

DIN EN 62853

ICS 03.120.01; 35.100.01

Einsprüche bis 2015-02-19

Entwurf**Zuverlässigkeit offener Systeme
(IEC 56/1575/CD:2014)**Open Systems Dependability
(IEC 56/1575/CD:2014)**Anwendungswarnvermerk**

Dieser Norm-Entwurf mit Erscheinungsdatum 2014-12-19 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@vde.com möglichst in Form einer Tabelle. Die Vorlage dieser Tabelle kann im Internet unter www.din.de/stellungnahme oder für Stellungnahmen zu Norm-Entwürfen der DKE unter www.dke.de/stellungnahme abgerufen werden;
- oder in Papierform an die DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE, Stresemannallee 15, 60596 Frankfurt am Main.

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

Gesamtumfang 82 Seiten

DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE

Inhalt

	Seite
Nationales Vorwort.....	4
Einleitung	5
1 Anwendungsbereich.....	6
2 Normative Verweisungen	6
3 Begriffe	6
4 Zuverlässigkeit offener Systeme	9
4.1 Belange der Zuverlässigkeit offener Systeme.....	10
4.2 Ziele	11
4.3 Verwandte Begriffe	11
4.4 Erreichen von Zuverlässigkeit offener Systeme	11
5 Anforderungen an die Zuverlässigkeit offener Systeme	12
5.1 Zuverlässigkeitsnachweis.....	12
5.2 Zusicherungsmetafall	12
6 Prozesssichten und Zusicherungsmetafälle.....	12
6.1 Prozesssichten	12
6.2 Zusicherungsmetafall	13
7 Prozesssichten zum Erreichen von Zuverlässigkeit offener Systeme	13
7.1 Konsensschaffende Prozesssicht	13
7.2 Prozesssicht zum Erreichen von Verantwortung	15
7.3 Ausfallantwort-Prozesssicht	16
7.4 Prozesssicht der Änderungsanpassung.....	19
8 Zusicherungsmetafälle zum Erreichen von Zuverlässigkeit offener Systeme.....	20
8.1 Zusicherungsmetafall für Konsistenz innerhalb des Systems.....	21
8.2 Zusicherungsmetafall für Konsistenz zwischen Systemen	21
8.3 Gültigkeitszusicherungsmetafall	22
8.3.1 Zweck	22
8.4 Angemessenheitszusicherungsfall	23
8.5 Vertrauenszusicherungsmetafall	24
Anhang A (informativ) Beziehung zu anderen Zuverlässigkeitsnormen.....	25
A.1 IEC 60050-192 Internationales Elektrotechnisches Wörterbuch – Teil 192 – Zuverlässigkeit	25
A.2 Beziehung zu IEC 60300-1 Zuverlässigkeitsmanagement	25
A.3 Beziehung zu IEC 62741 Darlegung von Zuverlässigkeitsanforderungen. Der Zuverlässigkeitsnachweis und ISO/IEC 15026-2 Zusicherungsfall.....	25
A.4 Beziehung zu ISO/IEC 15288 System-Lebenszyklus-Prozesse und ISO/IEC 42010 System- und Software-Engineering – Architekturbeschreibung.....	25
Anhang B (informativ) Ein Beispiellebenszyklus mit Zuverlässigkeit offener Systeme	26
Anhang C (informativ) Eine Beispielvorgabe für Zusicherungsfälle	28

	Seite
Anhang D (informativ) Rückkopplung und Zuverlässigkeit von Informationssystemen	29
D.1 Effekt der Architektur auf die Zuverlässigkeit.....	29
D.2 Effekt der Rückkopplung	29
D.3 Vermittlung um Zuverlässigkeit zu behalten	31
D.3.1 Definition von Kopplung	31
D.3.2 Enge oder lose Kopplung.....	31
D.3.3 Änderung der Kopplung	36
D.3.4 Entkoppelnde Effekte	38
D.3.5 Einfachere Entkopplung	39
D.3.6 Wahl der Paare	39
D.3.7 Verwendung von Paaren, um Systeme zu entwerfen.....	39
Literaturhinweise	42
 Bilder	
Bild 1 – Ein Beispiellebenszyklus ([2]).....	26
Bild 2 – Enge und lose Kopplung	32
Bild 3 – Kopplungstypen.....	33
Bild 4 – Indirekte Kopplung als direkte Kopplung.....	35
Bild 5 – Beispiele für die Kopplung im Entwurf von Nahrungsmitteldienstleistungen	40
 Tabellen	
Tabelle 1 – Kopplung und die Merkmale eines Unternehmens	41

Nationales Vorwort

Das internationale Dokument IEC 56/1575/CD:2014 „Open Systems Dependability“ (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 dieses Dokument ist das nationale Arbeitsgremium K 132 „Zuverlässigkeit“ der DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE (www.dke.de) zuständig.

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.

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können. ISO [und/oder] IEC sind nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren.

Das Original-Dokument enthält Bilder in Farbe, die in der Papierversion in einer Graustufen-Darstellung wiedergegeben werden. Elektronische Versionen dieses Dokuments enthalten die Bilder in der originalen Farbdarstellung.

Zuverlässigkeit offener Systeme

Einleitung

Die Zuverlässigkeit offener Systeme ist als die Fähigkeit eines Systems definiert, ungeachtet der Unsicherheit, Unvollständigkeit und Unbestimmtheit der Einheiten des Systems und seiner Umgebung, weiterhin seinen Dienst zu verrichten. Die Zuverlässigkeit offener Systeme ist eine Systemeigenschaft, sodass es die Fähigkeit aufweist, ununterbrochen Problemfaktoren, die Ausfälle verursachen können, zu entfernen, bei Ausfall eine schnelle und entsprechende Aktion zu ergreifen, den Schaden zu minimieren, soweit wie möglich die von den Anwendern erwarteten Dienste sicher und ununterbrochen anzubieten, und die Verantwortung für den Systembetrieb und die Systemprozesse aufrechtzuerhalten.

Da das untersuchte offene System von Zeit zu Zeit unterschiedlich sein kann, und sich seine Beschreibung aus einer Perspektive von der aus einer anderen Perspektive unterscheiden kann, müssen die klassischen Methodologien adaptiert werden, um diese Entwicklung zu berücksichtigen.

Die angesprochene Zielgruppe dieser Norm reicht von Anwendern, Eignern und Kunden bis hin zu Organisationen, die daran beteiligt sind, und die dafür verantwortlich sind sicherzustellen, dass die Anforderungen an die Zuverlässigkeit offener Systeme erfüllt werden. Organisationen beinhalten alle Unternehmenstypen und -größen, öffentliche und private Institutionen wie beispielsweise Regierungsbehörden, Handelsunternehmen und gemeinnützige Vereine.

1 Anwendungsbereich

Diese Internationale Norm legt eine Reihe von Anforderungen fest, die an Systemlebenszyklen gestellt werden, um die Zuverlässigkeit offener Systeme bei einem offenen System zu erreichen. Diese Internationale Norm gilt für Produktlebenszyklen, Systeme, Prozesse oder Dienste, die Hardware, Software und menschliche Aspekte oder jegliche integrierte Kombination dieser Elemente einschließen.

Diese Internationale Norm erweitert IEC 60300-1, indem sie Anforderungen zum Erreichen von Zuverlässigkeit speziell bei offenen Systemen zur Verfügung stellt.

Diese Internationale Norm kann für zuverlässigkeitsbezogene Kommunikation, Kommunikation der Zuverlässigkeit, Zuverlässigkeitsbewertung durch die Interessenvertreter des Systemlebenszyklus und die Auswertung der Zuverlässigkeit über die Systemlebenszyklen verwendet werden, ist aber nicht darauf beschränkt.

Diese Internationale Norm ist nicht für Zertifizierungszwecke bestimmt.

2 Normative Verweisungen

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

IEC 60050-192, *International Electrotechnical Vocabulary – Part 192 – Dependability*

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

ISO/IEC 15288, *Systems and software engineering – System life cycle processes*

ISO/IEC 15026, *Software and systems engineering – Software and systems assurance – Part 1 Concepts and vocabulary*

IEC 62741/Ed1., *Guide to the demonstration of dependability requirements. The dependability case*

ISO/IEC 15026, *Software and systems engineering – Software and systems assurance – Part 2 Assurance case*

ISO/IEC/IEEE 42010, *Systems and Software engineering – Architecture description*

3 Begriffe

Für die Anwendung dieses Dokuments gelten die folgenden Begriffe.

3.1

Verantwortung

Fähigkeit einer Organisation seine Entscheidungen und Aktivitäten sowie ihren Gesamteinfluss auf die Gesellschaft zu rechtfertigen. Rechenschaft ist gegenüber den Interessenvertretern der Organisation und der Gesellschaft im Allgemeinen abzulegen

Anmerkung 1 zum Begriff: ISO 26000:2010 *Guidance on social responsibility*. Eine Organisation ist denen gegenüber verantwortlich, die durch ihre Entscheidungen und Aktivitäten betroffen sind, sowie gegenüber der Gesellschaft im Allgemeinen bezüglich des Gesamteinflusses auf die Gesellschaft und ihrer Entscheidungen und Aktivitäten.

