiert werden kann.

Diese Norm ist auf neue Systementwicklungen und auf die Erweiterung bestehender Systeme anwendbar, bei denen Hardware, Software und menschliche Elemente miteinander in Wechselwirkung stehen.

Diese Norm ist ebenfalls auf Lieferanten von Subsystemen und Produkten anwendbar, die Angaben zum System und Kriterien für die Systemintegration benötigen. Es werden Methoden und Werkzeuge für die Bewertung der Systemzuverlässigkeit und für die Verifizierung der Ergebnisse der Erfüllung der Zuverlässigkeitsziele angegeben.

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

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

3 Begriffe

Für die Anwendung dieses Dokuments gelten die folgenden Begriffe.

3.1

System

Satz von in Wechselbeziehung stehenden Elementen, die als Ganzes für einen bestimmten Zweck betrachtet werden, losgelöst von anderen Einheiten

ANMERKUNG 1 Ein System wird allgemein hinsichtlich der Ausübung einer bestimmten Funktion definiert.

ANMERKUNG 2 Das System wird so betrachtet, als ob es eine imaginäre Hülle hätte, welche die Verbindungen zwischen dem System und seiner Umgebung und anderen externen Systemen schneidet.

ANMERKUNG 3 Externe Mittel (also außerhalb der Systemgrenzen gelegen) können für den Betrieb des Systems erforderlich sein.

ANMERKUNG 4 Die Struktur eines Systems kann hierarchisch sein, z. B. System, Subsystem, Bauelement, usw.

3.2

Subsystem

System, das Teil eines komplexeren Systems ist

3.3

Betriebsprofil

vollständiger Aufgabensatz zur Erzielung einer spezifischen Systemzielsetzung

ANMERKUNG 1 Konfigurations- und Betriebsszenarien sind Teil des Systembetriebsmodus.

ANMERKUNG 2 Ein Betriebsprofil ist die Abfolge und Durchführung der von einem System geforderten Aufgaben zum Erreichen seiner betrieblichen Zielsetzung. Das Betriebsprofil repräsentiert ein spezifisches Betriebsszenarium für das betriebene System.

3.4

Funktion

elementare Operation, die das System ausführt und die das System befähigt, zusammen mit anderen elementaren Operationen (Systemfunktionen) eine Teilaufgabe auszuführen

[IEC 61069-1:1991, 2.2.5] [1]¹⁾

3.5

Element

Kombination von Bauelementen, die den Grundstein für die Ausführung einer bestimmten Funktion bilden

ANMERKUNG 1 Ein Element kann aus Hardware, Software und menschlichen Anteilen bestehen.

ANMERKUNG 2 Bei einigen Systemen sind Informationen und Daten wichtige Teile des Systembetriebs.

3.6

Integrität

Fähigkeit eines Systems, seine Form, Stabilität und Robustheit beizubehalten und seine Leistung und seinen Dienst weiterhin zu erbringen

4 Technische Realisierung der Systemzuverlässigkeit und Anwendungen

4.1 Allgemeines zur technischen Realisierung der Systemzuverlässigkeit

Zuverlässigkeit ist die Fähigkeit eines Systems, eine geforderte Funktion zu erreichen, wenn diese angefordert wird, um gegebene Zielsetzungen bei gegebenen Einsatzbedingungen zu erreichen. Zu den Zuverlässigkeitsmerkmalen gehören die Verfügbarkeit und ihre inhärenten oder äußeren sie beeinflussenden Faktoren wie Funktionsfähigkeit, Fehlertoleranz, Erholungsfähigkeit, Integrität, Sicherheit, Instandhaltbarkeit, Ausdauer und Instandhaltungsbereitschaft. Die Zuverlässigkeit eines Systems unterstellt, dass das System vertrauenswürdig und in der Lage ist, den gewünschten Dienst bei Anforderung zur Zufriedenstellung der Bedürfnisse der Benutzer zu leisten. Die Zielsetzung des Systems, seine Struktur, Eigenschaften und die die Systemzuverlässigkeit beeinflussenden Bedingungen sind in IEC 62347 [2] beschrieben. Dort wird zur Bestimmung der relevanten Systemfunktionen für die Festlegung der Systemzuverlässigkeit angeleitet.

Bei der technischen Realisierung der Systemzuverlässigkeit sind vier Hauptschritte zu unterscheiden:

- a) **Zuverlässigkeitsprozess festlegen** – In diesem Schritt werden die zur Realisierung der Zuverlässigkeit in einem System notwendigen technischen Prozesse festgelegt. Die Prozesse bestehen aus einer Abfolge von Tätigkeiten, die in jeder entsprechenden Lebenszyklusstufe umgesetzt werden müssen, damit das System die festgelegten Ziele erreichen kann bzw. das geforderte Verhalten zeigt. Der Zuverlässigkeitsprozess muss voll in den Entwicklungs- und Managementprozess integriert werden;
- b) **Zuverlässigkeit erreichen** – In diesem Schritt werden die festgelegten technischen Prozesse und das vorhandene Fachwissen in den jeweilig zutreffenden Lebenszyklusstufen umgesetzt. Ziel hierbei ist das schrittweise Erreichen der Zuverlässigkeitsziele einer jeden Systemfunktion durch die Realisierung des für diese Funktion verantwortlichen Subsystems und der Systemintegration (Zuverlässigkeitswachstum);
- c) **Zuverlässigkeit bewerten** – In diesem Schritt werden die Zuverlässigkeitsmerkmale bewertet, und es wird ermittelt, wie wirksam die Umsetzung in das System erfolgt ist. Es wird ermittelt, wie die jeweiligen Zuverlässigkeitsmerkmale den Projektbedürfnissen gerecht werden, und es können die Bewertungsmethodik und Begründung für diese Attribute bestimmt werden;
- d) **Zuverlässigkeit messen** – In diesem Schritt werden die Zuverlässigkeitsmerkmale für Verträge, Spezifikationen und Bewertungen quantifiziert. Aufgabe dieses Prozesses ist es, jeder Zuverlässigkeitskenngröße ein Zuverlässigkeitsmaß mit zugehörigem Zahlenwert zuzuweisen. Ziel hierbei ist es, eine Absichtserklärung in quantifizierbaren Begriffen auszudrücken, um das gegenseitige Verständnis des jeweiligen Sachverhaltes zu erleichtern und eine Basis für vertragliche Festlegungen zu erhalten.

