

DIN EN 62741

ICS 29.020; 31.020; 33.020; 35.020

**Leitfaden zur Darlegung von Zuverlässigkeitsanforderungen –
Der Zuverlässigkeitsnachweis
(IEC 62741:2015);
Deutsche Fassung EN 62741:2015**

Demonstration of dependability requirements –
The dependability case
(IEC 62741:2015);
German version EN 62741:2015

Démonstration des exigences de sûreté de fonctionnement –
Argumentaire dans le cadre de la sûreté de fonctionnement
(IEC 62741:2015);
Version allemande EN 62741:2015

Gesamtumfang 47 Seiten

DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE

Anwendungsbeginn

Anwendungsbeginn für die von CENELEC am 2015-03-24 angenommene Europäische Norm als DIN-Norm ist 2015-10-01.

Nationales Vorwort

Vorausgegangener Norm-Entwurf: E DIN EN 62741:2013-07.

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

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

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

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

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

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

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

Leitfaden zur Darlegung von Zuverlässigkeitsanforderungen –
Der Zuverlässigkeitsnachweis
(IEC 62741:2015)

Demonstration of dependability requirements –
The dependability case
(IEC 62741:2015)

Démonstration des exigences de sûreté de
fonctionnement –
Argumentaire dans le cadre de la sûreté de
fonctionnement
(IEC 62741:2015)

Diese Europäische Norm wurde von CENELEC am 2015-03-24 angenommen. CENELEC-Mitglieder sind gehalten, die CEN/CENELEC-Geschäftsordnung zu erfüllen, in der die Bedingungen festgelegt sind, unter denen dieser Europäischen Norm ohne jede Änderung der Status einer nationalen Norm zu geben ist.

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

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

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

CENELEC

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

CEN-CENELEC Management Centre: Avenue Marnix 17, B-1000 Brüssel

© 2015 CENELEC – Alle Rechte der Verwertung, gleich in welcher Form und in welchem Verfahren, sind weltweit den Mitgliedern von CENELEC vorbehalten.

Ref. Nr. EN 62741:2015 D

Vorwort

Der Text des Dokuments 56/1591/FDIS, zukünftige 1. Ausgabe der IEC 62741, erarbeitet vom IEC/TC 56 „Dependability“, wurde zur parallelen IEC-CENELEC-Abstimmung vorgelegt und von CENELEC als EN 62741:2015 angenommen.

Nachstehende Daten wurden festgelegt:

- spätestes Datum, zu dem dieses Dokument auf nationaler Ebene durch Veröffentlichung einer identischen nationalen Norm oder durch Anerkennung übernommen werden muss (dop): 2015-12-24
- spätestes Datum, zu dem nationale Normen, die diesem Dokument entgegenstehen, zurückgezogen werden müssen (dow): 2018-03-24

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

Anerkennungsnotiz

Der Text der Internationalen Norm IEC 62741:2015 wurde von CENELEC ohne irgendeine Abänderung als Europäische Norm angenommen.

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

IEC 60300-3-1	ANMERKUNG	Harmonisiert als EN 60300-3-1.
IEC 60300-3-4	ANMERKUNG	Harmonisiert als EN 60300-3-4.
IEC 61078	ANMERKUNG	Harmonisiert als EN 61078.
IEC 62347	ANMERKUNG	Harmonisiert als EN 62347.
IEC/ISO 31010	ANMERKUNG	Harmonisiert als EN 31010.
IEC 62198	ANMERKUNG	Harmonisiert als EN 62198.

