

DIN EN 62741

ICS 29.020; 31.020; 33.020; 35.020

Einsprüche bis 2013-09-22

Entwurf**Zuverlässigkeit von Systemen, Geräten und Bauteilen –
Leitfaden zur Darlegung von Zuverlässigkeitsanforderungen –
Der Zuverlässigkeitsnachweis
(IEC 56/1477/CD:2012)**

Reliability of systems, equipment and components –
Guide to the demonstration of dependability requirements –
The dependability case
(IEC 56/1477/CD:2012)

Anwendungswarnvermerk

Dieser Norm-Entwurf mit Erscheinungsdatum 2013-07-22 wird der Öffentlichkeit zur Prüfung und Stellungnahme vorgelegt.

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

Stellungnahmen werden erbeten

- vorzugsweise online im Norm-Entwurfs-Portal des DIN unter www.entwuerfe.din.de bzw. für Norm-Entwürfe der DKE auch im Norm-Entwurfs-Portal der DKE unter www.entwuerfe.normenbibliothek.de, sofern dort wiedergegeben;
- oder als Datei per E-Mail an dke@din.de möglichst in Form einer Tabelle. Die Vorlage dieser Tabelle kann im Internet unter www.din.de/stellungnahme oder für Stellungnahmen zu Norm-Entwürfen der DKE unter www.dke.de/stellungnahme abgerufen werden;
- oder in Papierform an die DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE (Hausanschrift: 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 98 Seiten

DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE

Inhalt

	Seite
Einleitung	5
1 Anwendungsbereich	6
2 Normative Verweisungen	6
3 Begriffe	7
4 Zielsetzung und Beschreibung des Zuverlässigkeitsnachweises	8
5 Grundsätze des Zuverlässigkeitsnachweises	10
5.1 Einleitung	10
5.2 Überblick über die Zuverlässigkeitsstrategie	12
5.3 Der Zuverlässigkeitsplan	13
5.4 Fortlaufende Sicherung der Zuverlässigkeit	13
5.5 Bewertung des Zuverlässigkeitsnachweises	14
6 Entwicklung des Zuverlässigkeitsnachweises	15
6.1 Einleitung	15
6.2 Anfänglicher Zuverlässigkeitsnachweis	16
6.3 Zuverlässigkeitsnachweis und Nachweisberichte in der Ausschreibungsphase	16
6.4 Maßnahmen des Kunden zur Zuverlässigkeit während der Beschaffung	17
6.5 Zuverlässigkeitsnachweis während der Nutzung durch den Kunden	17
6.6 Erweiterung	18
7 Einen Nachweis erbringen	18
8 Einen Nachweis darstellen	19
9 Begutachten der Angemessenheit eines Nachweises	19
Anhang A (informativ)	23
Anhang B (informativ) Allgemeine Anforderungen an den Zuverlässigkeitsnachweisbericht	24
Anhang C (informativ) Beispiele von Zuverlässigkeitsrisiken in verschiedenen Stadien des Lebenszyklus eines Systems	27
Anhang D (informativ) Checkliste von Punkten zur Begutachtung der Angemessenheit des Nachweises	29
Anhang E (informativ) Prozess zur Steuerung und Bewältigung von Zuverlässigkeitsrisiken	30
Anhang F (informativ) Zuverlässigkeitsnachweisrahmen	32
 Bilder	
Bild 1 – Die Ableitung von Behauptungen	10
Bild 2 – Festlegen und Entwickeln des Nachweisrahmens	11
Bild 3 – Die Beziehung zwischen dem Zuverlässigkeitsprozess, dem allgemeinen Lieferprozess und den erbrachten Nachweisen	12
Bild 4 – Veranschaulichung des fortlaufenden Sicherungs-Prozesses	14
Bild 5 – Beispiel zur Änderung der Verteilung der Belastung über dem Systemlebenszyklus	15
Bild 6 – Prozess zur Steuerung und Bewältigung von Zuverlässigkeitsrisiken	22

Tabellen

Tabelle F.1 – Nachweisrahmen für System „X“	34
Tabelle F.2 – Nachweisrahmen für System „Y“	38

Nationales Vorwort

Das internationale Dokument IEC 56/1477/CD:2012 „Reliability of systems, equipment and components – Guide to the demonstration of dependability requirements – The dependability case“ (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 prEN nur 2 Monate beträgt, und dann keine sachlichen Stellungnahmen mehr abgegeben werden können, sondern nur noch eine „JA/NEIN“-Entscheidung möglich ist, wobei eine „NEIN“-Entscheidung fundiert begründet werden muss, wird bereits der CD als DIN-Norm-Entwurf veröffentlicht, um die Stellungnahmen aus der Öffentlichkeit frühzeitig berücksichtigen zu können.

Für 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.

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

Zuverlässigkeit von Systemen, Geräten und Bauteilen – Leitfaden zur Darlegung von Zuverlässigkeitsanforderungen – Der Zuverlässigkeitsnachweis

Einleitung

Zuverlässigkeit ist ein wesentliches Leistungsmerkmal. Das Bereitstellen von Systemen mit akzeptablen Zuverlässigkeitsniveaus ist daher unerlässlich für das Erreichen von Leistungseffizienz und optimierten Lebenszykluskosten.

Ein Zuverlässigkeitsnachweis (en: dependability case) ist eine geeignete und überzeugende Möglichkeit der Aufzeichnung und Präsentierung einer durch Nachweise unterstützten Argumentation, dass die notwendige Zuverlässigkeit erreicht worden ist oder erreicht werden wird.

Die Zuverlässigkeit eines Systems hängt von allen Aspekten dieses Systems ab, darunter Komponenten, Prozesse, Hardware, Software, Personen und alle Schnittstellen, eingeschlossen Benutzerschnittstellen. Zuverlässigkeitsprogramme müssen alle diese Aspekte angemessen behandeln.

Unterschiedliche Systeme und Technologien erfordern unterschiedliche technische Aktivitäten, die für ein bestimmtes System spezifisch sein können. Um die Zuverlässigkeitsanforderungen für ein System erfüllen zu können, müssen die Anforderungen vollständig verstanden sein, und es muss eine geeignete Strategie mit definierten Projektmanagementaufgaben zur Erfüllung dieser Anforderungen entwickelt werden. Dazu gehören auch die Identifizierung von Risikobereichen der Zuverlässigkeit und eine Beschreibung, wie diese Risiken zu handhaben sind.

Die Strategie muss in ihrem Ansatz flexibel sein, um eine sich stufenweise entwickelnde Gewissheit bezüglich der Zuverlässigkeit zu bieten, indem die Ergebnisse von zuverlässigkeitsbezogenen Aktivitäten gegen die Zuverlässigkeitsanforderungen bewertet und die Zuverlässigkeitsprogramme je nach Notwendigkeit angepasst werden müssen. Insbesondere

- a) müssen die Zuverlässigkeitsanforderungen des Kunden ermittelt werden, und es muss dargelegt werden, dass sie vom Kunden und vom Lieferanten verstanden werden,
- b) muss ein Programm von Maßnahmen zur Erfüllung der Anforderungen geplant und eingeführt werden, und die Risiken müssen untersucht werden,
- c) muss dem Kunden zunehmende Gewissheit geboten werden, dass seine Zuverlässigkeitsanforderungen jetzt oder zukünftig erfüllt werden, und dass das Vertrauen in die Zuverlässigkeit im Verlauf des Programms zunimmt.

Der Lieferant muss festlegen, welche Maßnahmen zur Erfüllung des zweiten Ziels notwendig sind, und er muss dies mit dem Kunden abstimmen. Das dritte Ziel muss durch das Vermitteln zunehmender Gewissheit erfüllt werden. Es ist beabsichtigt, dass diese Gewissheit mittels eines Zuverlässigkeitsnachweises geboten wird.

Der Zuverlässigkeitsnachweis wird in Abschnitt 4 in allen Einzelheiten beschrieben. Er begleitet das System während dessen gesamter Lebensdauer und erfasst alle Nachweise bezüglich der Zuverlässigkeit aus Entwurfs- und Entwicklungsaktivitäten, Versuchen usw. bis hin zum Einsatz einschließlich der Felddaten.

Der Fortschritt wird mithilfe von Zuverlässigkeitsnachweisberichten überwacht. Dabei handelt es sich um regelmäßige Evaluierungen des Zuverlässigkeitsnachweises. Sie werden in Abschnitt 5 in allen Einzelheiten beschrieben.

Die vorliegende Norm bietet dem Kunden und den Lieferanten Anleitung, wie der Zuverlässigkeitsnachweis zu handhaben ist, und gibt auch Hilfestellung bei der Bewertung und Beurteilung der Angemessenheit der Ergebnisse der im Rahmen des Programms verwendeten Verfahren. Der Zuverlässigkeitsnachweis wird mithilfe eines fortschreitenden Prozesses geführt, der das Ergebnis in einem Nachweis-Rahmen im Vergleich zu den Zuverlässigkeitszielvorstellungen des Lieferanten erfasst.

In dieser Norm umfasst die Benennung „Zuverlässigkeit“ die folgenden Aspekte: Funktionsfähigkeit, Verfügbarkeit, Instandhaltbarkeit und Instandhaltungsbereitschaft. Der Zuverlässigkeitsnachweis kann auch Prüfbarkeit und Lebensdauer einschließen. Sicherheit wird in diesem Leitfaden nicht direkt angesprochen. Dennoch kann ein Großteil der Anleitung in dieser Norm auch für Sicherheitsnachweise verwendet werden.

1 Anwendungsbereich

Diese Norm enthält eine Beschreibung der Grundsätze des Zuverlässigkeitsnachweises und bietet Anleitung bezüglich seines Inhalts und seiner Anwendung in der Systemtechnik. Der Zuverlässigkeitsnachweis kann während des gesamten Lebenszyklus angewandt werden, von der Konzeptphase über die Entwicklung und Realisierung bis hin zum Einsatz sowie bei Erweiterung und schließlich der Stilllegung.

In dieser Norm werden durchgängig die Benennungen „Kunde“ und „Lieferant“ verwendet. Der Zuverlässigkeitsnachweis kann aber auch von anderen Organisationen als dem originären Kunden angewendet werden, wie etwa von Zertifizierungsstellen, Regulierern und den Nutzern des Systems. Außerdem kann der Zuverlässigkeitsnachweis durch andere Organisationen als den ursprünglichen Lieferanten aktualisiert oder erweitert werden, wie etwa durch den Nutzer des Systems, insbesondere, wenn das System für unterschiedliche Funktionen eingesetzt wird. Daher werden der Einfachheit halber die Benennungen „Kunde“ und „Lieferant“ durchgängig verwendet, wenn auf die Organisation Bezug genommen wird, die den Zuverlässigkeitsnachweis erhält oder verwendet bzw. auf die Organisation, die ihn anlegt bzw. aktualisiert.

Obwohl diese Norm in erster Linie für die Anwendung durch Systementwickler gedacht ist, wird sie auch für Gremien von Nutzen sein, die beauftragt sind, den Zuverlässigkeitsnachweis für ein Projekt zu erbringen, wo dies als notwendig erachtet wird.

Die für das Erreichen der Zuverlässigkeit erforderlichen Maßnahmen hängen von der Art und dem Entwicklungsstand des Systems ab, und sie variieren aller Wahrscheinlichkeit nach sehr stark von Projekt zu Projekt. Die Leitlinien sind ihrem Wesen nach nicht zwingend: sie sind allgemeiner Art und streben nicht an, erschöpfend zu sein.

Obwohl diese Norm Sicherheitsthemen nicht ausdrücklich anspricht, können doch die gleichen Grundsätze angewendet werden.

Dieses Dokument ist als Leitfaden gedacht; es ist nicht für Zertifizierungszwecke und nicht zur Beurteilung von Regelkonformität gedacht.

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 – Part 191 – Dependability*

IEC 60300-1, *Dependability management – Part 1: Guidance for management and application*

3 Begriffe

Für die Anwendung dieses Dokuments gelten die Begriffe nach IEC 60050-191^{N1)} und die folgenden Begriffe.

3.1

Zuverlässigkeitsnachweis

(en: **dependability case**)

nachweisbasierte, logisch aufgebaute und nachvollziehbare Argumentation zur Unterstützung der Behauptung, dass ein bestimmtes System die Zuverlässigkeitsanforderungen erfüllen wird

3.2

Zuverlässigkeitsnachweisrahmen

(en: **dependability evidence framework**)

Struktur, die beschreibt, welcher Nachweis erbracht werden wird / erbracht worden ist und wann

3.3

Zuverlässigkeitsrisiko

(en: **dependability risk**)

Möglichkeit der Nicht-Erfüllung einer festgelegten Anforderung an ein Zuverlässigkeitsmerkmal

3.4

handelsüblich (OTS)

(en: **off the shelf**)

nicht zu entwickelnder Liefergegenstand, der sowohl handelsüblich ist als auch in nennenswerten Mengen auf dem gewerblichen Markt verkauft wird

Anmerkung zum Eintrag: Wird manchmal auch als COTS (en: Commercial Off The Shelf) oder MOTS (en: Modified Off The Shelf) bezeichnet.