¹⁾ Zahlen in rechteckigen Klammern verweisen auf das Literaturverzeichnis.

4.2 Systemzuverlässigkeitsmerkmale und Leistungskenngrößen

Systemzuverlässigkeitsmerkmale sind diejenigen spezifischen auf die Zuverlässigkeit bezogenen Merkmale und zeitabhängigen Leistungskenngrößen, die dem System durch dessen Entwurf und Konstruktion inhärent sind. Einige Merkmale wie Systemleistungskenngrößen können quantifiziert und gemessen werden. Andere, nicht quantifizierbare Zuverlässigkeitsmerkmale können dennoch von einem gewissen Nutzen sein oder nützliche Informationen über diese Merkmale darstellen. Diese nicht quantifizierbaren Zuverlässigkeitsmerkmale können durch qualitative Begriffe beschrieben werden und so für subjektive Zuverlässigkeitsbewertungen wertvoll sein. Sowohl quantifizierbare als auch nicht quantifizierbare Merkmale sind wichtig, um die Eigenschaften der Systemzuverlässigkeit zu beschreiben. Beispiele nicht quantifizierbarer Merkmale sind der Wert einer Produktmarke, Benutzerfreundlichkeit und informative Hinweise. Beispiele quantifizierbarer Leistungskenngrößen sind Klarzeit, Ausfallhäufigkeit, mittlerer Ausfallabstand und Zeit für die Wiederherstellung aus einem gestörten Zustand zurück in den Normalbetrieb.

Die Hauptattribute der Systemzuverlässigkeit sind:

- a) **Verfügbarkeit:** Fähigkeit eines Systems, eine geforderte Funktion erfüllen zu können, wenn eine Anforderung an das System gestellt wird. Die Verfügbarkeit wird gekennzeichnet durch Maßgrößen wie prozentuale Klarzeit, also die relative Dauer, die das System im betriebsfähigen Zustand ist und seine geforderte Leistung erbringt, Ausfallhäufigkeit und Unklarzeit, also die Dauer eines Ausfallzustandes;
- b) **Funktionsfähigkeit:** Fähigkeit eines Systems, eine geforderte Funktion unter gegebenen Einsatzbedingungen für ein gegebenes Zeitintervall zu erfüllen. Die Funktionsfähigkeit wird gekennzeichnet durch Maßgrößen wie mittlerer Ausfallabstand und ausfallfreie Betriebsdauer;
- c) **Instandhaltbarkeit:** Fähigkeit eines Systems, nach einem Ausfall in einen Zustand zurückversetzt werden zu können, in dem es eine geforderte Funktion erfüllen kann, oder in solch einem Klarzustand erhalten werden kann unter den gegebenen Abwendungs- und Instandhaltungsbedingungen. Die Instandhaltbarkeit wird gekennzeichnet durch die mittlere Dauer bis zur Wiederherstellung und durch die Erholungsdauer;
- d) **Instandhaltungsbereitschaft:** Fähigkeit einer Organisation, unter gegebenen Bedingungen bei Bedarf die Mittel bereitzustellen, die für die Instandhaltung eines Systems erforderlich sind. Die Instandhaltbarkeit wird gekennzeichnet durch Maßgrößen wie Grad der Benutzung der Instandhaltungsmittel, Schulungsbedarf, Sonderwerkzeuge und Vorrichtungen, logistische Verzugsdauer und Umlaufdauer für die Wiederbeschaffung von Ersatzteilen.

Es gibt weitere auf die Zuverlässigkeit bezogene Merkmale für spezifische Systemanwendungen. Zu ihnen gehören neben anderen:

- e) **Erholungsfähigkeit:** Fähigkeit eines Systems, nach einem Ausfall in einen Zustand zurückversetzt werden zu können, indem es eine geforderte Funktion erfüllen kann, ohne dass die Hardware oder Software repariert werden muss. Sie wird gekennzeichnet durch Maßgrößen wie z. B. mittlere Dauer bis zur Erholung;
- f) **Prüfbarkeit:** Fähigkeit, ein System in vorgezeichneten Instandhaltungsebenen prüfen zu können, um anschließend Ersatz- und Reparaturmaßnahmen durchführen und um den Fehlzustandserkennungsgrad bestimmen zu können;
- g) **Dienstzugänglichkeit:** Fähigkeit eines Dienstes, auf Anforderung durch den Benutzer innerhalb festgelegter Toleranzen und anderen Randbedingungen bereitgestellt werden zu können. Sie wird gekennzeichnet durch Maßgrößen wie z. B. die Wahrscheinlichkeit, zu einem Dienst Zugang zu erhalten;
- h) **Dienstbeständigkeit:** Fähigkeit eines bereitgestellten Dienstes, bei gegebenen Bedingungen für eine gewünschte Dauer weiterhin bereitgestellt zu bleiben. Sie wird gekennzeichnet durch Maßgrößen wie die Wahrscheinlichkeit der Aufrechterhaltung je Zeitdauer.

Die Wiederherstellungsfähigkeit hängt von der Systemarchitektur, der Fehlertoleranz und den in das System hinein konstruierten selbstheilenden Merkmalen ab. Das Systemverhalten hängt von den Eigenschaften der Systemeinrichtungen, Konstruktion und Infrastruktur der Ressourcenbereitstellung ab. Die Attribute der Systemleistung sind im Allgemeinen dem Systementwurf inhärent. Die Leistungsattribute werden von der Fähigkeit des Systems und den Zuverlässigkeitsmerkmalen abgeleitet.