Inhalt

	Seite
Vorwort	2
Einleitung	5
1 Anwendungsbereich	6
2 Normative Verweisungen	6
3 Begriffe und Abkürzungen	6
3.1 Begriffe	6
3.2 Abkürzungen	7
4 Grundlagen des Zuverlässigkeitsnachweises	8
4.1 Grundsätze und Zweck	8
4.2 Beziehung zwischen dem Zuverlässigkeitsnachweis und Zuverlässigkeitsplänen	8
4.3 Fortlaufende Zusicherung der Zuverlässigkeit	9
5 Grundsätze des Zuverlässigkeitsnachweises	10
5.1 Beschreibung des Zuverlässigkeitsnachweises	10
5.2 Ansprüche im Zuverlässigkeitsnachweis aufstellen und darlegen	11
5.3 Verwendung von Indizien im Zuverlässigkeitsnachweis	12
5.4 Nachweisrahmen	13
5.5 Zuverlässigkeitsnachweisbericht	15
6 Erarbeitung des Zuverlässigkeitsnachweises	15
6.1 Allgemeines	15
6.2 Vorbereitung des Zuverlässigkeitsnachweises	16
6.3 Konzeptionsstufe	17
6.4 Entwicklungsstufe	18
6.5 Realisierungsstufe	18
6.6 Nutzungsstufe	19
6.7 Erweiterungsstufe	19
6.8 Stilllegungsstufe	20
7 Angemessenheit eines Nachweises begutachten	20
Anhang A (informativ) Nachweisrahmen	21
A.1 Allgemeines	21
A.2 Nur in diesem Anhang verwendete Abkürzungen	22
Anhang B (informativ) Allgemeine Anforderungen an den Zuverlässigkeitsnachweisbericht	39
B.1 Allgemeines	39
B.2 Für den Zuverlässigkeitsnachweisbericht benötigte Elemente	39
B.3 Kontext und Annahmen	39
B.3.1 Interessenträger	39
B.3.2 Systembeschreibung	40
B.3.3 Zuverlässigkeitsanforderungen	40

	Seite
B.3.4 Verwendungseinschränkungen	40
B.3.5 Annahmen	40
B.4 Risiken	40
B.5 Zuverlässigkeitsplan	41
B.6 Nachweisrahmen	41
B.7 Nachweisfundus	41
B.8 Überprüfung der bisherigen Nachweise	41
B.9 Ansprüche und Argumente	41
B.10 Schlussfolgerungen und Empfehlungen	41
Anhang C (informativ) Checkliste zur Begutachtung der Angemessenheit von Indizien	43
Literaturhinweise	44
Anhang ZA (normativ) Normative Verweisungen auf internationale Publikationen mit ihren entsprechenden europäischen Publikationen	45
Bilder	
Bild 1 – Veranschaulichung des fortlaufenden Zusicherungs-Prozesses	10
Bild 2 – Ansprüche aufstellen	11
Bild 3 – Festlegung und Entwicklung des Nachweisrahmens	14
Tabellen	
Tabelle A.1 – Nachweisrahmen für System „X“	23
Tabelle A.2 – Nachweisrahmen für System „Y“	27

Einleitung

Zuverlässigkeit ist die Fähigkeit zu funktionieren, wie und wann gefordert. Akzeptable Zuverlässigkeitsniveaus sind daher für eine nachhaltige Leistung und für optimierte Lebenszykluskosten wesentliche Eigenschaften.

Um ein zuverlässiges System zu erhalten, sollten Zuverlässigkeitsanforderungen aufgestellt, die Risiken für deren Nichterreichen ermittelt und ein geeigneter Tätigkeitssatz entwickelt werden, wie diese Anforderungen erreicht und nachgewiesen und die damit verbundenen Risiken beherrscht werden können. Ein Zuverlässigkeitsnachweis (en: dependability case) stellt einen geeigneten und überzeugenden Weg dar, das Ergebnis dieser Tätigkeiten an einem einzigen Ort zusammengefasst aufzuzeichnen und eine begründete Argumentation dafür zu liefern, dass die möglichen Risiken beurteilt und behandelt wurden und die nötige Zuverlässigkeit erreicht wurde oder diese in Zukunft nachhaltig erreicht werden wird. Der Zuverlässigkeitsnachweis ist das wichtigste Kommunikationsmittel zu Zuverlässigkeitsangelegenheiten zwischen Kunden, Lieferanten und anderen Interessenträgern und begünstigt deren gegenseitige Zusammenarbeit. Dies ist eine wesentliche Voraussetzung für das Erreichen der geforderten Zuverlässigkeit und führt zu einer vertrauensvollen Kunden/Lieferantenbeziehung.