3.5

Kunde

(en: **customer**)

Beteiligter, der die Einheit samt Zuverlässigkeitsanforderungen bestellt

Anmerkung zum Eintrag: Dies kann eine Organisation sein, ein Geldgeber, eine Abteilung, eine Gesellschaft oder ein Individuum und kann sich während des Lebenszyklus ändern.

3.6

Subsystem

(en: **sub-system**)

Teil eines Systems, der selbst ein System ist

3.7

Lieferant

(en: **supplier**)

Beteiligter, der die Einheit liefert, die die Zuverlässigkeitsanforderungen erfüllen soll

Anmerkung zum Eintrag: Dies kann eine Organisation sein, eine Abteilung, eine Gesellschaft oder ein Individuum und kann sich während des Lebenszyklus ändern.

3.8

System

(en: **system**)

Satz von in Wechselbeziehung oder Wechselwirkung stehenden Elementen

[ISO 9000:2005, 3.2.1]

Anmerkung zum Eintrag: Ein System kann Hardware, Software und den Faktor Mensch umfassen.

^{N1)} Nationale Fußnote: Im en. Original wird irrtümlicherweise auf IEC 60051-191 verwiesen; dies wurde in der dt. Fassung richtiggestellt.

3.9

Validierung

(en: validation)

Bestätigung durch Bereitstellung eines objektiven Nachweises, dass die Anforderungen für einen spezifischen beabsichtigten Gebrauch oder eine spezifische beabsichtigte Anwendung erfüllt worden sind

Anmerkung zum Eintrag 1: ISO 9000:2005, 3.8.5, ohne die dortigen Anmerkungen^{N2)}.

Anmerkung zum Eintrag 2: Validierung ist die Tätigkeit des Darlegens, dass das betrachtete System, vor oder nach der Inbetriebnahme, die Anforderungsspezifikation für dieses System in jeder Hinsicht erfüllt. Daher bedeutet Software-Validierung beispielsweise Bestätigung durch Prüfung und Bereitstellen eines objektiven Nachweises, dass die Software der Software-Anforderungsspezifikation genügt.

3.10

Verifizierung

(en: verification)

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

Anmerkung zum Eintrag 1: ISO 9000:2005, 3.8.4, ohne die dortigen Anmerkungen^{N3)}.

Anmerkung zum Eintrag 2: Im Kontext dieser Norm ist Verifizierung – für jede Phase des betreffenden Lebenszyklus – die Tätigkeit des Darlegens durch Analyse und/oder Prüfung, dass die Ergebnisse für die speziellen Eingaben in jeder Hinsicht die für die spezielle Phase gesetzten Ziele und Anforderungen erfüllen.

Anmerkung zum Eintrag 3: Beispielhafte Tätigkeiten der Verifizierung umfassen^{N4)}:

- a) Bewertung von Ergebnissen (Dokumente aus allen Phasen des Lebenszyklus), um – unter Berücksichtigung der spezifischen Eingaben für diese Phase – die Übereinstimmung mit den Zielen und Anforderungen der Phase sicherzustellen;
- b) Entwicklungsbewertungen;
- c) an den entworfenen Systemen durchgeführte Prüfungen, um sicherzustellen, dass sie entsprechend ihrer Spezifikation arbeiten;
- d) Integrationsprüfungen, bei denen verschiedene Teile eines Systems schrittweise zusammengebaut werden und mittels Durchführung von Umgebungsprüfungen, um sicherzustellen, dass alle Teile zusammenarbeiten.

4 Zielsetzung und Beschreibung des Zuverlässigkeitsnachweises

Die Zielsetzung des Zuverlässigkeitsnachweises ist, eine nachweisbasierte, logisch aufgebaute und nachvollziehbare Argumentation bereitzustellen, die die Behauptung unterstützt, dass ein bestimmtes System die Zuverlässigkeitsanforderungen erfüllen wird.

Der Zuverlässigkeitsnachweis ist von größtem Vorteil für hochwertige, in geringer Anzahl eingesetzte Systeme, für die ein direkter Nachweis der Zuverlässigkeit schwierig ist oder nur mit hohen Kosten zu erhalten ist. So kann ein geringwertiges, in hoher Stückzahl eingesetztes System, wie etwa ein Mobiltelefon, geprüft werden, um seine Betriebszuverlässigkeit oder Instandhaltbarkeit zu bestimmen, bevor es auf den Markt gebracht wird. Ein Atomkraftwerk dagegen ist etwas Einmaliges, und es ist diese Art von System, für die das Konzept des Zuverlässigkeitsnachweises entwickelt worden ist, um beim Managen zu helfen.

^{N2)} Nationale Fußnote: Im en. Original heißt es irrtümlicherweise „excluding some of the notes“. Dies wurde in der dt. Übersetzung richtiggestellt.

^{N3)} Nationale Fußnote: Im en. Original heißt es irrtümlicherweise „excluding some of the notes“. Dies wurde in der dt. Übersetzung richtiggestellt.

^{N4)} Nationale Fußnote: Im en. Original heißt es irrtümlicherweise „NOTE 2“, und die Unterpunkte sind mit d) bis g) bezeichnet. Dies wurde in der dt. Übersetzung richtiggestellt.

Für solche Systeme ist das Zuverlässigkeitsmanagement wesentlich für die Erfüllung der Zuverlässigkeitsanforderungen und, da Zuverlässigkeitsanforderungen keine absoluten Maße sind, machen Management, Überwachung und Reduzierung der Risiken, die Anforderungen nicht zu erfüllen, den Großteil der Beweisführung beim Zuverlässigkeitsnachweis aus.

Beginnend mit dem anfänglichen Anforderungskatalog umfasst der Zuverlässigkeitsnachweis festgelegte, vermeintliche und tatsächliche Risiken, Strategien für die Steuerung und Bewältigung dieser Risiken sowie für den zugehörigen Nachweis. Dieser Nachweis bezieht sich auf zugehörige und absichernde Informationen, einschließlich Zuverlässigkeitsbefunden aus Entwicklung, Prüfung, usw. bis hin zu Betriebs- und Instandhaltungsdaten, soweit erforderlich, und verzeichnet auch alle Änderungen. So erweist sich der Zuverlässigkeitsnachweis, selbst als ein Steuerungs-Dokument auf höchster Ebene, der in regelmäßigen Abständen durch die Herausgabe von Berichten zum Stand des Zuverlässigkeitsnachweises, die in direktem Zusammenhang mit den Befunden stehen, zusammengefasst wird. Er erfasst den Fortschritt und begleitet das Gerät/System während seines Lebenslaufes bis zur Entsorgung und ist daher ein sich stufenweise erweiterndes Beweismaterial.

Der Zuverlässigkeitsnachweisrahmen ist eine Matrix bestehend aus Zuverlässigkeitsrisiken, Anforderungen an die Nachweise bzgl. der Steuerung und Bewältigung der Risiken, notwendigen Aktivitäten, um die geforderten Nachweise zu erhalten, den Annahmekriterien für die Nachweise, Hinweisen auf die tatsächlich bereitgestellten Nachweise sowie auf die Bestätigung ihrer Annahme (oder Ablehnung). Er liefert die Nachvollziehbarkeit des Zuverlässigkeitsnachweisprozesses über die gesamte Systemlebensdauer. Er ist gleichermaßen auf die Risiken des Kunden wie auf die des Lieferanten anwendbar und wird üblicherweise in Form einer Matrix dargestellt.

Zuverlässigkeitsnachweisberichte sind periodische Fortschreibungen des Zuverlässigkeitsnachweises (üblicherweise zu im Programm vorab festgelegten Zeitpunkten, wie im Nachweisrahmen vereinbart). Sie berichten über den Nachweis und über die Schlussfolgerungen, die aus der Arbeit seit dem letzten Bericht gezogen worden sind (gegebenenfalls unter Verweis auf Papiere und Datenquellen), liefern eine Begutachtung der erreichten Gesamtzuverlässigkeit bzw. ihres Fortschritts sowie eine Bewertung und Evaluierung des Zuverlässigkeitsplans. Wenn im Vertrag gefordert, können sie dafür genutzt werden, diejenigen Angaben bereitzustellen, die eine Entscheidung darüber erlauben, ob im Projektlebenszyklus zur nächsten Phase fortgeschritten werden kann.

Es gibt zahlreiche Techniken, die dazu genutzt werden können, die Argumente und Behauptungen, die sich aus den gesammelten Daten ergeben, zu strukturieren. Anhang A nennt aussagekräftige Literaturstellen zu einigen dieser Techniken.

Diese Norm beschreibt den Zuverlässigkeitsnachweis über einen vollständigen Systemlebenszyklus. Um die Handlungsempfehlungen dieser Norm auf ein bestimmtes Projekt anzuwenden, sollten Projektmanager das Zuverlässigkeitsnachweisprogramm entsprechend zuschneiden.

Ein typischer Systemlebenszyklus besteht aus den folgenden Phasen:

- a) Konzept,
- b) Entwicklung,
- c) Realisierung,
- d) Einsatz,
- e) Erweiterung,
- f) Stilllegung.

Unterschiedliche Beschaffungs- oder Projektarten können unterschiedliche Kombinationen dieser Lebenszyklusphasen nach sich ziehen. Wenn etwa ein Kunde ein handelsübliches (OTS) System kauft, kann die Entwicklung schon vorher abgeschlossen worden sein, und der Zuverlässigkeitsnachweis umfasst nur die Realisierungs- und die Einsatzphase.

5 Grundsätze des Zuverlässigkeitsnachweises

5.1 Einleitung

Als eine nachweisbasierte, logisch aufgebaute und nachvollziehbare Argumentation zur Unterstützung der Behauptung, dass ein bestimmtes System den Zuverlässigkeitsanforderungen genügt, liefert der Zuverlässigkeitsnachweis einen Weg der ingenieurmäßigen Überlegungen, ausgehend von den Anforderungen bis hin zum Nachweis ihrer Erfüllung. Er liefert die Nachverfolgbarkeit dafür, warum bestimmte Verifizierungs- und Validierungsaktivitäten durchgeführt worden sind, und inwiefern sie als erfolgreich angesehen werden können. Er wird im Konzeptstadium begonnen, während des Systemlebenszyklus kontinuierlich überarbeitet und üblicherweise an vorher festgelegten Meilensteinen in Zuverlässigkeitsnachweisberichten zusammengefasst. Bild 1 zeigt das Konzept, Behauptungen beim Zuverlässigkeitsnachweis unter Verwendung der Nachweisquelle zu begründen und geltend zu machen. Dieser Nachweis kann Analysen, Strategien, Pläne, Prüfdaten, Annahmen, Argumente und Behauptungen beinhalten, die den Zuverlässigkeitsnachweis ausmachen.

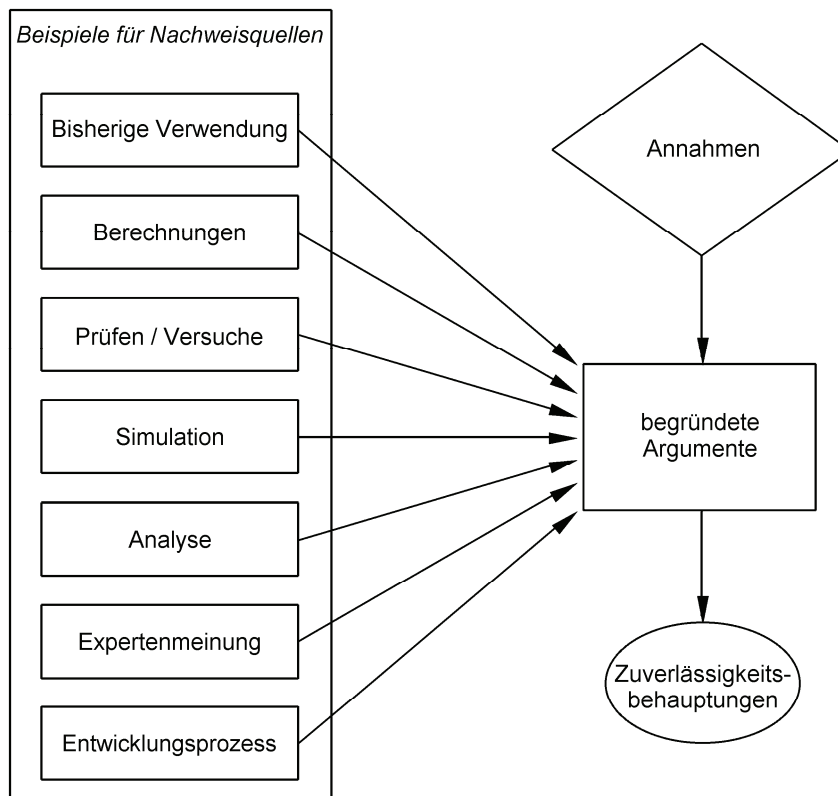


Bild 1 – Die Ableitung von Behauptungen

In der Praxis kann das Zusammentragen aller Dokumentation nur mühsam zu handhaben sein, besonders dort, wo es viele und unterschiedliche Quellen der Nachweise gibt. Eine annehmbare Lösung ist es, den Zuverlässigkeitsnachweis als die Menge angesamelter Zuverlässigkeitsnachweisberichte zu präsentieren, die wiederum auf ursprüngliche Nachweise verweisen. In solchen Fällen existiert der Zuverlässigkeitsnachweis nur als gedanklicher Entwurf.