Die Kenngrößen des Systemleistungsverhaltens werden aus Zeitmessungen und der Beobachtung von Vorfällen abgeleitet. Ein Vorfall ist ein unerwünschtes oder unerwartetes Ereignis, das entweder während

Systemtests oder im Betrieb beobachtet wurde und ein Hinweis auf einen stattgefundenen Ausfall sein könnte. Alle Vorfälle sollten aufgezeichnet und untersucht werden. Dadurch soll festgestellt werden, ob der Vorfall durch einen tatsächlichen Ausfall verursacht wurde oder ob er auf ein menschliches Versagen oder eine fälschliche Beobachtung zurückzuführen ist. Ein Ausfall ist eine Abweichung von der geforderten Leistung und Funktion des Systems. Jedoch könnte zum Zeitpunkt der Beobachtung ein Ausfall nicht zur vollständigen Beendigung der Systemfunktionen geführt haben, sondern lediglich das Systemverhalten verschlechtert oder die Leistung eingeschränkt haben. Das Ausmaß der Verschlechterung sollte vor einer Klassifizierung als Ausfall definiert und für Messungen entsprechend festgelegt werden.

5 Zuverlässigkeit gestalten

5.1 Zuverlässigkeitsmanagement

Zuverlässigkeit ist eine technische Disziplin und wird über technische Grundsätze und Praktiken gestaltet. IEC 60300-1 und IEC 60300-2 werden in diesem Teil von IEC 60300 zur Formulierung von Strategien zum Zuverlässigkeitsmanagement verwendet und für allgemeine technische Vorgehensweisen bei der Umsetzung von Zuverlässigkeitselementen und Aufgaben. Zusätzliche Managementprozesse zur Behandlung systemspezifischer Managementangelegenheiten werden eingeführt. Zuverlässigkeitsmanagement bedarf der Projektplanung, der Zuweisung von Ressourcen und Zuverlässigkeitsaufgaben, der Überwachung und Sicherung, der Ergebnismessung, der Datenanalyse und der fortwährenden Verbesserung. Zuverlässigkeitstätigkeiten sollten zusammen mit anderen technischen Disziplinen durchgeführt werden, um die notwendigen Synergiewirkungen zu erhalten und um den Wert der Projektergebnisse zu erhöhen. Das Projekt sollte so auf die aktuellen Bedürfnisse zugeschnitten werden, dass es möglichst kostengünstig gestaltet werden kann. Sofern zutreffend sollte eine Lebenszykluskostenanalyse dazu verwendet werden, die Ressourcen richtig zuzuweisen und die Kosten für den Erwerb des Systems und der gesamten Lebensdauerkosten zu beurteilen.

5.2 Systemzuverlässigkeitsprojekte

Im Projektmanagement ist die Zuverlässigkeit ein entscheidender Faktor. Zuverlässigkeit wirkt sich auf die Kosten der Projektumsetzung aus. Bei der Projektumsetzung stehen spezifische Zuverlässigkeitsbelange im Mittelpunkt, die wirksam gelöst werden müssen. Zuverlässigkeit hat erhebliche Auswirkungen darauf, wie das Projekt die Erwartungen des Kunden letztendlich erfüllt. Aus Sicht der Systementwicklung ist die Realisierung der Zuverlässigkeit in Systemen ein wichtiger wirtschaftlicher Entscheidungsfaktor, sie sollte daher voll in die Entwicklung integriert und in den Entscheidungsprozess der Leitung mit einbezogen werden. Das Gestalten der Obsoleszenz, die Bewertung des Projektrisikos, technische Abwägungen, Betrachtung der Lebenszykluskosten, Vergabe von Aufgaben nach außen und Koordinierung der Lieferkette sind einige Beispiele der Zuverlässigkeitstätigkeiten in der Systementwicklung und Projektdurchführung.

Nicht in allen Projekten wird ein ganzes System neu entwickelt. Die meisten Systeme werden aus der Integration von Subsystemen und aus handelsüblichen Produkten gebildet, die zusammen die Systemfunktionen bereitstellen. Bei großen Systementwicklungen oder bei Systemerweiterungsprojekten kann es sein, dass mehrere Entwickler von Subsystemen und Unterauftragnehmer für Lieferungen und Dienstleistungen an dem Projekt mitwirken, damit dieses rechtzeitig fertiggestellt werden kann. In solchen Fällen ist ein Projektmanagement zur Koordinierung der unterschiedlichen Projektteile unerlässlich. Bei einem Systemzuverlässigkeitsprojekt können die folgenden speziellen Zuverlässigkeitsaktivitäten notwendig sein:

- a) Verwendung einer neuen Technologie planen und umsetzen;
- b) Ausarbeitung von Zuverlässigkeitsspezifikationen für Systeme und Subsysteme;
- c) Zuverlässigkeit von handelsüblichen Produkten beurteilen, mit denen Systemfunktionen realisiert werden sollen;
- d) Bewertung der Fähigkeit von Lieferanten, den Anforderungen des Zuverlässigkeitsprojekts gerecht zu werden;
- e) Zuverlässigkeit für die Systemabnahme sicherstellen.

Tätigkeiten für die Systemzuverlässigkeit können in jeder Stufe des Systemlebenszyklus durchgeführt werden. Einige Zuverlässigkeitsaufgaben können besondere Fähigkeiten und Schulungen erfordern, so etwa in den technischen Disziplinen Softwareentwicklung, Logistikunterstützung und menschliche Zuverlässigkeit.