Anmerkung 2 zum Begriff: ISO 15489-1:2001 *Information and documentation – record management – Part 1 General*. Prinzip, dass Einzelne, Organisationen und die Gemeinschaft für ihre Aktionen verantwortlich sind und es erforderlich sein kann, dass sie diese gegenüber anderen erklären.

3.2

Angemessenheit (eines Zusicherungsfall)

ein Zusicherungsfall ist bezüglich einer bestimmten Eigenschaft ausreichend, falls das Erreichen der bestimmten Eigenschaft den Hauptanspruch des Zusicherungsfall beinhaltet

Anmerkung 1 zum Begriff: Ein Zusicherungsfall kann konsistent und gültig sein, falls sein Hauptanspruch eine Trivialität ist, aber ein Zusicherungsfall mit einem trivialen Hauptanspruch sollte nicht akzeptiert werden. Ein Zusicherungsfall ist ausreichend, falls der Bereich der Aspekte, den seine Ansprüche abdecken, groß genug ist, um die Zustimmung der Interessenvertreter zu erlangen. Angemessenheit ist eine der Eigenschaften, die anhand des Konsens der Interessenvertreter beurteilt wird.

3.3

Architektur

grundlegende Konzepte oder Eigenschaften eines Systems in seiner Umgebung, die durch seine Elemente, Beziehungen und durch seine Entwurfs- und Entwicklungsprinzipien verkörpert werden

[ISO 42010: 2011]

3.4

Zusicherungsfall

durchdachtes, prüffähiges Artefakt, das die Behauptung unterstützt, dass sein Oberanspruch (oder eine Reihe Ansprüche) erfüllt ist/sind, einschließlich der systematischen Argumentation und seiner zugrundeliegenden Beweise und expliziter Annahmen, die die Ansprüche unterstützen

Anmerkung 1 zum Begriff: Ein Zusicherungsfall enthält Folgendes und dessen Beziehungen: Ein Anspruch oder mehrere Ansprüche bezüglich der Eigenschaften, Argumente, die die Beweise und jegliche Annahmen mit dem Anspruch/den Ansprüchen logisch verknüpfen, Beweismaterial und möglicherweise Annahmen, die diese Argumente für den Anspruch/die Ansprüche unterstützen und eine Begründung für die Wahl des Oberanspruchs und des Verfahrens der Beweisführung, eine Darstellung eines Anspruchs oder von Ansprüchen und die Unterstützung dieser Ansprüche.

[QUELLE: ISO/IEC 15026-1:2014]

ANMERKUNG Ein Zusicherungsfall darf als ein durchdachtes und zwingendes Argument verstanden werden, das durch Beweismaterial unterstützt wird, dass ein System, Dienst oder eine Organisation bei einer festgelegten Anwendung, in einer festgelegten Umgebung wie vorgesehen arbeitet.

3.5

Zusicherungsmetafall

Zusicherungsfall, dessen Oberanspruch eine Aussage über einen anderen Zusicherungsfall ist, der Zielzusicherungsfall genannt wird. Ein Zusicherungsmetafall ist durch die folgenden Informationen gegeben: (a) der Name des Zusicherungsmetafalles; (b) der Zweck des Zusicherungsmetafalles; (c) die Eigenschaft des festzusetzenden Zielzusicherungsfall; (d) der Zielzusicherungsfall; (e) ein Argument, das durch den Beweis unterstützt wird, der seinen Oberanspruch „d) erfüllt c)“ demonstriert

3.6

Änderungsanpassung

Aktivitäten, um ein offenes System aufgrund Änderungen seines Zwecks oder seiner Umgebung, die die Wiederherstellung des Konsenses der Interessenvertreter hinsichtlich des offenen Systems erfordern, zu verändern und zu adaptieren

3.7

Konsens

explizite oder implizite Vereinbarung zwischen den Interessenvertretern des Systems von Interesse, zu seinen Anforderungen, seiner Risikobehandlung und der zum System dazugehörigen Verantwortung

3.8

Zuverlässigkeit

Fähigkeit zu funktionieren, wie und wann gefordert

Anmerkung 1 zum Begriff: Siehe ebenfalls [IEC 60300-1:201x, 60050-191-02-03].

3.9**Zuverlässigkeits-Prozesssicht**

Eine Zuverlässigkeits-Prozesssicht besteht aus der Beschreibung der folgenden Informationen. Siehe Abschnitt 6.1 dieser Internationalen Norm. (a) Name der Prozesssicht; (b) Zweck der Prozesssicht (Ziele); (c) Ergebnisse der Prozesssicht; und (d) Identifizierung und Beschreibung der Zuverlässigkeitsaktivitäten, die die Prozesssicht implementieren

Anmerkung 1 zum Begriff: Der Begriff Prozesssicht wurde ursprünglich in ISO/IEC 15288:2008 aufbauend auf dem Begriff der Sichten in ISO/IEC 42010:2007 eingeführt. (Zum Hintergrund des Begriffs der Prozesssichten wird auf ISO/IEC 15288:2008, Anhang D verwiesen.) Der Begriff der Prozesssichten in dieser Internationalen Norm beruht jedoch auf dem Begriff der Zuverlässigkeitsprozesse innerhalb der Lebenszyklen, die in IEC 60300-1 (CD3), Anhang C festgelegt sind.

3.10**Ausfallantwort**

sofortige Aktivität, die gegen einen Ausfall unternommen wird, um seinen Schaden zu minimieren, um sich davon zu erholen, und um der Verantwortung nachzukommen

3.11**Unbestimmtheit (der Beschreibung eines offenen Systems)**

Eigenschaft einer Beschreibung eines offenen Systems, dass die Interpretation von Beschreibungen eines offenen Systems nicht bestimmt ist. Unbestimmtheit bedeutet auch, dass die Beschreibungen eines Systems nicht alle relevanten Informationen beschreiben können; gegeben sei irgendeine Beschreibung, dann gibt es immer Eigenschaften, die nicht anhand dieser Beschreibung bestimmt werden können

3.12**interne Konsistenz (eines Zusicherungsfalles)**

Konsistenz eines Zusicherungsfalles in sich selbst

3.13**Überwachung (eines Systems)**

Sammeln und Speichern der Daten, die den Zustand des Systems darstellen und Alarmierung verantwortlicher Parteien bei Anomalien

3.14**offenes System**

ein System, dessen Grenzen, Funktionen und Struktur sich mit der Zeit verändern und sich gemäß der Perspektive unterscheiden

3.15**Zuverlässigkeit offener Systeme**

Fähigkeit, nach besten Kräften, weiterhin den Dienst eines Systems, ungeachtet der Unsicherheit, Unvollständigkeit und Unbestimmtheit der Einheiten des Systems und seiner Umgebung, zu verrichten

Anmerkung 1 zum Begriff: Die Zuverlässigkeit offener Systeme ist eine Eigenschaft eines Systems, sodass es die Fähigkeit aufweist, ununterbrochen Problemfaktoren zu entfernen, die Ausfälle verursachen können, bei Ausfall eine schnelle und entsprechende Aktion zu ergreifen, den Schaden zu minimieren, soweit wie möglich die von den Anwendern erwarteten Dienste sicher und ununterbrochen anzubieten, und die Aktivitäten und Aufgaben, die zum Erreichen von Verantwortung für den Systembetrieb und die Systemprozesse notwendig sind, aufrechtzuerhalten.

3.16**Prozess**

Menge von in Wechselbeziehung stehender oder miteinander interagierender Aktivitäten, die Eingaben in Ausgaben umwandeln

[ISO 9000]

3.17**Prozesssicht**

Sicht, die einer Prozessperspektive entspricht. Vgl. ISO/IEC 15288:2008, Anhang D

3.18

Prozessperspektive

die Prozessperspektive ist festgelegt durch: seine Interessenvertreter: – Anwender der Norm; – die Belange die sie betrifft: die Prozesse, die benötigt werden, um ein spezielles Engineeringinteresse widerzuspiegeln; – die Inhalte der resultierenden Prozesssichten sollten beinhalten: – Name der Prozesssicht; – Zweck der Prozesssicht; – Ergebnisse der Prozesssicht; und Identifizierung und Beschreibung der Prozesse, Aktivitäten und Aufgaben, die die Prozesssicht implementieren und auf die Quellen dieser Prozesse, Aktivitäten und Aufgaben in anderen Normen verweist

Anmerkung 1 zum Begriff: Die Anforderungen zur Dokumentierung von Perspektiven sind in ISO/IEC 42010, Unterabschnitt 5.3 zu finden. Diese Beschreibung ist mit jenen Anforderungen konsistent.

Anmerkung 2 zum Begriff: ISO/IEC 15288:2008, Abschnitt D.4 enthält ein Beispiel zur Anwendung dieser Perspektive.