Der Nachweisrahmen erfasst den gegenwärtigen Satz von Maßnahmen zur Einhaltung der Regelkonformität sowie Maßnahmen (und ihre Erfolgskriterien) zur Minderung von Zuverlässigkeitsrisiken. Er wird üblicherweise in Form einer Matrix präsentiert. Die Anzahl, der Inhalt sowie Ziele und Zeitskalen der Zuverlässigkeitsnachweisberichte werden durch den Nachweisrahmen festgelegt und vorgeschrieben. Dies beginnt mit der anfänglichen Arbeit an Zuverlässigkeitsstrategie und -plan und wird während des Projektes laufend aktualisiert. Jeder Zuverlässigkeitsnachweisbericht gibt den letzten Stand des Nachweisrahmens wieder (dies ist in Bild 2 veranschaulicht). Dieses Element des Zuverlässigkeitsnachweises enthält Einzelheiten der anfänglichen Anforderung und eine Begründung für das vorgeschlagene System.

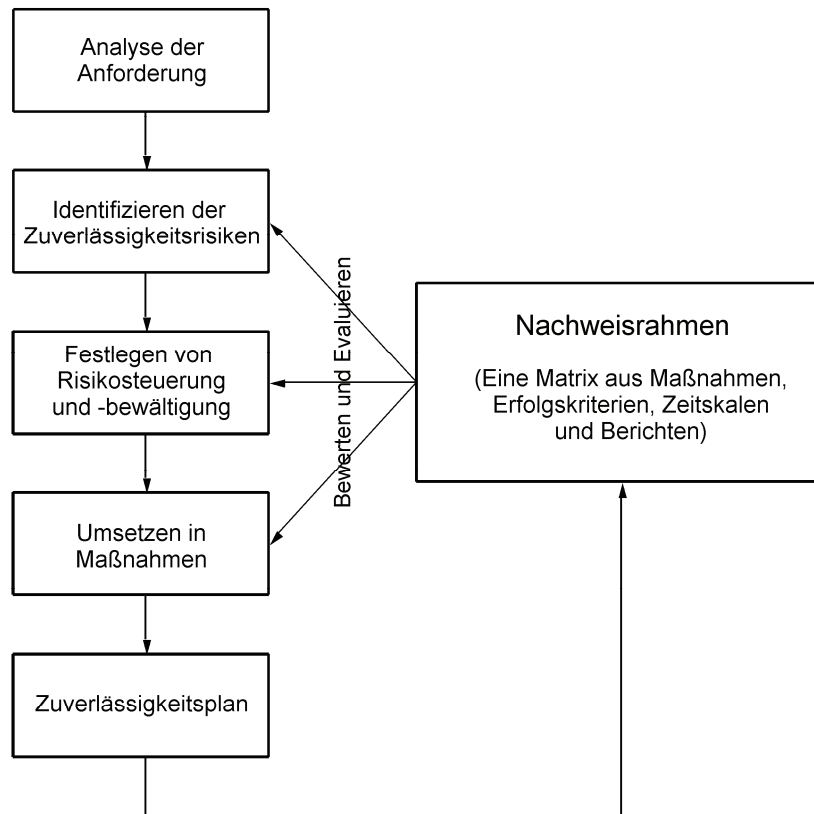


Bild 2 – Festlegen und Entwickeln des Nachweisrahmens

Zuverlässigkeitsmaßnahmen sollten in die allgemeinen Projektmanagementaktivitäten eingebunden sein. Bild 3 veranschaulicht die Beziehung zwischen Zuverlässigkeitsmaßnahmen und dem Gesamtprozess und wie beide durch Nachweise unterstützt werden.

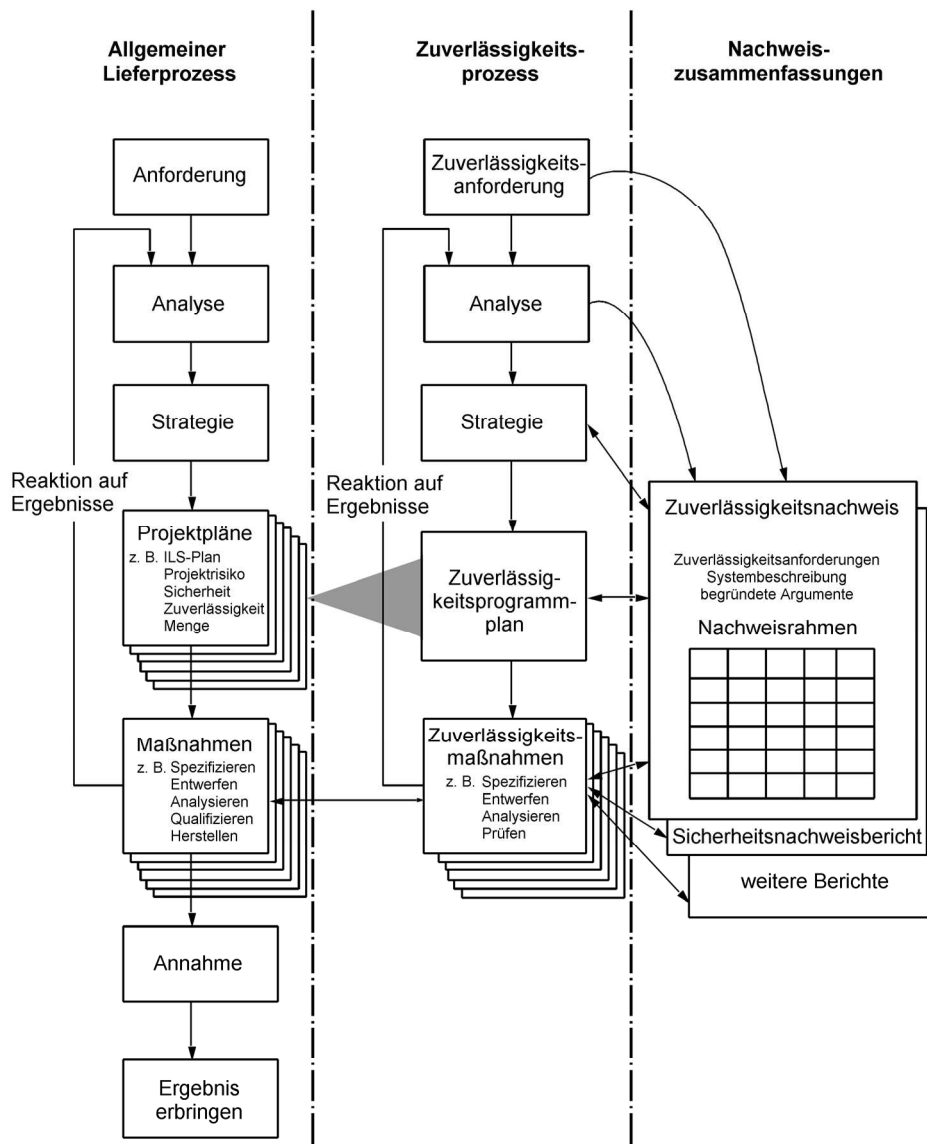


Bild 3 – Die Beziehung zwischen dem Zuverlässigkeitsprozess, dem allgemeinen Lieferprozess und den erbrachten Nachweisen

5.2 Überblick über die Zuverlässigkeitsstrategie

Alle „Projekte“ sollten im Zuverlässigkeitsplan eine übergreifende Zuverlässigkeitsstrategie haben und fort-schreiben. Damit soll sichergestellt werden, dass das beschaffte System die geforderten Zuverlässigkeits-eigenschaften auch über seine gesamte Lebensdauer einhält. Die Strategie sollte auch genau beschreiben, wie die Zuverlässigkeitsmerkmale auch während der Anwendung überwacht werden sollten.

Der Kunde sollte die Zuverlässigkeitsanforderungen festlegen und wie sie überprüft werden sollen. Die Zu-verlässigkeitsanforderungen sollten den voraussichtlichen Systemeinsatz und sein Umfeld einbeziehen. Falls es seitens des Kunden keine speziellen Vorgaben gibt, sollte die Verpflichtung beim Lieferanten liegen, die Initiative zu ergreifen und geeignete Zuverlässigkeitsentwurfsziele vorzuschlagen und wie diese überprüft werden sollen.

Auf der Basis der Analyse der Zuverlässigkeitsanforderungen sollte sich der Lieferant für eine robuste Entwurfsphilosophie für die spätere Lösung entscheiden. Die Betrachtung der Risiken bezüglich der Erfüllung der Zuverlässigkeitsanforderungen führt zu einer Strategie für das Risikomanagement und für das Vermitteln der notwendigen Gewissheit. Das Programm der Maßnahmen sollte Verifizierung und Rückinformationen zur Bewertung des Zuverlässigkeitsplans im Licht des Erreichten enthalten.

Die Zuverlässigkeitsstrategie sollte die Zuverlässigkeitsmaßnahmen und, wie diese die folgenden Punkte behandeln, ansprechen:

1. Die Begutachtung der gegenwärtig vorliegenden Nachweise;
2. Bildung und Aufrechterhaltung einer Struktur neuer Nachweise, Annahmen, Behauptungen und Argumentationen, die für die Sicherung der Zuverlässigkeit benötigt werden;
3. Festlegung geeigneter Zuverlässigkeitsverfahren, die für das Liefern des Nachweises notwendig sind;
4. die Annahmen sollten gerechtfertigt sein und die Behauptungen sollten auf der Basis dessen, was in der Vergangenheit erreicht worden ist, realisierbar und realistisch sein;
5. die Strategie sollte mit den Zuverlässigkeitsanforderungen verknüpft sein und durch eine Wiederbegutachtung der Zuverlässigkeitsrisiken unter der Annahme, dass die Strategie umgesetzt worden ist, gerechtfertigt sein;
6. Zeitskalen und Annahmekriterien für die erforderlichen Nachweise sollten abgeleitet werden;
7. eine Zuverlässigkeitsprüfstrategie, die Vorschriften für Zuverlässigkeitsfunktionsprüfungen umfasst, sollte ebenfalls abgeleitet werden;
8. spezielle Anforderungen an den Zuverlässigkeitsplan; die Festlegung und die Entwicklung des Nachweisrahmens zur Handhabung der Anforderungen an die Nachweise.

5.3 Der Zuverlässigkeitsplan

Der Zuverlässigkeitsplan und der Zuverlässigkeitsnachweisbericht sind zwei wichtige Dokumente, die das Erreichen von Zuverlässigkeit unterstützen. Der Zuverlässigkeitsplan sollte eine klare Beschreibung der Management- und Organisationsstruktur für Zuverlässigkeit enthalten sowie ein systematisches Programm von Maßnahmen zur Erfüllung der Anforderungen und zur Bereitstellung zunehmender Gewissheit über die Zuverlässigkeit.

Im Konzeptstadium kann der Zuverlässigkeitsplan den Zuverlässigkeitsnachweisbericht des Lieferanten als einen Abschnitt oder als Anhang enthalten. Während des Projektes kann der Zuverlässigkeitsnachweisbericht an vorher festgelegten Meilensteinen des Projektes zusammen mit einem Fortschrittsbericht vorgelegt werden, und schließlich am Ende des Vertrags als Nachweis, dass die Zuverlässigkeitsanforderungen erfüllt worden sind. Dies kann Änderungen am Zuverlässigkeitsplan notwendig machen.

Der Zuverlässigkeitsplan kann als ein lebendes Dokument verstanden werden. Falls Ergebnisse aus technischen und anderen Risikosteuerungs- und -bewältigungsmaßnahmen darauf hindeuten, dass eine oder mehrere Zuverlässigkeitsmaßgrößen nicht auf dem erwarteten, zur Erfüllung der Zuverlässigkeitsanforderungen notwendigen Niveau liegen, sollten zusätzliche oder modifizierte Maßnahmen ergriffen werden. Der Zuverlässigkeitsplan sollte angepasst werden, um diese zur Erfüllung der Zuverlässigkeitsanforderungen notwendigen Änderungen widerzuspiegeln.

Einige Maßnahmen, die traditionell als Teil des Zuverlässigkeitsprogramms gesehen werden, tragen nicht direkt zur Gewissheit über die Zuverlässigkeit bei, sondern sind eingeschlossen, um Informationen für andere Disziplinen zu generieren, wie etwa für Sicherheit und Instandhaltungsbereitschaft. Obwohl diese Maßnahmen im Zuverlässigkeitsplan erscheinen können, müssen sie nicht notwendigerweise dazu genutzt werden, Gewissheit über die Zuverlässigkeit zu generieren, die im Zuverlässigkeitsnachweis erscheint.

5.4 Fortlaufende Sicherung der Zuverlässigkeit

In jedem Projekt besteht die Gefahr von Defiziten beim Erreichen von Zuverlässigkeitseigenschaften. Das Erkennen von Zuverlässigkeitsrisiken sollte der Anlass sein, ein Programm spezifischer Zuverlässigkeitsmaßnahmen auszuwählen, ebenso wie Prüfmaßnahmen für den zentralen Entwurf, die die Risiken mindern. Das Ziel ist, eine Menge von Indizien zu schaffen, die die Sicherheit dafür geben, dass die Zuverlässigkeitsanforderungen erfüllt werden und welches die Unsicherheit um die Zuverlässigkeitsanforderungen stufenweise reduziert.