5.3 Zuschneiden auf die Projektbedürfnisse

Ein Systemzuverlässigkeitsprojekt wird eingerichtet, um besondere Zuverlässigkeitsangelegenheiten mit Belang für das System zu behandeln. Der Zweck der Anpassung (oder des Zuschneidens) des Projekts an die tatsächlichen Gegebenheiten liegt in der Gestaltung der verfügbaren Projektressourcen und der Auswahl der geeigneten Methoden zur wirksamen Problemlösung. Beispiele für anzupassende Tätigkeiten in einem Systemzuverlässigkeitsprojekt sind:

- a) Budgetplanung für die Zuweisung von Zuverlässigkeitsressourcen, um die Projektziele und die Auslieferung erfüllen zu können;
- b) Beurteilung alternativer Technologien für den Erwerb hochzuverlässiger Produkte;
- c) Auslagerung von Subsystementwicklungen, wenn bezüglich der Anforderungen an den Reifegrad der Software strenge Kriterien zu erfüllen sind und die Prozessüberwachung entscheidend ist;
- d) erforderliche Schulungsdauer, um sich mit einem neuen Zuverlässigkeitsanalysewerkzeug ausreichend vertraut zu machen;
- e) Auswahl von Unterauftragnehmern zur Bereitstellung der Instandhaltung vor Ort bei kritischen Systemen mit sehr hohen Erwartungen an die Verfügbarkeit, bei denen keine geplante Abschaltung vorgesehen ist.

IEC 60300-2 enthält eine Anleitung zum Anpassen und Zuschneiden von Zuverlässigkeitsprogrammen und Projekten.

5.4 Zuverlässigkeitssicherung

Die Tätigkeiten zur Sicherung der Zuverlässigkeit sollten Teil der Qualitätssicherungsaufgaben eines Systemzuverlässigkeitsprojektes sein. So soll sichergestellt werden, dass alle geplanten und systematischen Tätigkeiten, die im Qualitätssystem durchgeführt und nötigenfalls auch nachgewiesen werden, ein angemessenes Vertrauen erzeugen und dass die Anforderungen an das System und die Produktqualität erfüllt werden. Zu den wichtigsten Tätigkeiten zählen die Projektplanung, die Zuweisung der technischen und der Managementverantwortung, Verifizierung der Ergebnisse der Zuverlässigkeitsbewertung, Validierung der erhaltenen Zuverlässigkeitsdaten hinsichtlich der Systemabnahme, Beobachtung der Zuverlässigkeit, über Ausfälle berichten und Analyse der Daten für prompte korrektive und präventive Maßnahmen, Dokumentation relevanter Informationen zur Zuverlässigkeit und Pflege von Prüfaufzeichnungen für objektive Beweise und eine Bewertung durch das Management mit dem Ziel der Prozessverbesserungen. IEC 60300-2 enthält weitere Angaben zur Auswahl von Zuverlässigkeitsprogrammelementen und Aufgaben, um Systemzuverlässigkeitsprojekte entsprechend auszurichten.

6 Realisierung der Systemzuverlässigkeit

6.1 Prozess der Entwicklung der Zuverlässigkeit in Systemen

6.1.1 Allgemeines zum Zuverlässigkeitsprozess

Das Aufstellen eines Prozesses ist eine wesentliche Voraussetzung für ein erfolgreiches Management der Projektaufgaben und Koordinierung der Tätigkeiten. Der Zuverlässigkeitsprozess sollte zur leichteren Realisierung der Zuverlässigkeit im System in den allgemeinen technischen Prozess integriert werden. Der Zuverlässigkeitsprozess liefert spezifische Eingaben bei wichtigen Entscheidungspunkten im Systemlebenszyklus und erleichtert so die Projektumsetzung. Diese wichtigen Entscheidungspunkte werden beim Abschluss kritischer Projektmanagementphasen erreicht, so bei der Ermittlung der Marktgegebenheiten, in der Systementwicklung und Produktrealisierung, bei der Systemabnahme, im laufenden Betrieb, bei Erweiterungen und bei der Außerbetriebnahme. Angaben und Informationen zur Zuverlässigkeit sind bei diesen wichtigen Entscheidungspunkten für die Rechtfertigung weiterer geschäftlicher Investitionen von entscheidender Bedeutung.

6.1.2 Systemlebenszyklus und Prozesse

Der Zeitpunkt, zu dem man mit der technischen Realisierung der Zuverlässigkeit in Systemen beginnen sollte, ist die früheste Lebenszyklusstufe. Der Anwender sollte in dieser Lebenszyklusstufe eine wirksame technische Entwicklung starten.

Die Beschreibung der Systemlebenszyklusstufen kann aus Sicht einer allgemeinen Systementwicklung erfolgen. Es gibt aber auch andersartige Beschreibungen eines Systemlebenszyklus. IEC 60300-2 beschreibt die Produktlebenszyklusphasen aus Sicht des Projektmanagements. ISO/IEC 15288 [3] beschreibt einen ähnlichen Systemlebenszyklus aus Sicht der Informationstechnik und der Softwareentwicklung. Die Anleitung in diesem Teil von IEC 60300 beruht auf der Konzeption der Systemlebenszyklusstufen, siehe Bild 1. Systemstufen sind genaue technische Übergangspunkte, wogegen Projektphasen sich überlappen können, wenn das Management aus übergeordneten geschäftlichen Überlegungen so entscheidet. Das in IEC 60300-2 beschriebene Projektrisikomanagement gilt für den gesamten Lebenszyklusprozess.