[QUELLE: ISO/IEC 15288:2008, Anhang D]

3.19

Belastbarkeit

adaptive Leistungsfähigkeit einer Organisation in einer komplexen und veränderlichen Umgebung

[AS5050 (NWIP zur Übernahme durch ISO, bis dahin nicht auf diese Norm verweisen sondern die Definition verwenden)]

3.20

System von Interesse

<NOCH AUSZUFÜLLEN. WIRD ERKLÄREN: DASS ES VERSCHACHTELTE EBENEN VON SYSTEMEN GIBT, DASS DIE SYSTEM- UND EBENENGRENZEN NICHT KLAR GETRENNT SIND, DASS UNSER INTERESSE VON EINER EBENE ZU EINER ANDEREN WECHSELT UND DASS UNSER INTERESSE ZUR SELBEN ZEIT MEHRERE EBENEN ÜBERSPANNT.>

3.21

Gültigkeit (eines Zusicherungsfalles)

Stichhaltigkeit bezüglich der realen Welt

3.22

Sicht

Darstellung eines gesamten Systems aus der Perspektive einer damit in Verbindung stehender Menge von Bedenken

[QUELLE: ISO/IEC 42010:2007, IEEE Std 1471-2000]

3.23

Perspektive

Spezifikation der Konventionen zur Konstruktion und Verwendung einer Sicht. Ein Muster oder eine Vorlage aus der die individuellen Sichten, durch Festsetzung der Zwecke und Zielgruppen einer Sicht und der Techniken für ihre Erzeugung und Analyse, entwickelt werden

[QUELLE: ISO/IEC 42010:2007, IEEE Std 1471-2000]

4 Zuverlässigkeit offener Systeme

Zuverlässigkeit ist die Fähigkeit nach Bedarf und bei Bedarf zu funktionieren [IEC 60300-1:201X]. Teil 1 von IEC 60300 beschreibt das Zuverlässigkeitsmanagement nach dieser Definition. Heutige Einheiten erfordern jedoch aufgrund der folgenden Belange, zusätzlich zu der Beschreibung in IEC 60300-1, eine neue Betrachtung des Zuverlässigkeitsmanagements. [2]

- Sie sind groß, komplex und miteinander verbunden.
- Sie enthalten Blackbox-Komponenten. (Blackbox-Komponenten sind Komponenten, deren Funktionalität und Schnittstelle zu anderen Komponenten explizit festgelegt sind, aber deren Implementierungsdetails nicht spezifiziert sind.)
- Ihre Grenze, Funktion und Struktur tendiert dazu, unklar und sich ständig entwickelnd zu sein.
- Verantwortung ist kaum sicherzustellen.

- Aktionen zum Erreichen von Zuverlässigkeit müssen nicht nur in der Entwicklungsphase durchgeführt werden, sondern während des Lebenszyklus, einschließlich der Nutzungsphase und möglicherweise nach der Außerbetriebnahme.

Wie kann Zuverlässigkeit in Systemen erreicht werden, die groß und komplex sind *und sich ständig verändern*? Diese Frage ist zur Zeit eines der dringendsten Zuverlässigkeitsthemen. Moderne Systeme können während ihrer Lebensdauer nicht unveränderlich sein. Unablässige Änderungen sind eine Regel für Anwenderanforderungen, Dienstziele, Dienste, die über ein Netz empfangen wurden, Blackbox-Komponenten, die technologische Grundlage, usw. Herkömmliche Ansätze, z. B. Fehlertoleranztechniken, Risikoanalyse und formale Verifikation, die versuchen, die Systeme zu stabilisieren, können nicht die endgültige Antwort sein.

Dieser Abschnitt bietet Hintergrundinformationen zum Konzept der Zuverlässigkeit offener Systeme. Die normativen Teile dieser Internationalen Norm legen die Anforderungen an einen Systemlebenszyklus fest, um Zuverlässigkeit offener Systeme zu erreichen.

Die Zuverlässigkeit offener Systeme berücksichtigt den Aspekt moderner Systeme, die dazu tendieren außerhalb der Voraussetzungen zu fallen, die im herkömmlichen Zuverlässigkeitsmanagement gemacht werden. Systeme werden nicht länger als endgültig angenommen, sondern als offene Systeme, über die unser Wissen nicht vollständig oder sicher sein kann. Die Zuverlässigkeit offener Systeme zielt darauf ab, Dienstkontinuität bei derartiger Unvollständigkeit, Unbestimmtheit und Unsicherheit zu erreichen, oder einfacher, die Dienstkontinuität ungeachtet unerwarteter Ausfälle und unvorhersehbarer Änderungen zu erreichen. Es ist kein Merkmal eines Systems, sondern ein Merkmal des gesamten Lebenszyklus dieses Systems.

4.1 Belange der Zuverlässigkeit offener Systeme

Das herkömmliche Zuverlässigkeitsmanagement vermeidet Ausfälle effektiv durch den Schutz eines Systems vor den Risiken nachteiliger Änderungen. Es setzt voraus, dass die Bedürfnisse der Interessenvertreter, die Nebenbedingungen des Systems, die Anforderungen an das System und die Annahmen über die Umgebung weitgehend vorher festgelegt und unveränderlich sind. Obwohl zeitabhängige Aspekte ihr Hauptanliegen sind, wird angenommen, dass die betrachteten zeitlichen Abhängigkeiten, wie zum Beispiel Alterungsdegradation, vorhersehbar sind.

Jedoch werden diese Voraussetzungen des herkömmlichen Zuverlässigkeitsmanagements bei modernen Systemen immer weniger anwendbar. Diese Systeme weisen immer mehr Merkmale sogenannter „Systeme von Systemen“ [1] und „offener Systeme“ [2] auf. Änderungen an diesen Systemen sind weniger vorhersehbar und steuerbar.

Ein modernes System muss seine Dienste mit einer großen Vielzahl anderer miteinander verbundener Systeme austauschen. Diese umgebenden Systeme werden nach ihren eigenen Prinzipien und Interessenvertretern verwaltet und ihre Schnittstellen sind Änderungen aufgrund verschiedener Gründe vorbehalten. Die durchdringende Natur des Systems bedeutet, dass es einer vielfältigen Menge an Interessenvertretern dienen muss. Jede(r) hat sein/ihr eigenes Ziel, das sich mitunter verändert und es gibt möglicherweise keine einzelne Autorität über das System. Somit verändern sich die externen Bedingungen des Systems, wie zum Beispiel Anforderungen und Nebenbedingungen, häufig und unvorhersehbar und sind zu einem bestimmten Zeitpunkt schwer vollständig zu erfassen.

Im System selbst ist ebenfalls eine ähnliche Unsicherheit und Unvollständigkeit vorhanden, d. h. über seine Funktionen, interne Struktur und die Grenze. Seine Untersysteme werden oftmals von unterschiedlichen Parteien verwaltet und die Integratoren des Systems haben möglicherweise kein vollständiges Wissen und Kontrolle über sie. Während des Betriebs dürfen durch verschiedene Interessenvertreter Dienste und Komponenten dem System dynamisch hinzugefügt oder aus dem System entfernt werden, was die Systemgrenze unklar macht.

Aus diesen Gründen sowie der reinen Komplexität und des Umfangs des Systems ist es für jeden Interessenvertreter sehr schwierig, das System und sein Management auf ausreichende Vollständigkeit und Sicherheit festzulegen, zu verstehen oder zu steuern. Unvorhersehbare Änderungen und unerwartete Ausfälle verschiedenen Grades sind Teil des Systemverhaltens. Die Verwendung des Begriffs offene Systeme betont diesen Aspekt moderner Systeme.

Die Zuverlässigkeit offener Systeme legt einen Schwerpunkt darauf, Dienstkontinuität unter unvorhersehbaren und veränderlichen Risiken zu erreichen.

Die wahren, impliziten Erwartungen an das System sind immer relativ zum Kontext anderer umgebender Systeme und Interessenvertreter. Wenn sich der Kontext ändert und die Unvollständigkeit und Unsicherheit auf die eine oder andere Art beigelegt werden, müssen sich die Anforderungen und Annahmen des Systems an die entsprechenden Änderungen anpassen. Diese Änderungen können im Voraus nicht vollständig erwartet oder festgelegt werden.

Das Zuverlässigkeitsmanagement eines Systems kann für ein einzelnes System nicht länger in sich geschlossen sein. Es kann auch nicht das Management nach einem Ausfall als außerhalb seines Anwendungsbereichs betrachten. Die verschiedenen unterschiedlichen Ebenen der Zuverlässigkeitsziele der verschiedenen unterschiedlichen Ebenen von Systemen, die das Zielsystem umgeben, müssen berücksichtigt werden.

Ungeachtet unvorhersehbarer und nicht identifizierter Risiken kann niemand für die Zuverlässigkeit vollständig verantwortlich sein, sie muss aber auf geeignete Weise verwaltet werden, um den Betrieb des Systems aufrechtzuerhalten.

4.2 Ziele

Es reicht nicht aus, die Zuverlässigkeit innerhalb der Grenze fester Anforderungen für das und Annahmen über das System zu erreichen, und alles andere als „außerhalb des Anwendungsbereichs“ zu verweisen. Als eine Frage der Einstellung muss man sogar unter nicht eingehaltenen Annahmen, Anforderungen, die durch externe Änderungen außer Kraft gesetzt wurden und schließlich unter Systemausfällen, nach Vertrauen ins System streben.

Das Hauptziel ist es, einen Grad an Dienstkontinuität, im Kontext der umgebenden Systeme, Interessenvertreter und der Umgebung, so gut wie möglich und unter jeglichen Bedingungen aufrechtzuerhalten.