Die Risiken, die Zuverlässigkeitsanforderungen nicht zu erfüllen, sollten verstanden werden, ihre Bedeutung sollte abgeschätzt werden, und, falls notwendig, sollten die Risiken mittels Anwendung von Risikomanagementmethoden gesteuert und bewältigt werden. Der Risikomanagementprozess beginnt im Angebotsstadium

und setzt sich fort durch Entwicklung, Realisierung und Einsatz. Dies ist ein aktiver Prozess, der auf sich ändernde Risikoniveaus reagiert sowie auf mit dem Projektfortschritt auftretende neue Risiken.

Bild 4 zeigt die Art und Weise, wie sich das Unsicherheitsniveau im Laufe des Projekts ändert. Die senkrechte Achse steht für das festgestellte Niveau der Unsicherheit zu einem beliebigen Zeitpunkt des Projektes. Da der Umfang der Nachweise zur Zuverlässigkeit zunimmt, nimmt die Unsicherheit ab, und damit ergibt sich zunehmende Gewissheit. Die waagerechte Achse steht für die Zeit im Projekt, vom Angebotsstadium „a“ über den Projektbeginn „b“, zur formalen Annahme „c“, den anfänglichen Betrieb und die mögliche Überarbeitung/Erweiterung „d“ und darüber hinaus.

Das Bild zeigt zwei Arten von Produktentwicklungen: Neu-Entwicklung und die Modifizierung handelsüblicher Produkte (OTS). Zum Zeitpunkt „a“ (Angebotsstadium) ist das Niveau der Unsicherheit relativ hoch, aber mit dem Fortschritt des Projektes nimmt diese Unsicherheit ab, bis zum Zeitpunkt „c“ (Annahme) die Menge an Indizien ausreicht, die Zuverlässigkeit bei Aufnahme des Betriebes sicherzustellen. Die Menge an Indizien (Gewissheit) sollte auch während des Einsatzes ergänzt werden, indem Informationen aus erfolgreichen Versuchen und dem Einsatz erfasst werden, und sich die verbliebenen Zuverlässigkeitsrisiken offensichtlich weiter verringern.

Es sollte berücksichtigt werden, dass sich die Unsicherheit nicht immer verringern muss. Es kann Situationen geben, in denen die Wahl einer anderen Entwurfsoption, eine Technologie-Einführung oder eine Modell-änderung/Hochrüstung einen Teil der Indizien obsolet macht, und demzufolge neue Indizien gesammelt werden müssen. Auch kann es Zeitabschnitte geben, in denen keine Indizien hinzukommen, beispielsweise während Prüfungen, bevor die Prüfergebnisse freigegeben werden. Außerdem ist es eher der Normalfall als die Ausnahme, dass sich Anforderungen, Umfeld etc. während jeder Phase der Produkt- bzw. Projekt-lebensdauer ändern können, und dem muss deshalb das Zuverlässigkeits-Risikomanagement Rechnung tragen.

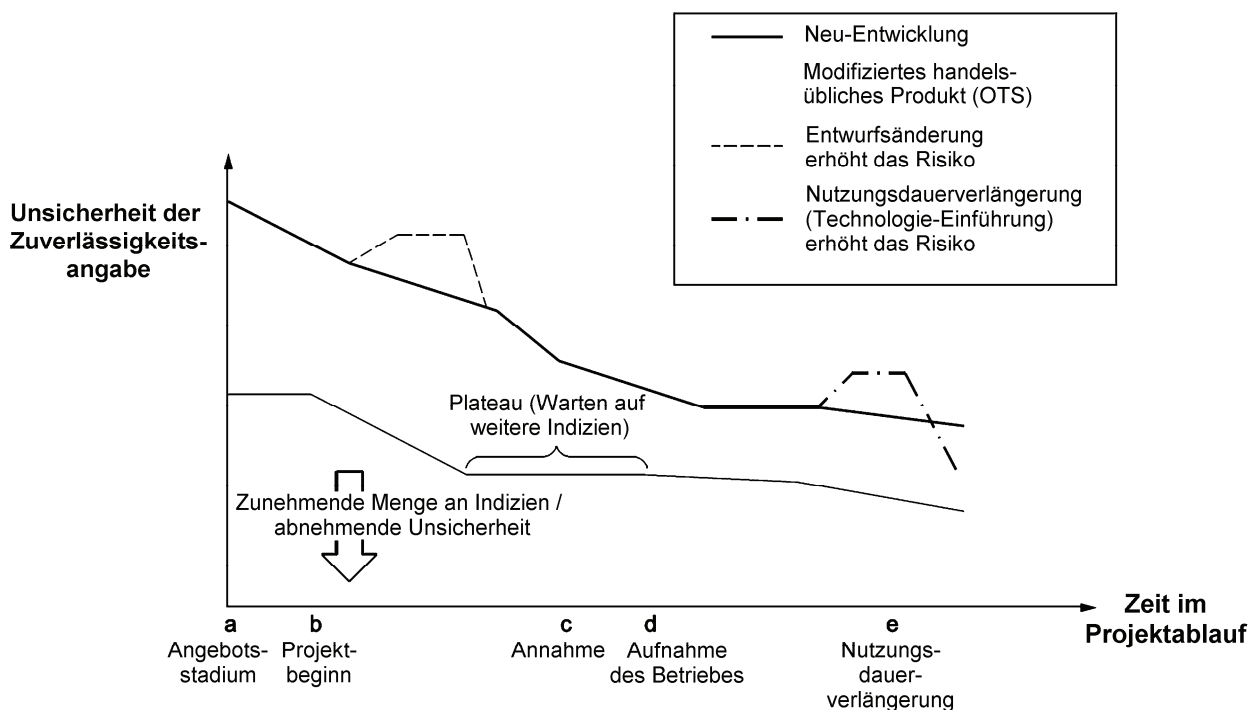


Bild 4 – Veranschaulichung des fortlaufenden Sicherungs-Prozesses

5.5 Bewertung des Zuverlässigkeitsnachweises

Der Zuverlässigkeitsnachweis muss bewertet werden, und er muss im Falle wesentlicher Änderungen bei den folgenden Punkten aktualisiert werden:

- Entwurf,
- Einsatz- oder Umgebungsbedingungen,

- c) Schnittstellensysteme,
- d) Kundenanforderungen oder -erwartungen,
- e) tatsächliche Leistung und Entwurfsziel.

6 Entwicklung des Zuverlässigkeitsnachweises

6.1 Einleitung

Die Verteilung der Belastung beim Entstehen des Zuverlässigkeitsnachweises während des Lebenszyklus eines typischen Systems ist in Bild 5 veranschaulicht. Dieses Bild bezieht sich auf diejenige Lösung, die der Lieferant entwickelt oder vorschlägt, um die Anforderungen des Kunden zu erfüllen. Während der Konzept- und Definitionsphase könnte der Lieferant (bzw. könnten die Lieferanten) mehrere Lösungen entwickeln, von denen der Kunde eine auswählt, die dann realisiert und eingesetzt wird.

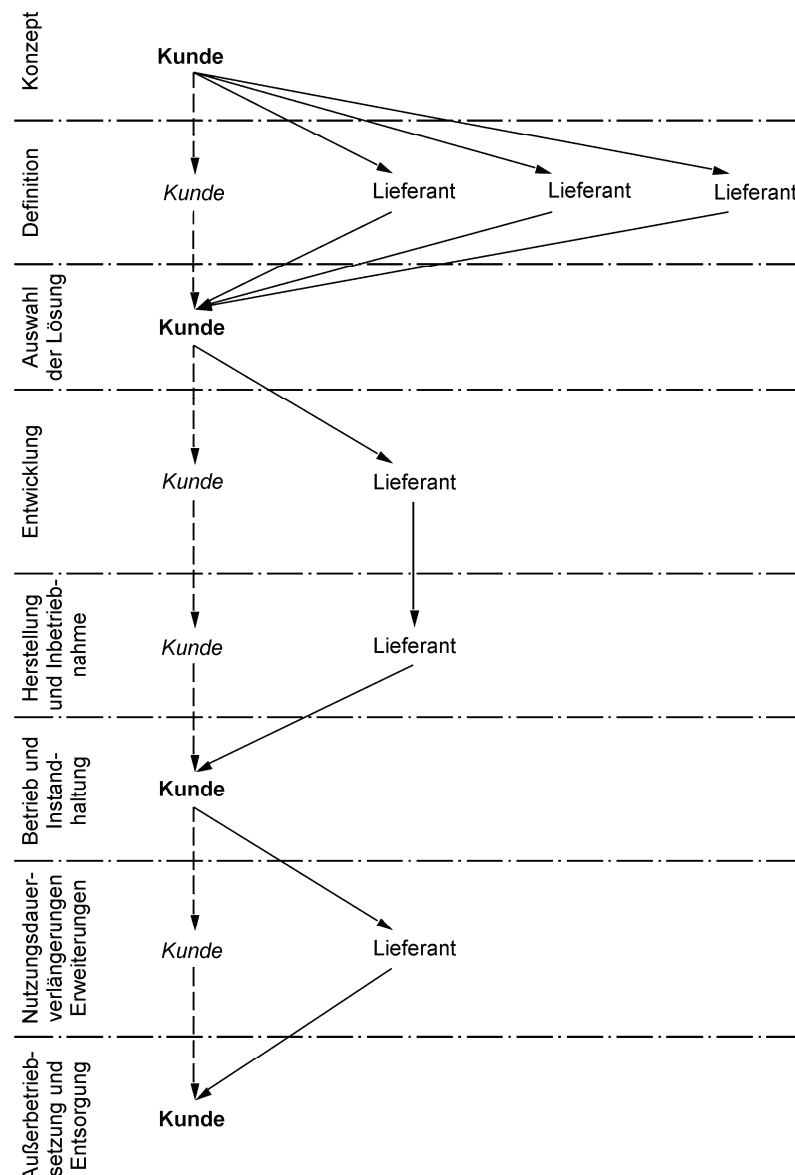


Bild 5 – Beispiel zur Änderung der Verteilung der Belastung über dem Systemlebenszyklus

6.2 Anfänglicher Zuverlässigkeitsnachweis

Der Kunde sollte die Zuverlässigkeitsanforderungen, und wie diese überprüft werden sollen, festlegen. IEC 62347 und IEC 60300-3-4 geben Anleitung bezüglich der Spezifizierung von Zuverlässigkeit. Die Zuverlässigkeitsanforderungen sollten die Anforderungen bezüglich Verfügbarkeit, Funktionsfähigkeit, Instandhaltbarkeit und Instandhaltungsbereitschaft umfassen, aber ebenso andere Aspekte, wie etwa:

- a) Systemeinsatz, einschließlich der weniger offensichtlichen Aspekte des Einsatzes, wie Lagerung und Transport;
- b) Ausfalldefinition;
- c) Umgebung (einschließlich atmosphärischer, regionaler/gebietsspezifischer sowie Instandhaltungs- und Unterstützungsfestlegungen) und
- d) Mensch-Maschine-Schnittstellen.

Alle diese Dinge können einen Einfluss auf die Systemzuverlässigkeit haben.

Wenn seitens des Kunden keine speziellen Weisungen vorliegen, ist es Aufgabe des Lieferanten, die Initiative zu ergreifen und Zuverlässigkeitsentwurfsziele vorzuschlagen und wie diese überprüft werden sollen. Falls notwendig, sind Verweise auf andere Dokumente oder Belege ebenfalls eingeschlossen (wie etwa die Dokumente, die die vorgeschlagenen Risiko-, Sicherheits-, Instandhaltungsbereitschafts- sowie Umweltmanagementvereinbarungen genau beschreiben). In diesem Fall müssen sich Lieferant und Kunde über die Anforderungen einig werden, bevor das Projekt in die nächste Phase eintritt. Normen, die Prozesse beschreiben, die verwendet werden könnten, um robuste Vereinbarungen zwischen Kunde und Lieferant zu erreichen, sind in Anhang A aufgelistet.

Es ist wesentlich, dass alle an der Zuverlässigkeit Beteiligten und von ihr Betroffenen zu diesem Zeitpunkt konsultiert werden, um sicherzustellen, dass die Anforderungen vollständig erfasst sind. Fachmännischer Rat und die Anwendung von Zuverlässigkeitsmodellierungstechniken sind wahrscheinlich erforderlich, um zu verifizieren, dass die Anforderungen angemessen und ausreichend sind. Der Kunde sollte auch die in das Risikoregister des Gesamtprojektes aufzunehmenden Zuverlässigkeitsrisiken festlegen. Zu diesem Zeitpunkt können Risiken bestimmt werden, die allen möglichen Lösungen gemeinsam sind, und die spezielle und zeitgerechte Maßnahmen zu ihrer Minderung erfordern. Diese Risiken können zu einem anfänglichen Nachweisrahmen erforderlicher minimaler Sicherungsmaßnahmen führen, und diese Maßnahmen können umgekehrt einen Teil der vertraglichen Anforderungen oder des Lieferumfangs bilden. Wo es ein umfangreiches Programm einschließlich einer nicht unerheblichen, dem Wettbewerb unterliegenden Entwurfs- oder Entwicklungsphase gibt, ist dieser Aspekt ausschlaggebend, und er kann in einer gewissen Ausführlichkeit notwendig sein, um sicherzustellen, dass Zuverlässigkeit Teil einer allgemeinen Bewertungsmethodik für Bieter wird.