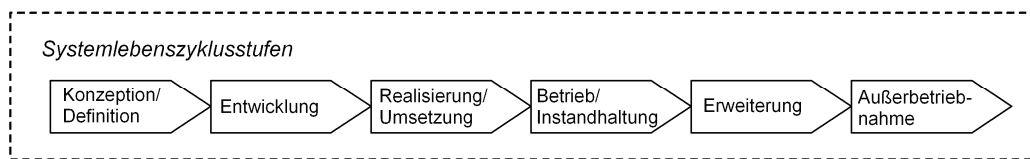


Bild 1 – Übersicht über einen Systemlebenszyklus

Die technischen Realisierungsprozesse bestehen aus einer Abfolge von Prozessstätigkeiten, die in jeder der der einzelnen Tätigkeit entsprechenden Stufe des Lebenszyklus durchgeführt werden, mit dem Ziel, das beabsichtigte Systemverhalten und die Zuverlässigkeitszielsetzungen zu erreichen. Die technische Realisierung der Zuverlässigkeit in einem System kann nicht isoliert erfolgen. Dies wird in Verbindung mit anderen technischen Disziplinen (z. B. Konstruktion) und unterstützenden Tätigkeiten (z. B. Qualitätssicherung) erfolgen, die alle auf die Realisierung der Systemfunktionen in der beabsichtigten Anwendung ausgerichtet sind. Anhang A zeigt eine logische Abfolge von Lebenszyklustätigkeiten.

Nachfolgend sind die Zielsetzungen der wichtigsten in einem Lebenszyklus auszuführenden Tätigkeiten aufgeführt:

- bei der Festlegung der Anforderungen werden die Bedürfnisse der Anwender und die Einschränkungen der Systemanwendungen ermittelt;
- bei der Analyse der Anforderungen wird die vom Anwender vorgesehene Systemanwendung in eine technische Sicht für die Entwicklung des Systems umgesetzt. Dazu wird ein Profil für den betrieblichen Einsatz entwickelt;
- beim Architekturentwurf wird eine Grobkonzeption für das System erarbeitet, mit der die geforderten Betriebsszenarien realisiert werden können. Dafür werden die benötigten einzelnen Systemfunktionen ermittelt und den Hardware-, Software- und menschlichen Elementen zugeordnet;
- beim Entwurf und der Beurteilung der Funktionen werden die praktischen Mittel und Wege ermittelt, wie die Funktionen realisiert werden können, um zwischen verschiedenen Lösungen abwägen und optimieren zu können;
- bei der Dokumentation der Systementwicklung werden Systeminformationen erfasst. Hierzu gehören auch für den Systementwurf geeignete Zuverlässigkeitsdaten;
- beim Systementwurf und der Subsystementwicklung werden die spezifizierten System- und Subsystemfunktionen geschaffen;
- in der Realisierung werden die System- und Subsystemelemente in Hardware- und Softwareform produziert;
- in der Integration werden das System und die Subsysteme gemäß dem Architekturentwurf zusammengebaut;
- bei der Verifizierung wird bestätigt, dass die spezifizierten Anforderungen an den Entwurf vom System erfüllt werden;
- bei der Installation/dem Übergang wird die Fähigkeit des Systems hergestellt, die geforderte Leistung und den geforderten Dienst in der spezifizierten Betriebsumgebung zu erbringen;

- k) bei der Validierung/Inbetriebnahme wird der objektive Nachweis erbracht, dass das System die funktionalen Anforderungen erfüllt;
- l) während des Betriebes soll das System den geforderten Dienst erbringen;
- m) durch die Instandhaltungsbereitschaft wird sichergestellt, dass das System den geforderten Dienst erbringen kann;
- n) durch Erweiterung wird die Systemleistung durch hinzugefügte zusätzliche Merkmale verbessert und erweitert;
- o) die Außerbetriebnahme/Abschaltung beendet die Existenz der Systemeinheit (Anlage).

6.1.3 Prozessanwendungen im Systemlebenszyklus

Ein Prozess ist ein integrierter Satz von miteinander verbundenen oder in Wechselwirkung stehenden Tätigkeiten, der Eingaben in Ausgaben, also Ergebnisse umwandelt. Prozesse werden bei der funktionalen Organisation (z. B. Qualitätsmanagementsysteme, QMS, Projektmanagement), bei geschäftlichen Transaktionen (z. B. Erwerb, Lieferkettenvereinbarungen) und in der technischen Planung und Umsetzung (z. B. Produktentwicklung, Systembewertungen) als Referenzmodelle verwendet. Dieser Teil von IEC 60300 legt den Schwerpunkt auf Prozesse für die technische Realisierung der Zuverlässigkeit in Systemen.

Bild 2 zeigt ein Beispiel eines Prozessmodells. Bei der technischen Realisierung bestehen die primären Eingaben üblicherweise aus einem Anforderungsdatensatz oder vom Kunden geäußerten Bedürfnissen. Die Ergebnisse können aus verarbeiteten Daten, die eine gewünschte Lösung wie etwa eine Spezifikation beschreiben, aus einem gefertigten Produkt oder einer Dienstleistung bestehen. Es gibt für Steuerungs-, und Lenkungszwecke und zu Vorbereitungszwecken weitere mit dem Prozess verbundene Eingaben. Die Prozesstätigkeiten wandeln die primären Eingaben in die gewünschten Ergebnisse um. Diese Umwandlung geschieht abhängig von den durch die ermöglichenden Mechanismen vorgegebenen Bedingungen und dazugehörigen Einflussfaktoren. Einige Einflussfaktoren können steuerbar sein wie etwa betriebliche Prozeduren zur Aktivierung des Prozesses; andere können nicht steuerbar sein, wie etwa das Wetter oder plötzliche Klimaänderungen. Ermöglichende Mechanismen wie Verfahren und Werkzeuge sind für die Durchführung der Umwandlung unerlässlich. Dieses Prozessmodell wird für die Umsetzung der in diesem Teil von IEC 60300 beschriebenen technischen Prozesse verwendet.