4.3 Verwandte Begriffe

Belastbarkeit ist mit der Zuverlässigkeit offener Systeme eng verwandt. Beide Begriffe betrachten die Abweichung vom Normalbetrieb. Belastbarkeit betont jedoch den Prozess zum Normalbetrieb zurückzukehren, während die Zuverlässigkeit offener Systeme die Tatsache hervorhebt, dass sogar die Definition von „Normalbetrieb“ mitunter oder aufgrund der Perspektive, die der Interessenvertreter einnimmt, oder aufgrund der Umgebung variieren kann.

Andererseits unterscheidet sich die Idee der Fehlertoleranz von jener bei der Zuverlässigkeit offener Systeme. Es wird angenommen, dass eine vorher festgelegte Liste alle wesentlichen potentiellen Fehler aufzählt; beziehungsweise wird vorausgesetzt, dass die Schaffung einer solchen Annahme der einzige Weg ist, an der Zuverlässigkeit zu arbeiten. Um Fehlertoleranz zu erreichen, muss ein festgelegtes, greifbares Verfahren gegeben sein, um von der Abweichung zum Normalbetrieb zurückzukehren, wobei Abweichung und Normalbetrieb explizit festgelegt sind. Bei der Zuverlässigkeit offener Systeme werden die Situationen betrachtet, in denen dies nicht explizit festgelegt werden kann.

4.4 Erreichen von Zuverlässigkeit offener Systeme

Systeme werden nicht länger als endgültig angenommen, sondern als offene Systeme über die unser Wissen nicht vollständig oder sicher sein kann. Die Zuverlässigkeit offener Systeme zielt darauf ab, Dienstkontinuität bei derartiger Unvollständigkeit und Unsicherheit zu erreichen, oder einfacher, die Dienstkontinuität ungeachtet unerwarteter Ausfälle und Änderungen zu erreichen. Es ist dann kein Merkmal eines Systems, sondern ein Merkmal des gesamten Lebenszyklus dieses Systems. Die Zuverlässigkeit offener System ist eine Eigenschaft eines Systems, sodass es die Fähigkeit aufweist:

- ununterbrochen Problemfaktoren zu entfernen, die Ausfälle verursachen können;
- schnelle und entsprechende Aktionen zu ergreifen, wenn ein Ausfall auftritt;
- Schaden zu minimieren und abzumildern;

- soweit wie möglich die von den Interessenvertretern erwarteten Dienste ununterbrochen anzubieten, und;
- die Aktivitäten und Aufgaben aufrechtzuerhalten, um Verantwortung für den Systembetrieb und die Systemprozesse zu erreichen.

5 Anforderungen an die Zuverlässigkeit offener Systeme

Damit ein Systemlebenszyklus die Zuverlässigkeit offener Systeme unterstützt, sollte Folgendes bereitgestellt werden.

5.1 Zuverlässigkeitsnachweis

Ein Zuverlässigkeitsnachweis, dessen Oberanspruch angibt, dass der Systemlebenszyklus mit allen in Abschnitt 7 festgelegten Prozesssichten ausgerüstet ist, d. h. konsensschaffende Prozesssicht, Prozesssicht zum Erreichen von Verantwortung, Ausfallantwort-Prozesssicht und Prozesssicht der Änderungsanpassung.

5.2 Zusicherungsmetafall

Zusicherungsfälle, die in Abschnitt 8 festgelegt wurden (d. h. Zusicherungsfall der inneren Systemkonsistenz, Zusicherungsfall der Konsistenz zwischen Systemen, Gültigkeitszusicherungsfall, Angemessenheitszusicherungsfall und Vertrauenszusicherungsfall), deren Zielzuverlässigkeitsnachweis 5.1 ist.

6 Prozesssichten und Zusicherungsmetafälle

Die Aktivitäten, um Zuverlässigkeit offener Systeme zu erreichen, sind über Prozesse im Systemlebenszyklus verteilt. Der Begriff der Prozesssicht wurde eingeführt, um solche Aktivitäten an einem einzelnen Ort zusammenzutragen. Er wurde ursprünglich in ISO/IEC 15288:2008 aufbauend auf dem Begriff der Sichten in ISO/IEC 42010:2007 eingeführt. (Zum Hintergrund des Begriffs der Prozesssichten wird auf ISO/IEC 15288:2008, Anhang D verwiesen.) Der Begriff der Prozesssichten in dieser Internationalen Norm beruht jedoch auf dem Begriff der Zuverlässigkeitsprozesse innerhalb der Lebenszyklen, die in IEC 60300-1 (CD3), Anhang C festgelegt sind.

Diese Internationale Norm übernimmt Prozesssichten als ein Framework, um die geforderten Aktivitäten festzulegen. Abschnitt 7 legt vier Prozesssichten zum Erreichen von Zuverlässigkeit offener Systeme fest.

Um die Zuverlässigkeit offener Systeme zu erreichen, ist die Existenz der Aktivitäten in der Prozesssicht nicht ausreichend, es muss auch sichergestellt werden, dass diese Aktivitäten tatsächlich die in den Prozesssichten festgelegten Eigenschaften aufweisen. Diese Internationale Norm erfordert einen Zuverlässigkeitsnachweis [IEC 62741/Ed1: *Demonstration of dependability requirements. The dependability case*] [ISO/IEC 15026-2 *Assurance case*] als eine Demonstration der Zusicherung der Zuverlässigkeit.

Offene Systeme sind unklar und veränderlich; folglich müssen sich deren Zuverlässigkeitsnachweise mitunter ändern, aber ob deren Änderung konsistent für die Änderung des Systems ist, ist nicht offensichtlich. Das Ergebnis der Untersuchung dieser Konsistenz ist in dieser Internationalen Norm als Zusicherungsmetafall gefordert. Ein Zusicherungsmetafall ist hier ein Zusicherungsfall über den Zuverlässigkeitsnachweis. Abschnitt 8 legt die Anforderungen an die Zusicherungsmetafälle fest.

6.1 Prozesssichten

Eine Zuverlässigkeits-Prozesssicht wird durch Bereitstellung der folgenden Informationen festgelegt:

- a) Name der Prozesssicht;
- b) Zweck der Prozesssicht (Ziele);
- c) Ergebnisse der Prozesssicht; und
- d) Identifizierung und Beschreibung der Zuverlässigkeitsaktivitäten, die die Prozesssicht implementieren.

ANMERKUNG Abschnitt 7 legt jede der vier Zuverlässigkeits-Prozesssichten durch Bereitstellung obiger Punkte a) - d) fest. Die Implementierung dieser Prozesssichten muss nach einem angemessenen Zeitraum überprüft werden, sodass sie, falls notwendig, geändert werden kann.

6.2 Zusicherungsmetafall

Ist ein Zielzusicherungsfall gegeben, dann ist ein Zusicherungsmetafall ein Zusicherungsfall über den Zielzusicherungsfall. Daher ist ein Zusicherungsmetafall ein Spezialfall eines Zusicherungsfalles. Ein Zusicherungsmetafall ist durch die folgenden Informationen nach ISO/IEC 15026-2 *Assurance Case* gegeben:

- Begründung. Der Begründungsteil eines Zusicherungsmetafalles gibt den Zweck des Zusicherungsmetafalles an;
- Oberanspruch. Der Oberanspruch eines Zusicherungsmetafalles besteht aus Eigenschaften des einzurichtenden Zielzusicherungsmetafalles;
- Argument. Das Argument eines Zusicherungsmetafalles demonstriert seinen Oberanspruch mit Unterstützung seines Beweises;
- Beweis.

Abschnitt 8 legt fünf Zusicherungsmetafälle durch Folgendes fest:

- e) Name des Zusicherungsmetafalles;
- f) Zweck des Zusicherungsmetafalles; und
- g) durch den Zusicherungsmetafall einzurichtende Eigenschaften.

7 Prozesssichten zum Erreichen von Zuverlässigkeit offener Systeme

7.1 Konsensschaffende Prozesssicht

In offenen Systemen ist der Konsens zwischen Interessenvertretern der Ersatz für die objektive Wahrheit, da es kein vollständiges Verständnis des gesamten Systems und seiner Umgebung gibt. Der Konsens ist die einzige Sache, die als Kriterium für die Systemlebenszyklusprozesse funktionieren kann, selbst wenn der Konsens nur einen Teil des Systems und seiner Umgebung erfasst. Darüber hinaus muss der Konsens explizit dokumentiert werden und angemessen über den Systemlebenszyklus verwaltet werden. Ein derartiges Management des Konsenses erfordert, neben anderen Dingen, die fortlaufende Validierung des Konsenses und seiner zugrundeliegenden Regeln gegen fortlaufende Änderungen des Systems, der Grenze und der Umgebung.

7.1.1 Zweck

Zweck der konsensschaffenden Prozesssicht ist es, einen Konsens zwischen den Interessenvertretern eines offenen Systems als Grundlage des Systemlebenszyklus zu schaffen.

7.1.2 Ergebnisse

7.1.2.1

Interessenvertreter und ihre Rollen bezüglich des Systems von Interesse werden identifiziert.

7.1.2.2

Die Voraussetzung für jeden Interessenvertreter wird implizit oder explizit eruiert.