6.3 Zuverlässigkeitsnachweis und Nachweisberichte in der Ausschreibungsphase

Bei Erhalt einer Lieferanfrage, die auch einen ersten Zuverlässigkeitsnachweisbericht umfasst, sollte der Lieferant die Zuverlässigkeitsanforderungen analysieren und eine Strategie zur Erfüllung dieser Anforderungen entwickeln. Wenn der Kunde keine spezifischen Vorgaben macht, ist es Aufgabe des Lieferanten, geeignete Zuverlässigkeitsanforderungen zusammen mit einer Strategie zu entwickeln, diese zu erfüllen. Beim Entwickeln der Strategie sollten die folgenden Aspekte Berücksichtigung finden:

- a) Verstehen der Anforderungen;
- b) Analyse der Anforderungen zur Festlegung von Zielen für die Systemzuverlässigkeit;
- c) Berücksichtigung vorhandener Nachweise;
- d) Festlegung von Risikobereichen (innerhalb des Risikoregisters des Gesamtprojektes).

Anhang C enthält Beispiele von Zuverlässigkeitsrisiken in verschiedenen Lebenszyklusphasen.

Die Entwicklung der Strategie führt zu einem Plan von Zuverlässigkeitsmaßnahmen und einem skizzierten Zuverlässigkeitsnachweisbericht. Der Inhalt des Zuverlässigkeitsplans (der in die Antwort an den Kunden aufzunehmen ist) ergibt sich aus den Aufgaben, die Zuverlässigkeitsanforderungen zu erfüllen und die Zuverlässigkeitsrisiken zu mindern. In diesem Stadium sollte der Zuverlässigkeitsnachweisbericht die Entwicklung der Strategie zur Erlangung von Gewissheit über die Zuverlässigkeit diskutieren und die Rechtfertigung der inner-

halb des Zuverlässigkeitsprogramms vorgeschlagenen Maßnahmen dokumentieren. Das Ziel der Entwicklung der Strategie ist, dem Lieferanten und dem Kunden Vertrauen zu vermitteln, dass das Risiko, die Zuverlässigkeitsanforderungen nicht zu erfüllen, minimiert ist, bevor Mittel bereitgestellt werden.

Es ist unabdingbar, dass der Lieferant die Anforderungen vollständig versteht. Diese Anforderungen sollten im weitesten Sinne betrachtet werden, insofern, als sie nicht nur Zuverlässigkeitsanforderungen enthalten sollten, sondern auch andere Aspekte, wie etwa Systembetrieb, seine Umgebung, die Mensch-Maschine-Schnittstellen sowie Instandhaltungsbereitschaft, die alle Auswirkungen auf die Systemzuverlässigkeit haben. Um dieses Verständnis zu verstärken, sollte der Lieferant in einen Dialog mit dem Kunden eingebunden sein. Dieser Dialog mündet in eine tragfähige Aussage über die Kundenanforderung und alle ihre betrieblichen und umweltmäßigen Bedingungen. Diese Aussage vermittelt Vertrauen, dass das erste Ziel des Zuverlässigkeitsprogramms (siehe IEC 60300-1) erfüllt worden ist. Wenn der Kunde und der Lieferant die Anforderungen nicht schon in einem früheren Stadium vereinbart haben, müssen sie jetzt vereinbart werden.

Die Zuverlässigkeitsanforderungen müssen verstanden und analysiert werden, um die Zuverlässigkeitszielwerte des Lieferanten festlegen zu können. Der Zielwert des Lieferanten ist folglich ein Entwurfsziel, um eine Begrenzung für die Zuverlässigkeitsanforderung zu geben. Alle Anforderungen, die die Systemzuverlässigkeit betreffen, sollten analysiert werden, um ihre Auswirkungen auf die System- und die Subsystem-Ebene zu bestimmen, und die Ergebnisse dieser Untersuchungen sind Bestandteil des Zuverlässigkeitsnachweises. Beispielsweise können die Anforderungen des Kunden bezüglich der Umwelt für das System als Ganzes von Bedeutung sein, aber aufgrund ihres Einbauortes können manche Einheiten stark abweichenden Umgebungsbedingungen unterliegen.

Der Lieferant sollte seine Entwurfsphilosophie und hauptsächlichen Konstruktionsmerkmale erläutern und dann die Risikobereiche für die Zuverlässigkeit des vorgeschlagenen Entwurfs benennen. Die Schlüssel-Aspekte, die betrachtet werden sollten, sind Systemreife (z. B. ein neues Konzept im Vergleich mit Systemen, die bereits existieren), die voraussichtlichen Zuverlässigkeitsmerkmale, Zeitskalen und Kosten. Manchmal können die Risiken mit Hilfe einer Checkliste ermittelt werden, aber technisches Fachwissen sollte einen wesentlichen Beitrag liefern. Diese Zuverlässigkeitsrisiken sollten mit anderen Risiken des Vertrags im Risikomanagementplan des Gesamtprojekts zusammengefasst werden. Die Zuverlässigkeitsrisiken und die Strategie für deren Steuerung und Bewältigung sind ein Bestandteil des Zuverlässigkeitsnachweises.

Im Angebotsstadium sollte der Zuverlässigkeitsnachweisbericht auch einen teilweise ausgefüllten Nachweisrahmen enthalten, bestehend aus den vorgeschlagenen Maßnahmen für die Zuverlässigkeit, ihren „Erfolgskriterien“ und den Projektmeilensteinen, zu denen diese Nachweise erbracht werden sollten. Der Nachweisrahmen sollte mit Fortschritt des Vertrages aktualisiert werden, mit Bezugnahmen auf die Ergebnisse dieser Maßnahmen. Die „Erfolgskriterien“ sind diejenigen Kriterien, anhand derer die Zuverlässigkeitsnachweisberichte beurteilt werden müssen, da sie die notwendigen Nachweise liefern. Die Kriterien können quantitativ und/oder qualitativ sein, d. h. numerisch und/oder nicht-numerisch. Das Erfolgskriterium etwa für eine Verbesserung der Überlebenswahrscheinlichkeit könnte sein, die Überlebenswahrscheinlichkeit des Systems auf 0,95 zu steigern, wohingegen das Erfolgskriterium für eine Ausfallfolgemäßnahme sein könnte, alle kritischen Einzelausfälle zu erkennen und zu eliminieren.

6.4 Maßnahmen des Kunden zur Zuverlässigkeit während der Beschaffung

Während der Beschaffung sollte der Kunde die vom Lieferanten erstellten Zuverlässigkeitsnachweisberichte prüfen und die Verringerung der Zuverlässigkeitsrisiken überwachen, ebenso wie die zunehmende Erfüllung der Zuverlässigkeitsanforderungen.

6.5 Zuverlässigkeitsnachweis während der Nutzung durch den Kunden

Sobald das System den Betrieb aufnimmt, ist es wichtig, dass seine Zuverlässigkeit erhalten bleibt. Die jeweilige Leistung des Systems und Änderungen in der Art seiner Nutzung oder der Umgebung, in der es genutzt wird, sollten sorgfältig überwacht werden. Signifikante Änderungen sollten analysiert und Korrekturmaßnahmen ergriffen werden, um die Niveaus der in der Anforderung (in den Anforderungen) festgelegten und dann realisierten Zuverlässigkeit wiederherzustellen, soweit machbar und vertretbar.

Die Grundlage für den Zuverlässigkeitsnachweis hängt davon ab, wer für das System im Einsatz verantwortlich ist. Wenn der Original-Lieferant beauftragt ist, das System zu betreiben, kann er seinen Zuverlässigkeitsnachweis fortführen. Wenn der Kunde für den Betrieb des Systems verantwortlich ist, dann wird er

voraussichtlich den Zuverlässigkeitsnachweis auf seine Interpretation der Zuverlässigkeitsnachweisberichte abstellen, zusammen mit Nachweisen aus beliebigen Zuverlässigkeitsdarlegungen. Es kann auch sein, dass mehr als eine Organisation das System nutzen und jede den Zuverlässigkeitsnachweis getrennt entwickelt könnte.

6.6 Erweiterung

Es ist oft der Fall, dass das System während der Nutzungsphase Erweiterung erfordert, was vertraglich geregelte Tätigkeiten seitens eines Lieferanten nach sich ziehen kann. Falls dies geschieht, sollte der Lieferant einen Zuverlässigkeitsnachweis erstellen, der auf dem Zuverlässigkeitsnachweis des Kunden aufsetzt. Die Überwachungsmaßnahmen des Kunden und ihre Ergebnisse sollten in den Zuverlässigkeitsnachweis aufgenommen werden.

7 Einen Nachweis erbringen

Der Zuverlässigkeitsnachweis beruht auf verschiedenen Quellen und unterschiedlichen Nachweisniveaus, die sich von Plänen und Programmen, Normen, Ressourcen und Kompetenzen erstrecken bis hin zu detaillierten Ergebnissen aus numerischen Analysen und Prüfungen.

Diese Nachweisquellen können umfassen:

- a) Leistung bei früherem Einsatz;
- b) Analyse des geforderten Betriebszyklus;
- c) Entwurfsberechnungen;
- d) Vorhersagen und Modellbildung;
- e) Prüfung;
- f) Simulation;
- g) Expertenwissen einschließlich früher dokumentiertem Erfolg des Lieferanten;
- h) korrekte Umsetzung bewährter Methoden;
- i) Zuverlässigkeitsnachweise des Lieferanten.

Während der Entwicklungsphase werden Zuverlässigkeitsmaßnahmen ergriffen, um Nachweise zu generieren. Es ist wichtig, dass die Ergebnisse dieser Maßnahmen (die Nachweise) bezüglich ihrer „Erfolgskriterien“ fortlaufend bewertet und auch hinsichtlich des Erreichens der endgültigen Zuverlässigkeitszielwerte begutachtet werden. Falls die Ergebnisse darauf hinweisen, dass irgendwelche Merkmale der Systemzuverlässigkeit nicht auf dem erwarteten Niveau für dieses spezielle Stadium des Programms liegen oder dass ein Nachweis nicht seinen „Erfolgskriterien“ genügt, dann muss möglicherweise die Strategie geändert werden. Der Zuverlässigkeitsplan würde um die zusätzlichen oder modifizierten Maßnahmen ergänzt werden.

Mit Fortschritt des Lebenszyklus werden Nachweise generiert und gesammelt. Anfangs können sie nur Hinweise darauf geben, dass die Anforderungen voraussichtlich erfüllt werden. Mit dem Projektfortschritt werden die Nachweise jedoch aussagekräftiger, um das Erfüllen der Zuverlässigkeitsanforderungen zu untermauern. Bei Vertragsende besteht die Erwartung, dass der Nachweisrahmen belegt, dass die Zuverlässigkeitsanforderungen erfüllt worden sind. Es ist schwierig, das gesamte Ausmaß des Nachweises in seinen vielen Formen, die vorgelegt werden können, zu beschreiben; jedoch werden typische Beispiele dafür, was der Nachweis für die Zuverlässigkeit umfassen kann, in Anhang F gezeigt.

Bild 1 zeigt, dass die begründeten Argumente im Zuverlässigkeitsnachweis unterschiedliche Arten von Nachweisen kombinieren und auch auf Annahmen aufsetzen können. Es ist wichtig, dass diese Annahmen offen dargelegt werden. Während des Zuverlässigkeitsprogramms sollten die Schlüsselannahmen soweit möglich gewissermaßen validiert und jede durch begründeten Nachweis ersetzt werden. Die begründeten Argumente erlauben, dass Behauptungen hinsichtlich der Zuverlässigkeitserwartungen aufgestellt werden; zusammen mit den sie unterstützenden Nachweisen bilden sie den Zuverlässigkeitsnachweis.

8 Einen Nachweis darstellen

Dieser Abschnitt bietet Anleitung dafür, wie ein Nachweis im Zuverlässigkeitsnachweis dargestellt werden kann. Die zum Erreichen der Zuverlässigkeit notwendigen Maßnahmen hängen von der Art des Systems und seinem Entwicklungsstand ab und werden wahrscheinlich von Projekt zu Projekt stark schwanken.

Bevor eine Zuverlässigkeitsmaßnahme ergriffen wird, müssen das Ziel dieser Tätigkeit voll verstanden und Erfolgskriterien definiert sein. Die Erfolgskriterien sollten jene sein, anhand derer die Maßnahme beurteilt werden kann, und sie werden eine Behauptung im Zuverlässigkeitsnachweisbericht untermauern. Es sollte beachtet werden, dass sich nicht alle Maßnahmen auf ein quantifiziertes Erfolgskriterium beziehen, sondern auch, je nach den Zielen der Maßnahme, qualitative Kriterien erfordern können. Beispielsweise sind die Erfolgskriterien für die Modellbildung nicht einfach, dass die Vorhersagen und Modellierungen die Übereinstimmung des vorgeschlagenen Entwurfs mit den Anforderungen zeigen. Wichtiger sind Überlegungen, wie etwa: Deckt die Modellierung den maßgeblichen Betrieb des Systems ab? Oder etwa: Sind alle Systembestandteile (beispielsweise Software) im Modell berücksichtigt?