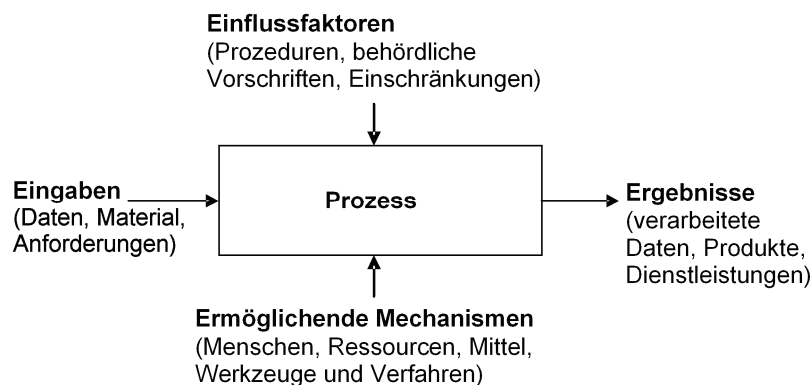


Bild 2 – Beispiel eines Prozessmodells

Mit technischen Prozessen wird Folgendes bezweckt:

- a) technische Realisierungsaufgaben erledigen und während der Systemkonzeption und Entwicklung technische Anpassungen durchführen;
- b) Betriebs-, Instandhaltungs- und Entsorgungsaufgaben für das System ausführen.

Um eine gewünschte Lösung zu erreichen, werden technische Prozesse sowohl rekursiv als auch iterativ ausgeführt. Dies trifft für alle Stufen des Systemlebenszyklus zu. Die Wechselbeziehungen der technischen Prozesse sind unabhängig von Systemgröße und Struktur. Prozesstätigkeiten wie Festlegung oder Analyse der Anforderungen und Architekturentwurf sind deduktive (von oben nach unten gerichtete) technische Vorgehensweisen zur Entwicklung und Realisierung der gewünschten Lösung (zum Beispiel das System in seine

Elemente und Komponenten aufgliedern); hingegen sind Integration und Verifizierung induktive (von unten nach oben gerichtete) Vorgehensweisen zur Realisierung der Systemkonfiguration und zur Validierung der Leistungsfähigkeit des Systems (zum Beispiel aus den einzelnen Elementen das System konstruieren). Der Übergang zwischen den Vorgehensweisen deduktiv und induktiv während der Umsetzungsstufe liegt beim Abschluss der Systeminstallation, nach der die Inbetriebnahme beginnt. Dies wird in der Ingenieurpraxis auch als „V“-Modell bezeichnet und ist in ISO/IEC 15288 [3] beschrieben.

ANMERKUNG Für weitere Informationen zum „V“-Modell wird auf ISO/IEC/TR 15271 [4] verwiesen.

ISO/IEC 12207 [5] setzt einen Rahmen für Software-Lebenszyklusprozesse. Dort sind Prozesse, Tätigkeiten und Aufgaben enthalten, die während des Erwerbs eines Softwareprodukts oder Dienstes sowie während der Lieferung, der Entwicklung, des Betriebs, bei der Instandhaltung und der Entsorgung der Softwareprodukte angewendet werden können. ISO/IEC 12207 [5] kann entweder für sich alleine oder in Verbindung mit ISO/IEC 15288 [3] angewendet werden.

Typische Beispiele für Prozessanwendungen in jeder Systemlebenszyklusstufe sind in Anhang A enthalten. Um spezifischen Projektbedürfnissen genügen zu können, ist die Kenntnis der Systemart und der Einsatzumgebung für das Anpassen der Prozessanwendung in der jeweiligen Systemlebenszyklusstufe unerlässlich.

6.2 Erreichen der Systemzuverlässigkeit

6.2.1 Allgemeines zum Erreichen der Systemzuverlässigkeit

Unter Erreichen versteht man die Maßnahmen, durch die eine Vorgabe erzielt und erfüllt wird. Sie spiegeln die Ergebnisse einer erfolgreichen Problemlösung wider. Die zum Erreichen der Systemzuverlässigkeit erforderlichen Maßnahmen können durch wirksame technische Bemühungen und eingesetztes Fachwissen in geeigneten Stufen des Systemlebenszyklus erzielt werden. Das Ziel ist ein fortschreitendes Erreichen der vorgegebenen Zuverlässigkeitsziele der einzelnen Systembestandteile und Systemfunktionen und deren Integration zum System. Das Erreichen der Systemzuverlässigkeit ist ein wichtiges Projektziel, das koordiniert und für die Systemabnahme nachgewiesen werden muss. Eine Systemabnahme ist üblicherweise eine vertragliche Vereinbarung, bei der der Kunde seine Anforderungen erfüllt sehen möchte. Das letztendliche Ziel ist es, die Erwartungen des Anwenders an die Leistungsfähigkeit des Systems zu befriedigen.

6.2.2 Kriterien für das Erreichen der Systemzuverlässigkeit

Systemzuverlässigkeit wird durch erfolgreiches Einarbeiten und die Umsetzung der einschlägigen Zuverlässigkeitsmerkmale und der zugehörigen Leistungsmerkmale in das System erreicht. Die Kriterien für das Erreichen der Systemzuverlässigkeit sollten Folgendes widerspiegeln:

- a) ein profundes Verständnis des erwarteten Systemverhaltens;
- b) ein profundes Verständnis der Betriebsbedingungen;
- c) die wirksame Umsetzung der Zuverlässigkeitsgrundsätze in die betriebliche Infrastruktur;
- d) die Anwendungsbedingungen;
- e) die Anwendung geeigneter Prozesse für die Realisierung des Systems;
- f) den Einsatz von Fach- und Erfahrungswissen für eine kostengünstige Einführung von Systemdiensten.

Diese Kriterien können erreicht werden, in dem man sich auf diejenigen Schlüsselfaktoren konzentriert, die für die Zuverlässigkeit des Systems von Belang sind. Die Schlüsselfaktoren werden identifiziert und unterstützen die Prozessanwendungen und die Verwirklichung der Systemziele. Dazu wird deren Bedeutung für die Umsetzung der Zuverlässigkeit begründet. Diese Kriterien sollten bei der Projektplanung und Umsetzung beachtet werden. Der Anwender sollte geeignete Zuverlässigkeitstätigkeiten so anpassen, dass den spezifischen Projektbedürfnissen aus Sicht des Systemlebenszyklus entsprochen wird.