ANMERKUNG Eine nicht identifizierte Voraussetzung kann möglicherweise schädlich für die Zuverlässigkeitskommunikation zwischen den Interessenvertretern sein und kann ein Hindernis bei der Konsensschaffung sein.

7.1.2.3

Die Anforderungserhebung wird in gerechter Weise durchgeführt, um nicht einen speziellen Interessenvertreter ungerechtfertigt zu bevorzugen.

ANMERKUNG Tendiert die erhobene Anforderung dazu, das Interesse eines speziellen Interessenvertreters abzubilden, wird früher oder später etwas Falsches zum Vorschein kommen. Falsche oder erzwungene Anforderungen, die ungültig sind, können einen unverhältnismäßigen Langzeiteinfluss auf das Versagen großer offener Systeme, Ihre Ziele zu erreichen, haben.

7.1.2.4

Anfängliche Interessenkonflikte zwischen Interessenvertretern werden auf gerechte und aufmerksame Weise gelöst und die objektive Begründung der Lösung wird zur Verfügung gestellt.

7.1.2.5

Die Mittel, um den Konsens der Interessenvertreter bei Änderungen der Anforderungen der Interessenvertreter, bei Änderungen des Systems von Interesse oder der Umgebung aufrechtzuerhalten, werden zur Verfügung gestellt.

ANMERKUNG Solche Änderungen werden möglicherweise durch die Behandlung nach einem Ausfall hervorgerufen.

ANMERKUNG Den Konsens der Interessenvertreter aufrechtzuerhalten, bedeutet ihn zu validieren, zu überdenken und zu erneuern.

7.1.2.6

Die Mittel zum Management der Beteiligung der Interessenvertreter am System von Interesse werden zur Verfügung gestellt. Dazugehörige Interessenvertreter sollten an der Entscheidungsfindung beteiligt werden und eine unberechtigte Teilnahme sollte vermieden werden. Die Mittel mit der die Eignung der Interessenvertreter für jede Entscheidungsmenge gerechtfertigt werden und die Teilnehmer sollten für eine Prüfung verfügbar sein.

7.1.2.7

Die Personen oder Einheiten, die zum Erreichen der oben angeführten Ergebnisse verantwortlich sind, werden identifiziert.

7.1.3 Implementierungsaktivitäten

<Anmerkung der Redaktion: Dieser Abschnitt ist zu erweitern, um zu erklären, wie die Ergebnisse der folgenden Aktivitäten aus 60300-1 zu erzielen sind.>

Festlegung der Einheitenanforderung

Identifizierung realisierbarer Entwurfslösungen

Aufrechterhaltung der Einheitenleistung durch Instandhaltung

Aufrüstung der entworfenen Einheit

Beendigung des Einheitendienstes nach einem Ausbuchsungsplan

Detaillierte Anforderungen an die Zuverlässigkeit

Erzeugung eines Zuverlässigkeitsplans für den gesamten Lebenszyklus

Zuverlässigkeitsvorhersage

Archivierung der erreichten Zuverlässigkeitsdaten für eine zukünftige Verwendung

7.2 Prozesssicht zum Erreichen von Verantwortung

Verantwortung ist die gesamte Verantwortlichkeit für die durchgeführten Entscheidungen und Aktionen in jedem Teil des Lebenszyklus eines Systems, einschließlich Entwicklung, Betrieb und Außerbetriebnahme. Verantwortung beinhaltet die Verantwortlichkeit Informationen für die Anwender und andere Interessenvertreter bereitzustellen. Es gibt keine zentrale Steuerung offener Systeme, sodass die Partei, die für eine Entscheidung oder eine Aktion verantwortlich ist nicht trivial identifiziert werden kann.

Verantwortung hat einen unmittelbaren Einfluss auf das Vertrauen der Menschen in das System und solche subjektiven Eigenschaften des Systems von Interesse sind essentiell für die Zuverlässigkeit.

Verantwortung ist notwendig, um die Zuverlässigkeit des Systems von Interesse und seiner Umgebung, einschließlich anderer miteinander verbundener Systeme, zu erreichen. Einflüsse von Ausfällen eines Systems können durch umgebende miteinander verbundene Systeme behoben werden, falls letzteres die bereitgestellten Informationen teilt.

7.2.1 Zweck

Der Zweck der Prozesssicht zum Erreichen von Verantwortung ist es, Vertrauen in das System von Interesse zu erlangen und Informationen über dieses mit den Interessenvertretern und miteinander verbundener Systeme in der Umgebung zu teilen.

7.2.2 Ergebnisse

7.2.2.1

Die Abbildung des Konsenses der Interessenvertreter auf die Systemüberwachung wird erstellt. Jede Aktion der Systemüberwachung ist auf spezifische Teile des Konsenses der Interessenvertreter rückführbar.

7.2.2.2

Das Personal oder die Organisation, die verantwortlich sind, Rechenschaft über das Systemverhalten abzugeben, werden klar identifiziert.

7.2.2.3

Der Betriebsprozess ist so organisiert, dass sofortige, gültige und angemessene Antworten auf berechtigte Anfragen eines Interessenvertreters nach Informationen über das System von Interesse während des gewöhnlichen Betriebs gegeben werden. Die Interessenvertreter sollten in der Lage sein solchen Antworten zu vertrauen.

ANMERKUNG Der Betriebsprozess ist ein Lebenszyklusprozess, der in ISO/IEC 15288 festgelegt ist. Dieser Prozess erstellt Anforderungen für das Personal und weist Personal zu, das das System betreibt, und überwacht die Dienste und die Betreiber-Systemleistung. Um die Dienste aufrechtzuerhalten, identifiziert und analysiert es Anomalien bezüglich der Vereinbarungen, der Anforderungen der Interessenvertreter und der organisatorischen Nebenbedingungen.

7.2.2.4

Die Ausfallantwort-Prozesssicht, wie sie in Abschnitt 7.3 festgelegt ist, ist so organisiert, sodass angemessene und relevante Informationen gewählt werden und jedem Interessenvertreter des Systems von Interesse, den Interessenvertretern der miteinander verbundenen Systeme und der allgemeinen Öffentlichkeit gegeben werden. Die gegebene Information ist umfassend und die Empfänger verstehen sie mühelos. Sie ist so gewählt, dass sie die empfängereigene Minderung von einem Schaden des Ausfalls aktiviert. Die Empfänger sind von der Angemessenheit und Gültigkeit der gegebenen Informationen überzeugt.

7.2.2.5

Das System von Interesse sammelt Logdaten und andere Beweise, um die Angemessenheit und Gültigkeit der bereitgestellten Informationen herzustellen und zu begründen. Die objektive Darstellung der Begründung dieser Einrichtung wird zur Verfügung gestellt. Die gesammelten Logdaten müssen gespeichert werden und müssen für eine spätere Untersuchung zugänglich sein.

7.2.2.6

Änderungen der Anforderungen des Systems, der Erwartungen an das System, der Beschreibungen des Systems und der Leistung des Systems werden dokumentiert und publiziert.

7.2.2.7

Lücken zwischen jeder der Anforderungen, Erwartungen, Beschreibungen und Leistung des Systems werden dokumentiert und publiziert.

7.2.2.8

Die Personen oder Einheiten, die zum Erreichen der oben angeführten Ergebnisse verantwortlich sind, werden identifiziert.

7.2.3 Implementierungsaktivitäten

<Anmerkung der Redaktion: Dieser Abschnitt ist zu erweitern, um zu erklären, wie die Ergebnisse der folgenden Aktivitäten aus 60300-1 zu erzielen sind.>

Aufrechterhaltung der Einheitenleistung durch Instandhaltung

Überwachung der Leistung

Betrieb und Wartung der Einheit

Datensammlung und Probenahme

7.3 Ausfallantwort-Prozesssicht

Das Ergebnis der Ausfallantwort-Prozesssicht eines Lebenszyklus ist es, dass die Dienste mit so geringen Störungen wie möglich fortbestehen, in der in dem Kontext am zweckmäßigsten Art und Weise. Der Ausfall ist möglicherweise unvorhergesehen oder vorhergesehen, wird aber als zu unwahrscheinlich oder zu teuer erachtet, um ihn zu verhindern, oder ist vorhergesehen und wird behandelt, aber dennoch aufgrund unvorhergesehener Ereignisse nicht verhindert. Es können keine spezifischen Gegenmittel für unvorhergesehene Ereignisse, die Ausfälle verursachen, vorbereitet werden. Es können und sollten jedoch im Voraus generische Maßnahmen vorbereitet werden, um ihre zügige Ausführung zu ermöglichen. Diese beinhalten Mittel, um schnell ausfallspezifische Gegenmaßnahmen für den vorliegenden Kontext zu bilden, oder falls nötig den Kontext zu ändern. Der Schutz gegen absehbare Ausfallarten führt ebenfalls, ungeachtet ihrer Ursachen, zu solchen generischen Maßnahmen. Menschliches Eingreifen spielt die Schlüsselrolle. Der Ausfall tritt auf, nachdem mechanische Mittel ausgereizt sind. Entscheidungsfindung und Implementierung der entschiedenen Aktionen sollten durch Computer unterstützt werden.

Menschliches Eingreifen spielt die Schlüsselrolle, da nicht alle Ausfälle durch vorprogrammierte mechanische Mittel verhindert oder abgeschwächt werden können. Entscheidungsfindung und Implementierung der entschiedenen Aktionen sollten durch Computer unterstützt werden.