Viele der existierenden Zuverlässigkeitsverfahren liefern nicht aus sich selbst heraus Gewissheit über die Zuverlässigkeit: diese ergibt sich nur, wenn sie in Kombination mit anderen zugehörigen Verfahren verwendet werden. Beispielsweise kann ein Analyseverfahren wie die Fehlzustandsbaumanalyse eine Entwurfschwäche aufdecken, aber Verbesserung und Gewissheit ergeben sich nur, wenn die Schwäche in Entwicklungsbewertungen behandelt wird.

Gewissheit über die Zuverlässigkeit ergibt sich nicht nur durch die Generierung von Ergebnissen aus Maßnahmen, sondern auch aus der Umsetzung von weiteren Maßnahmen, die aufgrund eines durch die Maßnahme erkannten Risikos ergriffen werden. Die Maßnahme zum richtigen Zeitpunkt durchzuführen, so dass sie den Entwurf beeinflusst, ist sehr wichtig. Daher besteht der aus der Untersuchung stammende Nachweis in der Dokumentation, die belegt, dass Maßnahmen rechtzeitig ergriffen worden sind.

Maßnahmen sollten parallel zum Entwurfsprozess durchgeführt werden, damit sich die Untersuchung auf den Entwurf auswirken und den endgültigen Entwurf wiedergeben kann. Wenn mehr als eine Entwurfsoption betrachtet wird, dann sollte jedes Ergebnis getrennt betrachtet werden, damit die Auswirkungen auf die Funktionsfähigkeit und die Ausfallfolgen begutachtet werden können, bevor die bevorzugte Entwurfsoption ausgewählt wird.

Von den Informationen, die sich aus einer Maßnahme für den Zuverlässigkeitsnachweis ergeben, kann angenommen werden, dass sie die folgenden Bestandteile enthalten (siehe Bild 3):

- a) Zielsetzung und Erfolgskriterium (was mit der Maßnahme erreicht werden soll, und Festlegen, wann die Maßnahme als erfolgreich angesehen werden kann);
- b) Ergebnisse (die Ergebnisse aus dieser Maßnahme);
- c) Annahmen;
- d) Nachweis (wie die Ergebnisse Behauptungen im Zuverlässigkeitsnachweisbericht untermauern);
- e) Entwicklung und Aufrechterhaltung des Nachweisrahmens (Wie werden die Ergebnisse der Maßnahme verwaltet, damit sie den letzten Entwurfsstand widerspiegeln?).

9 Begutachten der Angemessenheit eines Nachweises

Die Angemessenheit eines Nachweises ist in erster Linie eine Funktion seiner praktischen Auswirkung auf die Verringerung von Zuverlässigkeitsrisiken, d. h. auf die Erhöhung der Gewissheit. Obwohl es nicht notwendig ist, die Angemessenheit spezifischer detaillierter Zuverlässigkeitsaufgaben an sich zu begutachten, sind die Sichtbarkeit, die Nachvollziehbarkeit und die Qualität des produzierten Nachweises entscheidende Faktoren. Es ist daher notwendig zu bestätigen, dass der Nachweis in einem geschlossenen Regelkreis von Zuverlässigkeitsverfahren und -prüfungen generiert, gehandhabt, validiert und verwendet wird und dass er die wesentlichen Ziele von IEC 60300-1 erfüllt. Bild 6 veranschaulicht einen typischen geschlossenen Regelkreis (Steuerungs- und Bewältigungsprozess für Zuverlässigkeitsrisiken), auf dessen Grundlage in diesem Abschnitt Kriterien für die Begutachtung der Angemessenheit des Nachweises abgeleitet werden. Diese Tätigkeiten sollten jedoch bereits Bestandteil des Zuverlässigkeitsmanagements sein und sollten keinen zusätzlichen Aufwand erfordern.

Bild 6 enthält – von links nach rechts – vier Hauptbereiche:

- a) Erstens, der Bereich auf der linken Seite wiederholt die wesentlichen Ziele des Zuverlässigkeitsmanagements. Diese stellen die wichtigsten Kriterien für die Angemessenheit eines Nachweises dar und müssen durch den gesamten Risikosteuerungs- und -bewältigungsprozess als wichtigste Ziele berücksichtigt werden.
- b) Zweitens, die zur Sicherung der Zuverlässigkeit unabdingbaren Zuverlässigkeitsverfahren sind wichtige, „zielorientierte“ Prozesse für spezielle Analysen, Prüfungen und Ergebnisse, die von den entsprechenden üblichen Zuverlässigkeitsaktivitäten (oder maßgeschneiderten Zuverlässigkeitsaktivitäten) abhängen. Die Zuverlässigkeitsverfahren tauschen Nachweise untereinander aus und geben den Nachweis an die Zuverlässigkeitssteuerung aus.
- c) Drittens, die Zuverlässigkeitslenkung sind Prozesse, die darauf beruhen, „den Nachweis zu bewerten“ und zur Zuverlässigkeitsstrategie führen, zum „Zuverlässigkeitsplan“ und zum „Managen der Zuverlässigkeit“. In jedem Stadium sollte ungenügender Nachweis eine Bewertung der Zuverlässigkeitsstrategie innerhalb des „Zuverlässigkeitsplans“ in Gang setzen. „Managen der Zuverlässigkeit“ bietet einen Pfad zur Steuerung von Rückinformationen für alle Zuverlässigkeitsverfahren (sowie aus ihnen ausgewählte Zuverlässigkeitsmaßnahmen), um den geforderten Nachweis zu erbringen. Somit sind die Zuverlässigkeitsprozesse zu jeder Zeit darauf ausgerichtet, zunehmende Gewissheit zu liefern, dass die Risiken gesteuert und bewältigt werden.
- d) Viertens, nennt die rechte Seite von Bild 6 die wesentlichen Ergebnisse des Risikosteuerungs- und -bewältigungsprozesses; das sind: „Zuverlässigkeits-Risikoregister“ (das Teil des Projekt-Risikoregisters ist), „Zuverlässigkeitsnachweis und Berichte“ und die „Begutachtung der Angemessenheit“ des Nachweises. Es sollte beachtet werden, dass das letztere nicht die Angemessenheit des Zuverlässigkeitsnachweises und der Berichte an sich behandelt.

Der Prozess zur Steuerung und Bewältigung von Zuverlässigkeitsrisiken ist in jeder Projektphase und auf jede vertragliche Vereinbarung anwendbar. In Bild 6^{N5)} ist jedem Prozessblock lediglich für Verweiszwecke eine Kennung zugeordnet worden. Die Kennungen geben keine chronologische Reihenfolge, da die Prozesse interaktiv sind und oft nebeneinander ablaufen. In Abhängigkeit vom Stadium im Beschaffungszyklus für ein neues, ein in Entwicklung begriffenes oder ein handelsübliches System (OTS) variieren sowohl die Bedeutung verschiedener Verfahren als auch die Reihenfolge, in der sie durchgeführt werden. Es sollte jedoch immer ein Risikoregister und einen Zuverlässigkeitsplan als Kernelemente des Prozesses geben. Wo immer möglich, sollten die beiden allgemeinen Verfahren „Sammeln vorliegender Nachweise“ und „DRACAS / Rückinformationen aus dem Betrieb“ (DRACAS: Data Recording and Corrective Action System; dt. System für Datenerfassung und Korrekturmaßnahmen) permanent betrieben werden und mehrere Generationen und Versionen ähnlicher Systeme umfassen. Alle relevanten vorhandenen Informationen über die erreichte Zuverlässigkeit und die mit einem bestimmten Entwurf gemachten Erfahrungen sollten verwendet werden, um in ähnlichen Systemen Gewissheit über die Zuverlässigkeit zu erlangen.

Für einen bestimmten Systemlebenszyklus wird der Einstieg in den Prozess durch die Erstellung eines Zuverlässigkeitsnachweises unter Verwendung zumindest der Verfahren (a) bis (e) aus Bild 6 erreicht, einschließlich des Verfahrens der Zuverlässigkeitsmodellbildung/-simulation. Der vorhandene Nachweis (einschließlich Zuverlässigkeitsrisiken) wird bewertet, eine Zuverlässigkeitsstrategie wird festgelegt, und Zuverlässigkeitsplanung und -management werden eingeführt, um Zuverlässigkeitsmaßnahmen zu lenken und zu überwachen. Sobald der Prozess für ein bestimmtes Projekt angelegt worden ist, sollten Zuverlässigkeitsverfahren und -überwachung – durch die Zuverlässigkeitsrisiken gemindert werden und während des Beschaffungszyklus zum frühestmöglichen Zeitpunkt ein Hinweis geliefert wird, dass die Zuverlässigkeitsanforderungen erfüllt worden sind – in der zweckdienlichsten Art und Weise eingeführt und aufrechterhalten werden, um Nachweise zu generieren und zu verwalten.

Die wesentlichen Kriterien zur Begutachtung der Angemessenheit von Nachweisen sind daher die folgenden:

- 1) Der Nachweis als Ganzes ist eindeutig aus einem Prozess in Form eines geschlossenen Regelkreises zur Steuerung und Regelung von Zuverlässigkeitsrisiken abgeleitet, wie etwa in Bild 6; siehe Anhang E für Anleitung zu den Grundsätzen spezieller Prozessblöcke.

^{N5)} Nationale Fußnote: Im en. Original wird irrtümlicherweise auf Bild 7 verwiesen. Dies wurde in der dt. Übersetzung richtiggestellt.

- 2) Die Herkunft jedes einzelnen Nachweises ist eindeutig mit einem (oder mehreren) bestimmten Zuverlässigkeitsverfahren und/oder Überwachungsprozess(en) verknüpft.
- 3) Die Verknüpfungen zwischen jedem einzelnen Nachweis und dem Zuverlässigkeits-Risikoregister und dem Zuverlässigkeitsplan werden gezeigt.
- 4) Der Nachweis aus jeder einzelnen Zuverlässigkeitsmaßnahme wird entsprechend Anhang B vorgestellt.
- 5) Der Status jedes einzelnen Nachweises, hinsichtlich seiner Relevanz, Vollständigkeit, Genauigkeit und wie er genutzt worden ist, um das System zu beeinflussen und Risiken zu verringern, kann ohne Weiteres dem Nachweisrahmen entnommen werden.

Um die Angemessenheit des Nachweises begutachten zu können, sollte nach nachvollziehbaren Verfahren/Techniken, Annahmen und detaillierten Ergebnissen Ausschau gehalten werden. Folglich ist ein offener und ehrlicher Dialog zwischen Partnern von großer Bedeutung. Urteilsvermögen wird benötigt, um den vorgestellten Nachweis in Übereinstimmung mit den unter Punkt 1) bis 5) aufgeführten Kriterien zu begutachten, einschließlich seiner Wahrnehmbarkeit, Nachvollziehbarkeit und Qualität. Anhang D enthält eine Checkliste allgemeiner Punkte, die zwar nicht bindend sind, aber in geeigneten Situationen zusätzliche Anleitung für die Begutachtung der Angemessenheit des Nachweises bieten sollten.

Anhang E erläutert die Grundsätze der Prozessblöcke in Bild 6 und gibt Anleitung zum Kontext für die Begutachtung der Angemessenheit des Nachweises bezüglich der unter Punkt 1) bis 5) aufgeführten Kriterien. Normalerweise müssen alle Prozesse zur Zuverlässigkeitslenkung und die betreffenden Prozesse der Zuverlässigkeitsverfahren für ein bestimmtes System bzw. eine bestimmte Lebenszyklusphase in Erwägung gezogen werden; dabei wird die Auswahl irgendeines bestimmten Prozesses durch die Notwendigkeit gesteuert, einen Nachweis hinsichtlich der Zuverlässigkeitsrisiken zu liefern. Aufgrund des weiten Anwendungsbereichs der Anleitung empfiehlt Anhang E keine speziellen Zuverlässigkeitsmaßnahmen, sondern er verwendet gegebenenfalls Beispiele, wenn es darum geht, einen Punkt zu veranschaulichen.