- 1) **Grundsätze des Zuverlässigkeitsmanagements** – Dieses Kriterium beeinflusst die betriebliche Infrastruktur, die Zuweisung geeigneter Ressourcen, Benennung der Verantwortlichkeiten in der Organisationsleitung und der Projektführerschaft. Die Bedeutung der Grundsätze des Zuverlässigkeitsmanagements spiegelt die Kundenorientierung auf Zuverlässigkeitsmanagementstrategie und -verpflichtung wider sowie auf gemeinsame Bemühungen und systematische Vorgehensweise in Richtung wirksamer

Anwendung der in IEC 60300-1 beschriebenen Prinzipien des Zuverlässigkeitsmanagements. Die in IEC 60300-1 beschriebenen Grundsätze des Zuverlässigkeitsmanagements gelten für den gesamten in diesem Teil von IEC 60300 beschriebenen technischen Prozess.

- 2) **Zuverlässigkeitswissensbasis** – Dieses Kriterium betrifft die Genauigkeit der Interpretation der Marktbedürfnisse, die Eignung relevanter Informationen für die Einsetzung des Projektes, die Anwendung verfügbarer Normen und Spezifikationen, den Einfluss bei Vertragsverhandlungen und Begründung der Zuverlässigkeit für objektive Beweise. Die Bedeutung der Zuverlässigkeitswissensbasis liegt im Wettbewerbsvorteil und der technologischen Führerschaft, wenn neue Herausforderungen bei den Systemzuverlässigkeitsbelangen auftauchen.
- 3) **Entwurfsarchitektur** – Dieses Kriterium betrifft den Einsatz von Technologien in Systemanwendungen, die Auswahl von Hardware, Software und menschlicher Elemente zur Realisierung der Systemfunktionen, Systemintegration und den Systembetrieb sowie die leichte Erweiterbarkeit des Systems. Entwurfsarchitektur bedeutet ein zusammenhängendes und konstruktives Rahmenwerk für Systemintegrität und Realisierung. Sie ermöglicht erweiterte Fähigkeiten, erleichtert Kapazitätsausweitung, kostengünstigen Betrieb und eine gute Dienstgüte. Der Einsatz geeigneter Technologien erlaubt Entwurfsabwägungen durch Verwendung neuartiger Merkmale und Verbreiterung der technischen Anwendungsgrenzen.
- 4) **Lieferkettenkooperation** – Dieses Kriterium betrifft Kaufentscheidungen (selber herstellen, einkaufen), Vertragsvergabe nach Außen und Vergabeschemata an Unterauftragnehmer, Verifizierungs- und Validierungsverfahren und Dokumentation sowie Überwachungs- und Sicherungsprozesse. Der Wert des Lieferkettenmanagements ergibt sich aus der Kooperation von Käufer und Lieferant und dem Austausch relevanter Informationen im Beschaffungsprozess. Die Lieferkette bildet die notwendige Bindung für das Verfolgen wichtiger Informationen. Die Auswirkung auf das Geschäft ergibt sich aus der Zweckmäßigkeit administrativer Prozesse, geringeren Lieferkosten und Anreizen für die Lieferung von Qualitätsprodukten und Qualitätsdiensten.
- 5) **Ermöglichende Systeme** – Dieses Kriterium betrifft den Einsatz und die Verwendung von Methoden, Verfahren und Werkzeugen, die Zweckmäßigkeit der Entwicklungsergebnisse, die Erfordernisse der Personalschulung, die Einführung neuer Produkte und Systeme und die Strategien der Instandhaltungs- und Logistikunterstützung. Die Bedeutung der ermöglichenden Systeme liegt in der Verbesserung des Entwicklungs- und Lieferprozesses und dem wirksamen Einsatz von Verfahren und Werkzeugen zur schnellen Problemlösung. Ermöglichende Systeme brauchen nicht immer technisch komplex sein und benötigen nicht immer spezielle Fähigkeiten für deren Verständnis und Einsatz. Einige dieser Methoden sind einfache Prüflisten und Anweisungen, die es den Betreibern und Instandhaltern vor Ort ermöglichen, die richtige Entscheidung zu fällen und die richtige Maßnahme zu ergreifen. Weitere Angaben zu ermöglichenden Systemen sind in der Norm ISO/IEC 15288 [3] enthalten.
- 6) **Rückmeldung vom Kunden und Informationsmanagement** – Dieses Kriterium betrifft die Beziehungen zum Kunden hinsichtlich dessen Zufriedenheit und Treue, Bereitstellung wirksamer Kundendienstleistungen, Genauigkeit der Störmeldungen, Erfassung von Betriebsdaten und deren Analyse, wirksame Umsetzung korrekativer und präventiver Maßnahmen, Darstellung von Verhaltenstrends und Aufzeichnung der gemachten Zuverlässigkeitserfahrungen. Die Bedeutung relevanter Rückmeldungen ist Vorbedingung für die Darstellung von Verhaltenstrends, sie liegt im Erkennen kritischer Bereiche, die weiterer Behandlung bedürfen, und liegt in der Bereitstellung objektiver Beweise für Verifizierung und Validierung.

6.2.3 Methodik für das Erreichen der Systemzuverlässigkeit

Die für die Gestaltung der Zuverlässigkeit anwendbaren Methoden und Verfahren können anhand des Wissens der Kriterien und des Verständnisses ihrer Bedeutung für das Erreichen der Systemzuverlässigkeit ausgewählt werden. Zielsetzung ist es, mit diesen Methoden und Verfahren die Zuverlässigkeit in das System hinein zu entwickeln. Die relevanten Zuverlässigkeitsmerkmale sollen so in die Systemfunktionen integriert werden.