Menschliches Eingreifen spielt die Schlüsselrolle, da nicht alle Ausfälle durch vorprogrammierte mechanische Mittel verhindert oder abgemildert werden können. Für eine schnelle und angemessene Antwort, sollte das menschliche Eingreifen bei der Entscheidungsfindung und Implementierung der entschiedenen Aktionen durch Computer unterstützt werden.

Menschliches Eingreifen spielt die Schlüsselrolle, wenn der Ausfall auftritt, nachdem vorprogrammierte mechanische Mittel ausgereizt sind. Entscheidungsfindung und Implementierung der verschiedenen Aktionen sollten durch eine Kooperation zwischen Mensch und Computer unterstützt werden.

7.3.1 Zweck

Der Zweck der Ausfallantwort-Prozesssicht ist es, rückwirkende Mittel zum Management der zerstörerischen Auswirkungen des Systembetriebs, die beim Risikomanagement identifiziert werden, aber deren Ursachen absichtlich oder unabsichtlich identifiziert werden können, vorzubereiten. Diese Aktionen nach einem Ausfall beinhalten Maßnahmen gegen identifizierte Auswirkungen, für die zum Zeitpunkt der Identifizierung der Auswirkung nach bestem Wissen keine Ursachen vorstellbar sind. Es ist möglich sich auf solche Auswirkungen vorzubereiten, aber nur durch Vorbereitung dessen, was zu tun ist, nachdem sich solche Auswirkungen zeigen; Verhinderung und Schadensminderung sind nicht möglich, da die Ursache nicht identifiziert sein wird.

7.3.2 Ergebnisse

7.3.2.1

Es werden Mittel zur Erkennung von Fehlzuständen, Fehlaussagen, Ausfällen und ihrer Vorläufer bereitgestellt und angewandt. Eine objektive Beschreibung der Rechtfertigung der Angemessenheit dieser Menge an Mitteln wird gegeben. Außerdem werden die folgenden drei Listen bereitgestellt:

- h) Liste der schädlichen Ereignisse (d. h. Fehlzustände, Fehlaussagen und Ausfälle), die als möglicherweise auftretend erachtet werden;
- i) Liste der schädlichen Ereignisse die als unwahrscheinlich erachtet werden, die aber überwacht werden;
- j) Liste der schädlichen Ereignisse die als unwahrscheinlich erachtet werden und daher nicht überwacht werden oder die als absolut unwahrscheinlich erachtet werden.

ANMERKUNG Es gibt außerdem „nicht identifizierte“ oder „unerwartete“ schädliche Ereignisse. Diese können in keiner der oben angeführten Listen sein, da sie bisher von keinem der Interessenvertreter erkannt wurden.

7.3.2.2

Es werden Mittel zur Verfügung gestellt, um Ausfälle anhand der Vorläufer vorherzusagen.

7.3.2.3

Identifizierte Vorläufer und frühe Anhaltspunkte für Ausfälle werden überwacht.

7.3.2.4

Die Auswirkungsanalyse und die Einflussanalyse erkannter und vorhergesagter Ausfälle wird gegeben und ihr Ergebnis wird in einer objektiven, schriftlichen Form bereitgestellt; die letztere Bereitstellung ist essentiell, um das Vertrauen der Interessenvertreter zu erlangen.

7.3.2.5

Eine Menge von Aktionen nach Ausfall für das Eintreten des Ausfallereignisses (zu ergreifende Aktionen als Antwort auf Ausfälle des Systems von Interesse) werden zur Verfügung gestellt. Die Identifikation dieser Menge von Aktionen beruht auf dem Ergebnis der Auswirkungsanalyse und der Einflussanalyse. Diese Aktionen sind vom System von Interesse sowie vom Personal, das mit dem Systemlebenszyklus in Beziehung steht, durchzuführen.

7.3.2.6

Die für Ausfälle bereitgestellten Aktionen nach einem Ausfall verschärfen nicht den Schaden und erhöhen nicht das Risiko weiterer Schäden.

ANMERKUNG In einigen Fällen verursachen Aktivitäten zur Schadensminderung weitere Schäden. Diese sollten nicht schlimmer sein, als die, die ohne solches Eingreifen aufgetreten wären.

7.3.2.7

Es wird eine Menge zu ergreifender Aktionen nach einem Fehlschlagen der in 7.3.2.5 festgelegten Aktionen bereitgestellt. Wenn diese Aktionen selbst ausfallen, werden diese Aktionen entweder rekursiv angewandt, oder verschiedene Schichten von Aktionen für den Ausfall werden zur Verfügung gestellt.

7.3.2.8

Es werden Mittel zur Reduzierung des Schadens beim Ereignis von Ausfällen mit nicht identifizierten Ursachen bereitgestellt.

ANMERKUNG Mittel zur Reduzierung des Schadens beim Ereignis von Ausfällen mit nicht identifizierten Ursachen beinhalten jene, die sofort fehlerhafte Teile des Systems von Interesse identifizieren, jene, die nicht funktionierende Teile isolieren, um andere normal arbeitende Teile zu schützen, jene, die überlebende Dienste auf einer Ebene aufrechterhalten, die durch den Konsens der Interessenvertreter vereinbart wurde und jene, die zur Erholung vom Ausfall verwendet werden.

7.3.2.9

Es werden Mittel zur Verfügung gestellt, um Schäden am gesamten System zu reduzieren, das nicht nur aus dem System von Interesse sondern auch aus anderen angeschlossenen Systemen besteht.

7.3.2.10

Es werden Mittel bereitgestellt, um das System von Interesse an Änderungen in Hinsicht auf Ausfälle anzupassen.

ANMERKUNG Solche Änderungen beinhalten die Identifizierung der Ausfallauswirkungen, das Schadensauswertungsverfahren und die Auswertung des Wertes der Dienste, die vom System von Interesse bereitgestellt werden und durch die Anwender und das verbundene System durchgeführt werden.

7.3.2.11

Das Verfahren, um die notwendigen Informationen beim Fehlerereignis für andere Prozesssichten, wie zum Beispiel die Prozesssicht zum Erreichen von Verantwortung und die Prozesssicht der Änderungsanpassung, bereitzustellen, wird aufgebaut.

7.3.2.12

Die verantwortlichen Interessenvertreter, die die Aktivitäten und Aufgaben dieser Prozesssicht implementieren, müssen identifiziert werden.

7.3.3 Implementierungsaktivitäten

<Anmerkung der Redaktion: Dieser Abschnitt ist zu erweitern, um zu erklären, wie die Ergebnisse der folgenden Aktivitäten aus 60300-1 zu erzielen sind.>

Überwachung der Leistung

Vorhersage der Zuverlässigkeit

Analyse und Vorhersage der Zuverlässigkeit

Zuverlässigkeitswachstum durch Entwurfsänderungen und neue Softwareversionen

7.4 Prozesssicht der Änderungsanpassung

Das Ergebnis der Prozesssicht der Änderungsanpassung des Systemlebenszyklus ist es, dass das System seinen „gebrauchstauglich“ Zustand, ungeachtet unvorhergesehener Änderungen der Anforderungen, Umgebungen und in der Tat Ziele (des Zwecks), aufrechterhält. Die Prozesssicht verwirklicht dies durch Anpassung des Systems an die Änderungen. Es hält die Fähigkeit aufrecht, die Dienste durch echte Lösungen bis zur Lücke zwischen „Ist“ und „Soll“ weiterzubetreiben und fokussiert darauf sicherzustellen, dass derselbe Ausfall nicht wiederholt wird.

Es gibt viele Arten von Änderungen, die Anpassungen erfordern. Änderungen treten in anderen Systemen auf, die mit dem System von Interesse verbunden sind. Änderungen der technologischen, geschäftlichen und sozialen Umgebungen treten beim heutigen raschen Innovationstempo häufiger auf. Jede Erkennung von unerwarteten Ereignissen signalisiert eine Änderung der Annahmen, die immer unvollständig und unsicher sind. Änderungen sind möglicherweise nicht explizit offensichtlich; oftmals müssen sie zum Beispiel durch regelmäßige Überprüfungen aktiv ausfindig gemacht werden. Erforderliche Anpassungen müssen auch nicht notwendigerweise das System selbst betreffen. Die ganze Menge seiner Lebenszyklusprozesse muss überprüft werden, und wenn nötig adaptiert werden. Sogar die weitere Beeinflussung und Änderung der Umgebung könnte eine Anpassung sein.

7.4.1 Zweck

Der Zweck der Prozesssicht der Änderungsanpassung ist es, Änderungen der Anforderungen, der Umgebungen und des Systems von Interesse selbst zu erkennen, um es zu überdenken und die Aktionen durchzuführen, die benötigt werden, um die benötigten Dienste weiterhin bereitzustellen, und somit die Zuverlässigkeit des Systems von Interesse weiterhin zu wahren.

7.4.2 Ergebnisse

7.4.2.1

Es werden Änderungen des Kontexts, der Annahmen, der Risiken und anderes identifiziert, die eine Anpassung des Systems von Interesse erfordern.