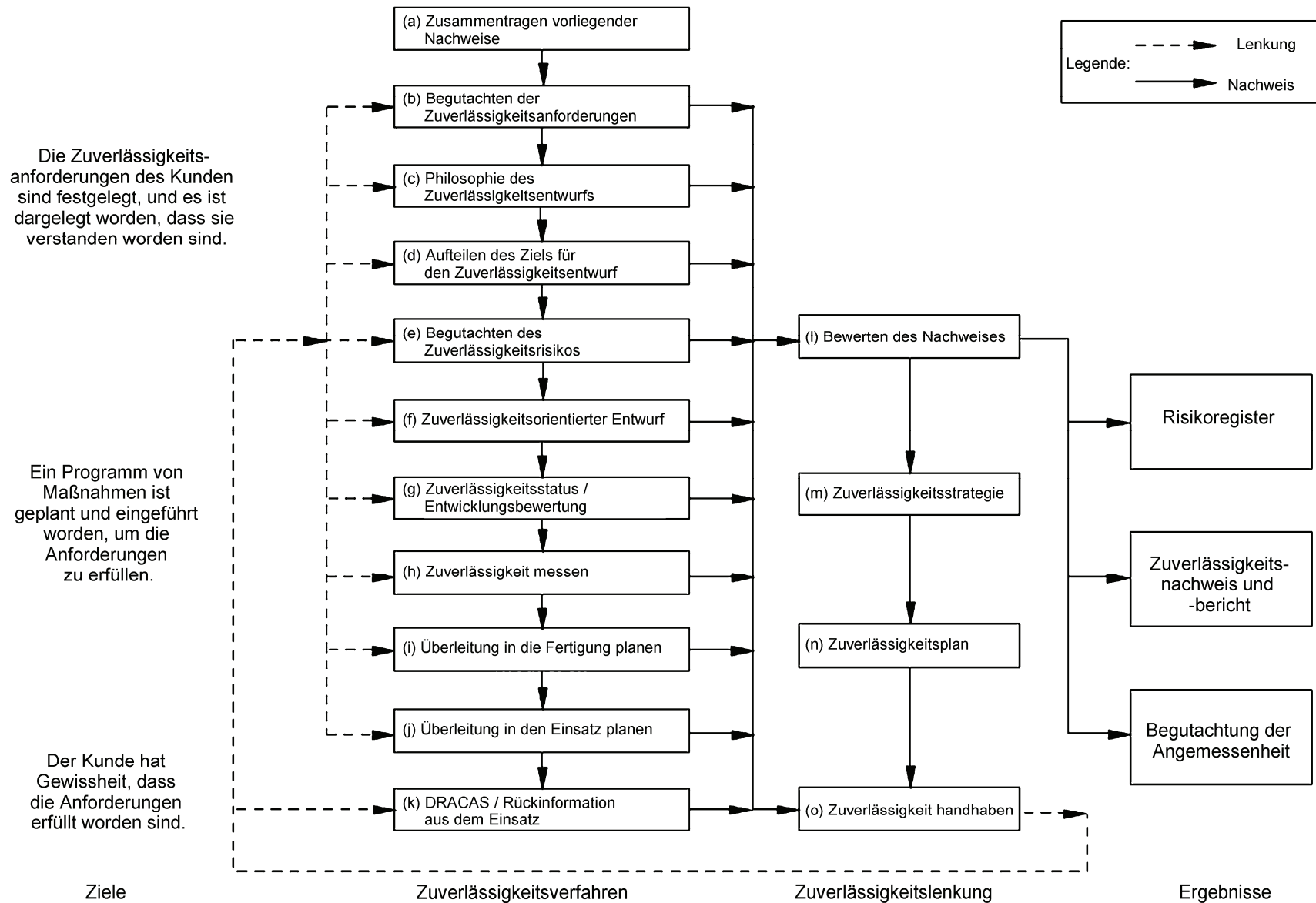


Bild 6 – Prozess zur Steuerung und Bewältigung von Zuverlässigkeitsrisiken

Anhang A (informativ)

A.1 Dokumente zum Thema „Strukturierung von Argumenten“

Toulmin method – Toulmin, S.: The Uses of Argument (1958; 2nd ed., 2003)

Goal Structuring Notation – GSN Community Standard

http://www.goalstructuringnotation.info/documents/GSN_Standard.pdf

A.2 Dokumente zum Thema „Formale Vereinbarungen treffen“

ISO/IEC 15026, *System and Software Assurance*

ISO/IEC 15288, *Systems Engineering – System lifecycle processes*

ISO/IEC 12207, *Systems and software engineering – Software lifecycle processes*

A.3 Dokumente zum Thema „Spezifizieren der Zuverlässigkeit“

IEC 62347, *Guidance on system dependability specifications*

IEC 60300-3-4, *Dependability management – Application guide – Guide to the specification of dependability requirements*

Anhang B (informativ)

Allgemeine Anforderungen an den Zuverlässigkeitsnachweisbericht

B.1 Zuverlässigkeitsnachweisbericht

Die folgenden Unterabschnitte liefern Überschriften und beschreiben den Inhalt für Rubriken innerhalb des Zuverlässigkeitsnachweisberichtes. Es wird nicht erwartet, dass sich diese Struktur für jedes Projekt eignet, aber es ist beabsichtigt, Anleitung zu geben, welche Informationen in den Berichten enthalten sein sollten.

Der Zuverlässigkeitsnachweisbericht stellt den Zuverlässigkeitsnachweis entsprechend dem Zuverlässigkeitsnachweisrahmen für ein bestimmtes Stadium bereit. Die Berichte liefern auf der Basis von Nachweis und Annahmen eine begründete Behauptung, dass das System die Zuverlässigkeitsanforderungen erfüllen wird. Von dem Bericht wird nicht erwartet, dass er alle für dieses Stadium produzierten Nachweise enthält, sondern dass er zusammenfasst und als ein „Wegweiser“ wirkt, der zeigt, wo der detaillierte Nachweis gefunden werden kann.

Diese Norm betrifft Zuverlässigkeit insgesamt, was so verstanden werden könnte, dass durch Dokumente belegter Nachweis für Zuverlässigkeit in einem einzigen Bericht zusammengefasst wird. Dies bedeutet aber nicht, dass die Zuverlässigkeitsnachweisberichte in demselben Bericht dokumentiert werden sollten. Falls der Nachweisrahmen getrennte Berichte erfordert, oder der Kunde oder Lieferant denkt, dass getrennte Berichte ein klareres Bild bieten oder eine gezieltere Herangehensweise ermöglichen, dann werden getrennte Nachweisberichte zur Funktionsfähigkeit und zur Instandhaltbarkeit als durchaus akzeptabel angesehen.

Wo es zweckmäßig erscheint, sollten die zu einem gegebenen Projekt gehörenden Zuverlässigkeitsnachweisberichte zur Verbesserung der Lesbarkeit und des Informationstransfers versuchen, ein gemeinsames Format zu verwenden.

B.1.1 Einleitung

Jeder Zuverlässigkeitsnachweisbericht sollte die übergeordneten Anforderungen im Nachweisrahmen, gegen die der Nachweis beurteilt werden muss, auflisten und auf diese verweisen und sollte bis zur ursprünglichen Forderung des Kunden zurückverfolgbar sein.

B.1.2 Systembeschreibung

Die Systembeschreibung sollte die folgenden Punkte enthalten:

- a) Physikalische Beschreibung – dieser Punkt sollte die physikalischen oder funktionalen Merkmale des Systems kurz beschreiben;
- b) Systemgrenzen – dieser Punkt sollte die physikalische oder funktionale Begrenzung des Systems beschreiben. Blockdiagramme können eine gute Veranschaulichungsmöglichkeit für die Begrenzung des im Nachweis betrachteten Systems sein;
- c) Betrieb – dieser Punkt sollte die Hauptaufgabe oder Funktion des Systems beschreiben sowie alle Nebenrollen. Die Beschreibung sollte auch die typische erwartete Einschaltdauer enthalten;
- d) Umgebung – dieser Punkt sollte das Einsatzumfeld des Systems beschreiben;
- e) Schnittstellen mit anderen Geräten/Systemen – dieser Punkt sollte die Geräte festlegen, die mit den Eingaben, Ausgaben und Diensten für das betrachtete System verbunden sind. Gegebenenfalls sollten auch Geräte beschrieben werden, die sich körperlich in der Nähe des Systems befinden;
- f) Ausgabestand/Software-Version – dieser Punkt sollte sich auf einen speziellen Ausgabestand des Systems beziehen, gegebenenfalls einschließlich der Software-Version(en);
- g) Konfigurationsüberwachung – dieser Punkt sollte sicherstellen, dass der Bericht den letzten Ausgabestand/die letzte Software-Version wiedergibt. Die Darstellung sollte angeben, wo der geltende Ausgabe-

stand/die geltende Software-Version festgelegt ist, beispielsweise im Stammdatensatz (en: master record index);

- h) Qualifikationsniveaus und Ausbildung der Mitarbeiter – das Qualifikationsniveau und die notwendige Ausbildung, um das System zu betreiben und instandzuhalten, sollten beschrieben werden;
- i) Instandhaltungsgrundsätze – dieser Punkt sollte die Betreuungsregelwerke für jede der Funktionen des Systems oder jedes der erwarteten Einschaltdauerprofile beschreiben.

B.1.3 Zuverlässigkeitsanforderungen

Dies sollte die Anforderungen des Kunden wiedergeben und wie der Lieferant diese interpretiert. Die Anforderungen sollten in ihrem weitesten Kontext verstanden werden, derart, dass sie die Umgebungs- und die Einsatzanforderungen enthalten, ebenso wie die explizit festgelegten Zuverlässigkeitsanforderungen. Der Lieferant sollte beschreiben, wie die Anforderungen für seine vorgeschlagene Entwurfslösung interpretiert und in auf das Vertragsziel bezogene Zuverlässigkeitsmaßnahmen umgesetzt worden sind.

B.1.4 Zuverlässigkeitsrisiken

Durch Analyse der Zuverlässigkeitsanforderungen sollte der Lieferant die mit dem System, das die Zuverlässigkeitsanforderungen erfüllt, verbundenen Zuverlässigkeitsrisiken bestimmen, und wie diese Risiken während des Vertrags gehandhabt werden oder gehandhabt worden sind.

B.1.5 Zuverlässigkeitsstrategie

Auf der Basis der erkannten Risiken, der Reife der vorgeschlagenen Entwurfslösung und der Zuverlässigkeitsanforderungen sollte der Lieferant eine Strategie zur Erfüllung der Anforderungen und zum Vermitteln der notwendigen Gewissheit festlegen. Diese Strategie begründet die Maßnahmen im Zuverlässigkeitsprogramm des Lieferanten und legt die Erfolgskriterien für diese Maßnahmen fest. Die Strategie muss im Zuverlässigkeitsplan erläutert werden.

B.1.6 Der Nachweisrahmen

Dieser Abschnitt sollte einen vollständigen Überblick oder Plan der Nachweise geben, die während der Entwicklungsphasen erbracht werden müssen. Er sollte auch zeigen, wann und von wem Zuverlässigkeitsnachweisberichte zu erstellen sind. Spezielle Einträge in den Nachweisrahmen können vom Kunden ausgewählt werden und können für Überwachungszwecke mit Zahlungen verknüpft werden, die an den Projektfortschritt gebunden sind.

B.1.7 Gesamtheit der Nachweise

Dieser Abschnitt sollte die vorhandenen Nachweise in ein Verzeichnis aufnehmen. Jeder einzelne Nachweis sollte auf den Nachweisrahmen und auf jedes der Risiken, das er mindert, bezogen sein. Die folgende Auflistung enthält Beispiele der Art von Nachweisen, die aufgenommen werden sollten:

- Informationen von relevanten Zuverlässigkeitsnachweisen ähnlicher Systeme oder aus Einsatz- und Instandhaltungserfahrungen;
- Nachweise und Nachweisberichte der Lieferanten;
- Analyse von Zuverlässigkeitsanforderungen und Betriebsbedingungen;
- Entwurfsphilosophie;
- Zielsetzungen;
- Risiken;
- Strategie, einschließlich Annahmen, Begründungen, Behauptungen;
- Plan der Zuverlässigkeitsmaßnahmen;
- Ergebnisse von Zuverlässigkeitsmaßnahmen; diese sollten die relevanten Entwurfsberechnungen für Zuverlässigkeit enthalten, den Einsatz bewährter Methoden, Vorhersagen und Modellbildung, Analysen,

Simulation, Erprobung, DRACAS / Rückinformation aus Einsatz und Instandhaltung sowie Expertenwissen;

- Prüfergebnisse und –maßnahmen;
- Fortlaufende Neubewertung von Risiken.

Die Gesamtheit der Nachweise sollte auch die Historie von Bewertungen und Aktualisierungen der Zuverlässigkeitsentwurfsphilosophie, von Zielen sowie von Strategie und Plan nachzeichnen, welche den sich ändernden Status der ursprünglichen Risiken berücksichtigen, ebenso wie alle neuen/neu auftretenden Risiken. Die Gesamtheit der Nachweise sollte unterscheiden zwischen dem harten Nachweis bzw. Fakten und den aus diesen Fakten abgeleiteten Argumenten oder daraus gezogenen Schlussfolgerungen.

B.1.8 Behauptungen zur Zuverlässigkeit

Typischerweise werden die Behauptungen derart sein, dass das System allen Zuverlässigkeitsanforderungen genügt. Dieser Abschnitt sollte eine logische Argumentation auf der Basis von Nachweisen und allen Annahmen liefern, warum jede der Anforderungen im Einsatz erfüllt werden wird. Alle Annahmen sollten ausführlich aufgelistet werden.

B.1.9 Grenzen für den Einsatz

Dieser Abschnitt sollte die Grenzen für den Systemeinsatz festlegen, was, falls sie überschritten werden, bedeutet, dass die Zuverlässigkeitsbehauptung nicht länger gelten muss. Diese Grenzen umfassen den Arbeitsbereich des Systems, das Umfeld und wesentliche Instandhaltungsmaßnahmen.

B.1.10 Bewertung des bisherigen Nachweise

Dieser Abschnitt sollte eine ausgewogene Bewertung der Gesamtheit der Nachweise liefern hinsichtlich ihrer Vollständigkeit, Aktualität und Annehmbarkeit in Bezug auf die im Nachweisrahmen enthaltenen Kriterien.