Die Methodik der Umsetzung der Zuverlässigkeit in Systemfunktionen kann nach zwei Gesichtspunkten betrachtet werden:

- a) deduktive (von oben nach unten gerichtete) Vorgehensweise, bei der die Systemarchitektur mit ihrer Systemzuverlässigkeit aus der Synthese von festgelegten Systemanforderungen und Marktinformationen entwickelt wird;

- b) induktive (von unten nach oben gerichtete) Vorgehensweise, bei der die Zuverlässigkeit in den Systemfunktionen auf der Grundlage von Entwicklungsregeln hinsichtlich Vereinfachung, Fehlertoleranz und Risikominderung realisiert wird.

Beide Vorgehensweisen schließen die Identifizierung von Zuverlässigkeitsmerkmalen und die Ermittlung ihrer Kenngrößen ein. Zuverlässigkeitsmerkmale sind die grundlegenden Maßgrößen für die Bewertung und das Erreichen der Systemzuverlässigkeit.

Für die Leistungsfähigkeit des Systems relevante Zuverlässigkeitsmerkmale sind zeitabhängig. Sie können aus Zeitmessungen quantifiziert und aus aufgezeichneten Ereignissen abgeleitet werden. Beispiele sind für die Systemverfügbarkeit die relative Klarzeit, für den Nachweis der Funktionsfähigkeit die Wahrscheinlichkeit, wie lange eine Betriebsfunktion ohne Ausfall zur Verfügung steht, und als Maß für die Schnelligkeit der Instandhaltung die vollständige Wiederherstellung des Systembetriebs innerhalb der vorgegebenen Unklarzeit.

Jedoch können nicht alle Zuverlässigkeitsmerkmale leicht nachgewiesen werden, da es zeitliche Einschränkungen, solche durch Kosten, durch technische Bedingungen oder durch projektbedingte Gründe gibt. Als Beispiele sind hochzuverlässige Systeme zu nennen, neue Systeme mit geringer Erfahrung im aktuellen Betrieb und allgemein angelegte Softwaresysteme zur Verwendung in neuen Umgebungen, sowie einige handelsübliche Produkte ohne bekannte Zuverlässigkeitserfahrungen. Hier sind andere Verfahren gefragt, um Vertrauen in deren Verwendung und gesicherte Zuverlässigkeit zu erhalten. Es sollte zur Kenntnis genommen werden, dass Zuverlässigkeitsmerkmale von Systemen stochastischer oder probabilistischer Art sind. Sie können durch lediglich indirekt bewertbare Merkmale gekennzeichnet sein, die nicht einfach aus direkten Messungen abgeleitet werden können. Hierfür typische Verfahren sind beispielsweise Zuverlässigkeits-Fallstudien, simulierte Prüffälle, Reifegradmodelle (en: capability maturity models) und Zuverlässigkeitswachstumsprogramme.

Zahlen und quantifizierbare Werte und Angaben bedürfen oft der Auslegung. Eine Messung der Ausfallrate könnte ohne sauberen Bezug auf den Zusammenhang oder nähere Erklärung der sonstigen mit zu berücksichtigenden Belange nicht aussagekräftig sein. Obwohl die Zahlenwerte von Ausfallraten als Indikatoren für Vergleiche alternativer Entwurfsoptionen verwendet werden können, könnten die zu Grunde liegenden Annahmen für eine Begründung bedenklich sein. Hier kommen statistische Werkzeuge ins Spiel, mit denen die Grenzen von Schlussfolgerungen und die Vertrauensgrenzen potentieller Gefährdungen bestimmt werden können. Als Beispiel sei eine Kopiermaschine genannt, für die der mittlere Ausfallabstand nicht allzu aussagekräftig sein kann, jedoch die von ihr produzierte Anzahl leerer Kopien je Monat ein Maß für die vergeudeten Kosten wäre.

Im Anhang B sind Beispiele für anwendbare Verfahren und Werkzeuge enthalten, mit deren Hilfe die geforderte Systemzuverlässigkeit leichter erreicht werden kann. Die für die Auswahl der geeigneten Verfahren und Werkzeuge erforderlichen Kenntnisse der Systembetriebsfunktionen und der Anwendungsumgebung sind in Anhang C beschrieben. Eine wirksame Anwendung dieser Methoden zur Lösung technischer Probleme bedingt die Konzentration auf kritische Themen und Belange. Die Einschränkungen dieser Verfahren und Werkzeuge bei speziellen Anwendungen sollten vermerkt werden, damit anschließend die Ergebnisse richtig interpretiert werden können.

6.2.4 Realisierung der Systemfunktionen

Systemfunktionen können durch Hardware, Software oder menschliche Elemente oder beliebigen Kombinationen daraus zwecks Erfüllung spezifischer Systemleistungsmerkmale realisiert werden. Nachfolgend werden allgemeine Hinweise beschrieben, die bei der Auswahl und beim Einsatz dieser Elemente im Sinne einer erfolgreichen Erfüllung der Zuverlässigkeitsvorgaben zu beachten sind.

- a) **Hardwareelemente** – Hardwareelemente bzw. Geräte werden üblicherweise bei der Konstruktion von Systemen eingesetzt. Hardwareelemente bzw. Geräte können aus mechanischen, elektrischen, elektronischen, optischen oder anderen physischen Komponenten oder Bauelementen bestehen. Sie werden in vielfältigen Konfigurationen zur Realisierung von Hardware- bzw. Gerätefunktionen eingesetzt. Die meisten heutzutage aus Hardwareelementen aktueller Technologie gebauten elektronischen Produkte sind ziemlich ausgereift. Die Entwicklungsvorgaben sind im Allgemeinen gut beschrieben. Bei gut gesteuertem und überwachtem Fertigungsprozess zeigen elektronische Produkte meist ein gleichmäßiges Verhalten. Qualität und Zuverlässigkeit können durch geeignete und bekannte Verfahren gesichert werden. Auch gibt es umfangreiche Datenbanken über Erfahrungswerte, mit denen man die