ANMERKUNG Die Einheiten, die solchen Änderungen unterliegen, beinhalten die Anforderungen der Interessenvertreter, Annahmen über die Umgebung des Systems von Interesse, die Wahrnehmung der durch das System von Interesse bereitgestellten Dienste durch die Interessenvertreter und das Verständnis des Konsenses durch die Interessenvertreter.

ANMERKUNG Die Identifikation wird von der Anforderungsänderung des Systems abgeleitet. Die Anforderungen dürfen sich verändern, wenn sich die Umgebung und der Zweck des Systems verändern. Eine andere Möglichkeit ist es, dass die Anforderungsänderung des Systems durch die Ursachenanalyse des vergangenen Ausfalls abgeleitet wird.

7.4.2.2

Es werden technische oder nicht technische Mittel für die Anpassung identifiziert, die für jede Änderung aus 7.4.2.1 benötigt werden. Es werden auch Mittel bereitgestellt, um die überarbeiteten Dienste mit geringsten Störungen der bestehenden laufenden Dienste einzusetzen.

7.4.2.3

Es wurde eine kausale Analyse durchgeführt, um den Grund klarzustellen, warum das System von Interesse den gebrauchstauglichen Zustand verlieren würde.

7.4.2.4

Es wird Unterstützung für Entwickler bereitgestellt, um mögliche Anpassungen zu entwickeln.

7.4.2.5

Es werden Mittel bereitgestellt, um die Interessenvertreter über mögliche Änderungen des Systems von Interesse und deren Auswirkungen zu informieren. Es wird auch Unterstützung für die Interessenvertreter für Verhandlungen unter veränderten Umständen bereitgestellt. Durch Anpassung an eine geänderte Umgebung wird der gebrauchstaugliche Zustand des Systems von Interesse für so viele Interessenvertreter wie möglich wiedererlangt, und dies geschieht ohne unzulässige Störungen an anderen Systemen, die an das System von Interesse angeschlossen sind, zu verursachen.

7.4.2.6

Die Änderungsverfolgung wird ordnungsgemäß aufrechterhalten, sodass die Rückverfolgbarkeit der Änderungen erreicht wird.

7.4.2.7

Die Zusammenarbeit mit der Prozesssicht zum Erreichen von Verantwortung wird aufgebaut.

7.4.2.8

Das Wissen, dass durch vergangene Erfahrung erlangt wurde, sollte effektiv genutzt werden. Die Informationen über „gelernte Lektionen“ werden erhalten und, wenn passend, aktiv auf andere Änderungen angewandt. Sie spiegeln sich in der Verbesserung des Systemlebenszyklus wieder. Das vorhandene Wissen über das System wird mit einem eigenen Managementplan ausgestattet.

7.4.2.9

Die Personen oder Einheiten, die zum Erreichen der oben angeführten Ergebnisse verantwortlich sind, werden identifiziert.

7.4.3 Implementierungsaktivitäten

<Anmerkung der Redaktion: Dieser Abschnitt ist zu erweitern, um zu erklären, wie die Ergebnisse der folgenden Aktivitäten aus 60300-1 zu erzielen sind.>

Festlegung der Einheitenanforderung

Einsatz der entworfenen Einheit

Aufrechterhaltung der Einheitenleistung durch Instandhaltung

Vorhersagen der Zuverlässigkeit

Analyse und Vorhersage der Zuverlässigkeit

Archivierung der erreichten Zuverlässigkeitsdaten für eine zukünftige Verwendung

Zuverlässigkeitswachstum durch Entwurfsänderungen und neue Softwareversionen

8 Zusicherungsmetafälle zum Erreichen von Zuverlässigkeit offener Systeme

Dieser Abschnitt fokussiert auf die Qualität der Zuverlässigkeitsnachweise von Systemlebenszyklen. Die Inhalte eines Zuverlässigkeitsnachweises beinhalten Anforderungen, Architekturentwurf und detaillierte Entwurfsspezifikationen, sowie die Ansprüche ihrer Zuverlässigkeitseigenschaften der Implementierung, Argumente für die Ansprüche, Beweise, die die Argumente unterstützen, Annahmen und Definitionen der überall dort verwendeten Begriffe und Modelle. Diese Internationale Norm erfordert die folgenden vier Arten von Metafällen zum Erreichen von Zuverlässigkeit offener Systeme.

Im Folgenden wird jeder der fünf Zusicherungsmetafälle durch die gegebenen Elemente e), f) und g) festgelegt, die in Abschnitt 6.2 angegeben sind.

8.1 Zusicherungsmetafall für Konsistenz innerhalb des Systems

Dieser Zusicherungsmetafall dient dazu, die logischen Aspekte des Zielzuverlässigkeitsnachweises zu diskutieren.

8.1.1 Zweck

Der Zweck des Zusicherungsmetafall für Konsistenz innerhalb des Systems ist es, die Konsistenz des Zielzuverlässigkeitsnachweises aufzubauen.

8.1.2 Festzusetzende Eigenschaften

8.1.2.1

Die Begriffe und Annahmen des Zielzuverlässigkeitsnachweises sollten klar festgelegt werden, um eine Grundlage für logische Schlussfolgerungen zu geben.

8.1.2.2

Ansprüche sollten unter Verwendung der festgelegten Begriffe in konsistenter Weise formuliert werden. Das durchzuführende Verifikationsverfahren sollte für jeden Anspruch festgelegt werden.

8.1.2.3

Das Argument des Zielzuverlässigkeitsnachweises sollte logisch konsistent sein.

ANMERKUNG Logische Konsistenz bedeutet hier, dass die Beschreibung des Arguments des Zusicherungsfalles in Bezug auf das Konsistenzkriterium explizit im Zusicherungsmetafall angegeben ist.

8.1.2.4

Der Interessenvertreter, der die Kontrollen und das Timing für diese Kontrollen durchführt, sollte festgelegt werden.

8.2 Zusicherungsmetafall für Konsistenz zwischen Systemen

Systeme sind üblicherweise mit anderen Systemen verbunden und solche Verbindungen erhöhen den Bedarf an zusätzlichen Anforderungen.

Der Zielzuverlässigkeitsnachweis des Lebenszyklus eines Systems ist durch den Zusicherungsmetafall in Relation zu den Zuverlässigkeitsnachweisen der anderen miteinander verbundenen Systeme auszuwerten. Da sich die Menge der miteinander verbundenen Systeme mit der Zeit verändert, ist die Liste der identifizierten Systeme in dieser Menge ein Teil der Vereinbarung der Interessenvertreter.

8.2.1 Zweck

Der Zweck des Zusicherungsmetafalles für Konsistenz zwischen Systemen ist es, das Abhängigkeitsverhältnis zwischen den Zuverlässigkeitsnachweisen miteinander verbundener Systeme aufzubauen.

8.2.2 Festzusetzende Eigenschaften

8.2.2.1

Die Menge der relevanten miteinander verbundenen Systeme und ihre Zuverlässigkeitsnachweise sollten identifiziert werden.

8.2.2.2

Die Begriffe, die in den identifizierten, relevanten Zuverlässigkeitsnachweisen festgelegt wurden, sollten auf die im Zielzuverlässigkeitsfall festgelegten Begriffe abgebildet werden. Im Gegenzug sollten die Begriffe, die im Zielzuverlässigkeitsnachweis festgelegt wurden, konsistent auf die Begriffe abgebildet werden, die in den identifizierten, relevanten Zuverlässigkeitsnachweisen festgelegt wurden. Diese Abbildungen sollten die Annahmen der Zuverlässigkeitsnachweise bewahren.

8.2.2.3

Die Änderung dieser externen Systeme sollte im Zielzuverlässigkeitsnachweis berücksichtigt werden.

8.3 Gültigkeitszusicherungsmetafall

Zusätzlich zur Konsistenz ist die Gültigkeit von Zuverlässigkeitsnachweisen in Bezug auf die reale Welt gefordert.

8.3.1 Zweck

Der Zweck des Gültigkeitszusicherungsmetafalles ist es, die Gültigkeit des Zielzuverlässigkeitsnachweises in Bezug auf die Realität, die sich die ganze Zeit über verändert, zu gewährleisten.

8.3.2 Festzusetzende Eigenschaften

8.3.2.1

Die Definition der Begriffe sollte dem Verständnis der Interessenvertreter angemessen entsprechen.

8.3.2.2

Die Wahl der Begriffe und Annahmen im Zielzuverlässigkeitsnachweis sollte gerechtfertigt werden. Die Kriterien für die Rechtfertigung sollten klargestellt werden.

8.3.2.3

Der Kontext sollte die tatsächliche Situation beschreiben, in der der Zielzuverlässigkeitsnachweis anzuwenden ist. Die Beschreibung des Systems und seiner Umgebung im Zielzusicherungsfall sollte die Realität wie vorgesehen darstellen.

8.3.2.4

Missbrauch der Begriffe und Annahmen, der über die vorgesehene Verwendung hinausgeht, sollte verhindert werden.

8.3.2.5

Die Beweismittel, auf die im Zielzuverlässigkeitsnachweis verwiesen wird, sollten existieren und sollten hinreichend starke Unterstützung für die Ansprüche bieten, die sie unterstützen sollen.