B.1.11 Schlussfolgerungen und Empfehlungen

Dieser Abschnitt sollte eine Übersicht der Schlussfolgerungen enthalten, die aus den bislang gesammelten Zuverlässigkeitsnachweisen gezogen worden sind, einschließlich einer Aussage, ob das System voraussichtlich die Zuverlässigkeitsanforderungen erfüllen wird. In vorläufiger Form sollte er vorschlagen, ob das Projekt zum nächsten Meilenstein fortschreiten sollte, oder welche weiteren Arbeiten für den Projektfortschritt erforderlich sind. Weiterhin sollte er empfehlen, welche Maßnahmen in Zukunft zu ergreifen sind, um die notwendige Gewissheit zu erzeugen, dass die Zuverlässigkeitsanforderungen erfüllt werden.

Der Stand der Zuverlässigkeitsannahmen, -nachweise, -argumente, -behauptungen und -restrisiken sollte zusammengefasst und diskutiert werden. Es sollten Schlussfolgerungen gezogen werden hinsichtlich des Standes der zunehmenden Gewissheit und der zur Minderung der Restrisiken notwendigen Maßnahmen.

Die Empfehlungen sollten auf den aktuellen Defiziten bei den vorhandenen Nachweisen aufsetzen und gegebenenfalls Änderungen an der Philosophie des Zuverlässigkeitsentwurfs, den Zielsetzungen, der Strategie sowie dem Plan vorschlagen, um den Fortschritt in Richtung Gewissheit, dass das System jede der Zuverlässigkeitsanforderungen erfüllen wird, zu maximieren.

Anhang C (informativ)

Beispiele von Zuverlässigkeitsrisiken in verschiedenen Stadien des Lebenszyklus eines Systems

Konzept des Systems	Fehler ^{N6)} des Kunden, die Anforderungen angemessen festzulegen.
	Fehler des Kunden, die Anforderungen korrekt festzulegen.
	Fehler des Kunden, ausreichend Ressourcen zur Erfüllung der Anforderungen bereitzustellen.
Aufzeigen von Lösungswegen	Fehler des Kunden, die Anforderungen dem Lieferanten mitzuteilen.
	Fehler des Lieferanten, die Anforderungen zu verstehen.
	Fehler des Lieferanten, alle Zuverlässigkeitsrisiken zu erkennen.
	Fehler des Lieferanten, einen geeigneten Plan zur Minderung der Zuverlässigkeitsrisiken aufzustellen.
	Fehler des Lieferanten, den Fortschritt zu überwachen.
Auswahl einer Lösung	Fehler des Kunden, die am besten geeignete Lösung auszuwählen.
	Fehler des Kunden, die Anforderungen gegebenenfalls zu modifizieren.
	Fehler des Kunden, die modifizierten Anforderungen dem Lieferanten mitzuteilen.
	Fehler des Lieferanten, die modifizierten Anforderungen zu verstehen.
	Fehler des Lieferanten, alle Zuverlässigkeitsrisiken zu erkennen.
	Fehler des Lieferanten, einen geeigneten Plan zur Minderung der Zuverlässigkeitsrisiken aufzustellen.
	Fehler des Kunden, den Fortschritt zu überwachen.
Darlegen der Lösung	Fehler des Lieferanten, nach seinem Plan zur Minderung der Zuverlässigkeitsrisiken zu arbeiten.
	Fehler des Lieferanten, den Fortschritt zu überwachen und zu bewerten und seinen Plan gegebenenfalls zu ergänzen.
	Fehler des Lieferanten, alle vorhandenen Daten zu erfassen und sie für den Nachweis geeignet aufzubereiten.
	Fehler des Lieferanten, ausreichend Nachweis zu erbringen, um die Zuverlässigkeit zur Zufriedenheit des Kunden darlegen zu können.
	Fehler des Kunden, den Fortschritt zu überwachen.

^{N6)} Nationale Fußnote: Im en. Original wird die Benennung „failure“ verwendet, aber offensichtlich nicht im Sinne von IEC 60050-191:2002, 191-04-01.

Realisierung der Lösung	Fehler des Lieferanten, die mit dem Übergang von der Entwicklung in die Fertigung verbundenen Zuverlässigkeitsrisiken zu erkennen und zu handhaben.
	Fehler des Lieferanten, den Fortschritt zu überwachen und zu bewerten und seinen Plan gegebenenfalls zu ergänzen.
	Fehler des Lieferanten, die Zuverlässigkeit seines Systems zur Zufriedenheit des Kunden darlegen zu können.
	Fehler des Kunden, den Fortschritt zu überwachen.
Betreuung der Lösung	Fehlen technischer Kapazität, das Produkt (oder Teile davon) zu realisieren.
	Fehler des Kunden, sicherzustellen, dass die Lösung wie festgelegt eingesetzt, instandgehalten und betreut wird.
	Fehler des Kunden, Änderungen beim Einsatz, im Umfeld und bei der Betreuung zu überwachen.
	Fehler des Kunden, Zuverlässigkeitsrisiken zu erkennen, die sich aus einer Änderung beim Einsatz, im Umfeld oder bei der Betreuung ergeben.
	Fehler des Kunden, die Zuverlässigkeitsrisiken zu mindern, die sich aus einer Änderung beim Einsatz, im Umfeld oder bei der Betreuung ergeben.
ANMERKUNG 1 Der Kunde kann einen Teil oder auch die gesamte Verantwortung für das Handhaben dieser Betreuungsrisiken einem Lieferanten übertragen.	
ANMERKUNG 2 Risiken, die mit Obsoleszenz verbunden sind, sind in „Betreuung“ eingeschlossen worden.	
Entsorgung der Lösung	Fehler des Kunden, die in dem Projekt „gesammelten Erfahrungen“ (einschließlich der Nachweise) (en: lessons learnt) zu erfassen, aufzuzeichnen und zu verbreiten.

ANMERKUNG 3 Spezielle Beispiele technischer Risiken sind nicht eingeschlossen worden, sollten aber von Fall zu Fall berücksichtigt werden.

Anhang D (informativ)

Checkliste von Punkten zur Begutachtung der Angemessenheit des Nachweises

Dieser Anhang stellt eine Checkliste bereit, die als eine Aufforderung verstanden werden sollte, Maßnahmen bei denjenigen Punkten zu veranlassen, die von Bedeutung sind, und keine „Ja“- oder „Nein“-Antwort nach sich ziehen. Urteilsvermögen ist erforderlich, um den vorgelegten Nachweis einschätzen zu können. Die Checkliste sollte nicht als zwingend oder erschöpfend verstanden werden: sie ist allgemein gehalten und gibt Anleitung zur Ergänzung der allgemeinen Anleitung, die in Abschnitt 9 dieser Norm gegeben wurde.

Checkliste:

- a) Sind die Zielsetzungen für die Maßnahme eindeutig festgelegt?
- b) Ist die Maßnahme systematisch und vollständig durchgeführt worden?
- c) Ist die Maßnahme zu einem Zeitpunkt durchgeführt worden, der Einfluss auf den Entwurf erlaubt hat?
- d) Sind der für die Maßnahme vorgesehene Einsatz und das vorgesehene Umfeld dokumentiert worden?
- e) Sind die physikalischen und funktionalen Grenzen der Maßnahme festgelegt worden?
- f) Sind alle Annahmen festgehalten worden (beispielsweise Eingangsdaten von anderen Systemen oder Diensten) und sind sie realistisch und vernünftig?
- g) Ist eine Begründung gegeben worden für das bei der Maßnahme verwendete Verfahren bzw. die verwendete Technik und ist die Begründung plausibel?
- h) Wer wurde während der Maßnahme zu Rate gezogen (beispielsweise Anwender, Mitarbeiter der Instandhaltung, Entwickler)? War dieses Niveau der Beratung angemessen?
- i) Sind die Empfehlungen aus der Maßnahme eindeutig und sind sie nachvollziehbar?
- j) Deutet der dokumentarische Nachweis darauf hin, dass die Empfehlungen umgesetzt worden sind?
- k) Sind die Ergebnisse aus der Maßnahme fortlaufend aktualisiert worden, um den letzten Stand des Entwurfs wiederzugeben und werden sie als Eingangsinformation für Entwicklungsbewertungen genutzt?

Anhang E (informativ)

Prozess zur Steuerung und Bewältigung von Zuverlässigkeitsrisiken

Dieser Anhang präsentiert die Grundlagen der Prozessblöcke in Bild 6. Er bietet Anleitung hinsichtlich des Kontextes zur Begutachtung der Angemessenheit des Nachweises gegenüber den Kriterien in Abschnitt 9. Die Prozesskennungen und -titel aus Bild 6 sind aufgelistet, gefolgt von einer Angabe der Grundsätze dazu, was der Nachweis enthalten sollte und wie er mit anderen Prozessen zusammenhängen würde. Gegebenenfalls sind anschauliche Beispiele enthalten. In der Regel sollten alle Zuverlässigkeitsüberwachungsprozesse und die relevanten Vorgehensweisen zur Zuverlässigkeit während jeder Lebenszyklusphase betrachtet werden.

- a) Zusammentragen vorliegender Nachweise – Informationen von relevanten Zuverlässigkeitsnachweisen ähnlicher Systeme oder aus betrieblicher Zuverlässigkeitserfahrung, einschließlich sowohl der Erfolge als auch Misserfolge; Argumentationen und Rechtfertigung für ihre Verwendung zur Minderung von Risiken und Erzeugung von Gewissheit; Bestätigung einer ständigen Verpflichtung zur Verbesserung der Zuverlässigkeit.
- b) Begutachten der Zuverlässigkeitsanforderungen – Interpretation der Szenarien für Betrieb und Instandhaltung, der Umweltprofile und das Verstehen folgender Punkte
 - Zuverlässigkeitsnachweis des Kunden;
 - zulässige/eingeschränkte Betriebsarten;
 - erhoffter betrieblicher Erfolg während der Einschaltdauer sowie Ausfallkriterien;
 - qualitative und quantitative Zuverlässigkeitsanforderungen;
 - notwendiger Lagerungs- und Transportbedarf;
 - zulässige Lasten.
- c) Philosophie des Zuverlässigkeitsentwurfs – ein Prozess ständiger Verbesserung und Verpflichtung, die Gewissheit eines robusten Entwurfs zu bieten, bekannte Ausfallmechanismen zu eliminieren oder die Zeit bis zum Ausfall auf ein annehmbares Niveau zu steigern; Fehlervermeidungstechniken für die Softwareentwicklung; spezielle Entwurfskriterien für Zuverlässigkeit (beispielsweise Redundanz/Fehlererkennung und -behebung), die notwendig sind, um die begutachteten Anforderungen [b)] unter Verwendung von an früheren Systemen gesammelter Erfahrungen [a)] zu erfüllen; zur Umsetzung der Philosophie notwendige Zuverlässigkeitsressourcen.
- d) Aufteilen der Zuverlässigkeitsziele – basierend auf geeigneter Zuverlässigkeitsanalyse und -modellbildung, quantitative/qualitative Zielsetzungen, aufgeteilt auf Subsysteme/Komponenten; Bestätigung, dass die Zielsetzungen praktikabel, realistisch und vollständig konsistent mit den Zuverlässigkeitsanforderungen sind.
- e) Begutachten von Zuverlässigkeitsrisiken – formalisierte, systematische Erkennung und Beurteilung von Zuverlässigkeitsrisiken; Einzelheiten technischer und auf die Zeitskala bezogener Risiken hinsichtlich der Zuverlässigkeitsanforderungen; Beiträge zum Zuverlässigkeitsrisikoregister, das den gegenwärtigen Stand aller erkannten Zuverlässigkeitsrisiken, gleichgültig, ob offen oder erledigt, genau wiedergibt sowie dessen Instandhaltung; Eingliederung in das Projekt-Risikoregister; Verknüpfungen mit der Zuverlässigkeitsstrategie im Zuverlässigkeitsplan und Wieder-Beurteilung der Risiken, um die auf der Basis der in der Zuverlässigkeitsstrategie enthaltenen Zuverlässigkeitsverfahren durchgeführte Risikosteuerung und -bewältigung begutachten zu können; Verknüpfungen mit dem Nachweisrahmen.
- f) Zuverlässigkeitsorientierter Entwurf – Entwurf, der die Zuverlässigkeitsanforderungen erfüllt, Entwurfsphilosophie, Zielsetzungen und Strategie [b), c), d) und m)]; Systembeschreibung/Begründung; Entwurfs-spielräume; Vertrauen in die Zuverlässigkeit an internen und externen Schnittstellen.
- g) Zuverlässigkeitsstatus / Entwicklungsbewertung – Nachweis unabhängiger Begutachtung und Bewertung von Entwurfsentscheidungen, Analysen und Prüfungen, die sich auf die Zuverlässigkeit auswirken, dokumentiert, um einen nachvollziehbaren Pfad zu bieten; Zuverlässigkeitsbeiträge zu formalen Entwicklungsbewertungen; Bestätigung, dass der Status der Zuverlässigkeitsprozesse und -maßnahmen mit der Strategie und dem Zuverlässigkeitsplan in Einklang sind.