8.3.2.6

Jeder Schritt der Schlussfolgerung im Argument des Zielzuverlässigkeitsnachweises sollte garantiert werden und diese Garantie sollte durch entsprechende Daten oder Fakten unterstützt werden.

8.3.2.7

Wo immer ein Anspruch in Unteransprüche geteilt wird, sollte die Wahl der Teilung gerechtfertigt werden.

ANMERKUNG Im Allgemeinen kann ein Anspruch auf viele Arten in Unteransprüche geteilt werden. Die Rechtfertigung für die Wahl der spezifischen Art der im Zielzuverlässigkeitsnachweis durchgeführten Teilung muss gegeben sein. Betrachtete Alternativen müssen aufgezeichnet werden und der gewählte Fall muss unter ihnen bezüglich der festgelegten Kriterien gerechtfertigt werden.

8.3.2.8

Die Argumente sollten fortwährend gegen die sich verändernde Realität, einschließlich der Änderungen in den miteinander verbundenen externen Systemen, validiert werden.

ANMERKUNG Die Realität verändert sich ständig. Also sollte die Validierung nicht nur während der Systementwicklung sondern auch fortwährend während des Betriebs stattfinden. Die Gültigkeit von Ansprüchen, die durch Argumente des Zielzuverlässigkeitsnachweises unterstützt werden, können zum Beispiel durch Überwachung des Systembetriebs oder durch Bereitstellung der Standardmittel für Fehlaussagen, die durch unerwarteten Ausfall verursacht werden, gestärkt werden.

8.3.2.9

Ein Interessenvertreter/die Interessenvertreter sollte(n) bestimmt werden, diesen Prozess durchzuführen, der kontinuierlich die Zusicherungsprozesse validiert und sie mit der sich fortwährend verändernden Betriebswirklichkeit der identifizierten Interessenvertreter und der miteinander verbundenen Systeme in Verbindung bringt.

8.4 Angemessenheitszusicherungsfall

Die in 8.3 geforderte Gültigkeit ist für einen gehaltvollen Zuverlässigkeitsnachweis nicht ausreichend, da ein Zuverlässigkeitsnachweis, der nur offensichtliche Fakten beansprucht (sprich: Ansprüche, die für Experten offensichtlich sind) gültig sein kann. Etwas das nicht offensichtlich ist, muss in einem sinnvollen Zuverlässigkeitsnachweis beansprucht werden; seine Ansprüche müssen im Vergleich zur realen Welt realistisch sein.

8.4.1 Zweck

Der Zweck des Angemessenheitszusicherungsfall es ist es, zu demonstrieren, dass der Zuverlässigkeitsnachweis gehaltvoll ist.

8.4.2 Festzusetzende Eigenschaften

8.4.2.1

Die Gesetze und Regeln der Organisation, die für den Systemlebenszyklus relevant sind, sollten identifiziert werden.

8.4.2.2

Der Zuverlässigkeitsnachweis, der bereitgestellt wurde, um die Anforderung 5.1 zu erfüllen, sollte die Anforderungen der relevanten in 8.4.2.1 identifizierten Gesetze und Regeln erfüllen.

8.4.2.3

Der Zuverlässigkeitsnachweis, der bereitgestellt wurde, um die Anforderung 5.1 zu erfüllen, sollte den Anforderungen der Vereinbarung die nach 7.1 konsensschaffende Prozesssicht errichtet wurden, folgen.

8.4.2.4

Ein relevanter sozialer Konsens sollte identifiziert werden, wie die Zusicherung der Zuverlässigkeit des Systemlebenszyklus festzusetzen ist.

8.4.2.5

Der Zuverlässigkeitsnachweis, der bereitgestellt wurde, um die Anforderung 5.1 zu erfüllen, sollte die Anforderungen des in 8.4.2.4 identifizierten sozialen Konsenses folgen.

8.5 Vertrauenszusicherungsmetafall

Im einfachsten Fall wird ein Zuverlässigkeitsnachweis von seinem Autor dazu verwendet, um die Leser von der Vertrauenswürdigkeit seines Anspruchs zu überzeugen; in anderen Worten, um dem Leser das Vertrauen des Autors zu vermitteln. Wenn der Leser so sicher ist wie der Autor, dann ist der Zuverlässigkeitsnachweis in dieser Hinsicht erfolgreich. Der Autor ist dazu verpflichtet, dies zu verwirklichen. Wer garantiert jedoch eine erfolgreiche Kommunikation, was insofern ein subtiles Problem werden kann, wenn ein Zuverlässigkeitsnachweis verwendet wird, um einen Konsens zwischen verschiedenen Interessenvertretern zu schaffen, die gleichzeitig Autoren und Leser seiner verschiedenen Teile sein dürfen. Zum Beispiel kann ein Interessenvertreter mit geringer Verpflichtung möglicherweise eine Vereinbarung absegnen, obwohl sein Verständnis und Vertrauen in den Zuverlässigkeitsnachweis gering ist. Nachteilige Auswirkungen müssen nicht auf den einen mit geringem Vertrauen begrenzt sein; offene Aspekte des Systems können die Lage verschlimmern.

Für einen Interessenvertreter ist es ein Teil der Demonstration seiner Verpflichtung gegenüber dem System, ein vertretbares hohes Maß an Vertrauen in einen Zuverlässigkeitsnachweis zu erlangen. Das Erreichen von Zuverlässigkeit offener Systeme erfordert zumindest in bestimmten Schlüsselrollen solche verpflichteten Interessenvertreter miteinander verbundener Systeme, um die „geteilte Verantwortung“ im Angesicht unerwarteter Ausfälle und Änderungen zu ergreifen.

Somit sollte ein Zuverlässigkeitsnachweis durch Mechanismen unterstützt werden, um das Maß an Vertrauen, das jeder Interessenvertreter in den Fall hat, zu verwalten und sollte über die dazugehörigen Daten verfügen, die demonstrieren, dass jeder das für seine Rolle angemessene Maß an Vertrauen erreicht hat.

8.5.1 Zweck

Der Zweck des Vertrauenszusicherungsmetafalles ist es, den Grad des Vertrauens, den jeder Interessenvertreter in das System und seinen Zuverlässigkeitsnachweis hat, explizit darzulegen.

ANMERKUNG Ein Interessenvertreter mit großer Verpflichtung gegenüber dem System würde ein höheres Vertrauen in den Zielzuverlässigkeitsnachweis haben. Interessenvertreter mit geringem Vertrauen und schwacher Verpflichtung können die Zuverlässigkeit des Systems untergraben. Ein Argument, dass jeder Interessenvertreter ausreichend starkes Vertrauen hat, zeigt an, dass es keine solchen Interessenvertreter gibt.

8.5.2 Festzusetzende Eigenschaften

8.5.2.1

Die Kriterien für das Maß an vertretbarem Vertrauen in den Zielzuverlässigkeitsnachweis sollten festgesetzt werden.

8.5.2.2

Es sollten entscheidende Interessenvertreter identifiziert werden, deren Vertrauen in den Zielzuverlässigkeitsnachweis einen starken Einfluss auf die Zuverlässigkeit des Systems hat.

8.5.2.3

Die Kriterien für die Maße vertretbaren Vertrauens sollten bestimmt werden.

8.5.2.4

Die Managementmechanismen für die Vertrauensmaße der Interessenvertreter sollten existieren und sollten garantieren, dass entscheidende Interessenvertreter ein angemessen hohes Maß an Vertrauen in den Zielzuverlässigkeitsnachweis haben.

Anhang A (informativ)

Beziehung zu anderen Zuverlässigkeitsnormen

A.1 IEC 60050-192 Internationales Elektrotechnisches Wörterbuch – Teil 192 – Zuverlässigkeit

Es gilt die Definition der Begriffe aus IEC 60050-192, vorausgesetzt, dass deren Definitionen in Abschnitt 3 dieser Internationalen Norm gegeben sind.

A.2 Beziehung zu IEC 60300-1 Zuverlässigkeitsmanagement

Die Anforderungen, die in dieser Internationalen Norm festgelegt sind, beruhen auf den in IEC 60300-1 gegebenen Prozessen, wo die Prozesse beschrieben sind, die am Management der Zuverlässigkeit innerhalb einer Organisation beteiligt sind und wo ein Framework zum Management von Zuverlässigkeitsaktivitäten zum Erreichen von Zuverlässigkeitsleistung aufgebaut wird.

A.3 Beziehung zu IEC 62741 Darlegung von Zuverlässigkeitsanforderungen. Der Zuverlässigkeitsnachweis und ISO/IEC 15026-2 Zusicherungsfall

Diese Internationale Norm erfordert einen wie in IEC 62741 beschriebenen Zuverlässigkeitsnachweis. Der Zuverlässigkeitsnachweis ist eine Instanz des Zusicherungsfalles, der in ISO/IEC 15026-2 festgelegt ist.

A.4 Beziehung zu ISO/IEC 15288 System-Lebenszyklus-Prozesse und ISO/IEC 42010 System- und Software-Engineering – Architekturbeschreibung

Diese Internationale Norm legt vier Prozesssichten fest. Der Begriff der Prozesssicht ist in ISO/IEC 15288 festgelegt, wo wiederum der Begriff Sicht verwendet wird, der in ISO/IEC 42010 festgelegt ist.