Die Ausarbeitung eines Zuverlässigkeitsnachweises kann auch durch die durchgeführten Aktionen zur Vorbereitung und Entwicklung der Argumentation innerhalb des Zuverlässigkeitsnachweises zu einer verbesserten Zuverlässigkeit führen. Die Ausarbeitung kann die Wirtschaftlichkeit eines Zuverlässigkeitsprogramms erhöhen, da eine Tätigkeit, die keinen Nachweis liefert, möglicherweise unnötig sein kann.

Die für das Erreichen der Zuverlässigkeit erforderlichen Tätigkeiten hängen von der Art und dem Entwicklungsstand des Systems ab und variieren wahrscheinlich erheblich von einem Projekt zu einem anderen.

In dieser Internationalen Norm umfasst die Benennung „Zuverlässigkeit“ durchgehend alle Aspekte der Funktionsfähigkeit (en: reliability), Verfügbarkeit, Instandhaltbarkeit und Unterstützbarkeit sowie weitere Merkmale wie beispielsweise Gebrauchstauglichkeit, Prüfbarkeit und Lebensdauer. Zusätzlich gehören zur Zuverlässigkeit eines Systems alle Aspekte dieses Systems einschließlich Bauelemente, Prozesse, Hardware, Software und die dazwischen liegenden Schnittstellen.

Diese Norm dient der Anleitung: Die Leitlinien sind keine Vorschriften, sie sind generischer Art, sie sollten auf die jeweiligen Zielsetzungen zugeschnitten werden und sind auch nicht erschöpfend.

Diese Norm behandelt weder Sicherheit noch Umwelt.

1 Anwendungsbereich

Diese Internationale Norm gibt Leitlinien für den Inhalt und die Verwendung eines Zuverlässigkeitsnachweises und stellt allgemeine Grundsätze für die Ausarbeitung eines Zuverlässigkeitsnachweises auf.

Diese Norm ist im Zusammenhang mit einem allgemeinen Projekt zu sehen, bei dem ein „Kunde“ bei einem „Lieferanten“ ein System bestellt, das bestimmte Zuverlässigkeitsanforderungen erfüllt, und der Kunde dann das System bis zu dessen Stilllegung beziehungsweise Außerbetriebnahme betreibt. Die in dieser Norm beschriebenen Verfahren können je nach Bedarf für andere Situationen modifiziert und darauf angepasst werden.

Der Zuverlässigkeitsnachweis wird üblicherweise vom Kunden und Lieferanten ausgearbeitet, er kann jedoch auch von anderen Organisationen eingesetzt und angepasst werden. Beispielsweise können Zertifizierungsstellen und Regulierer den eingereichten Zuverlässigkeitsnachweis daraufhin untersuchen, inwieweit dieser ihre eigenen Entscheidungen unterstützt; Anwender des Systems können den Zuverlässigkeitsnachweis aktualisieren oder erweitern, insbesondere dann, wenn sie das System für andere Zwecke anwenden.

2 Normative Verweisungen

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

IEC 60050-192, *International Electrotechnical Vocabulary – Part 192: Dependability*¹⁾

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

ISO 31000, *Risk management – Principles and guidelines on implementation*

3 Begriffe und Abkürzungen

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

3.1 Begriffe

3.1.1

Zuverlässigkeitsnachweis

(en: **dependability case**)

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

3.1.2

Nachweisrahmen

(en: **evidence framework**)

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

3.1.3

handelsüblich

OTS

(en: **off-the-shelf; OTS**)

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

¹⁾ Zu veröffentlichen.

Anmerkung 1 zum Begriff: Wird manchmal auch als COTS (en: commercial off-the-shelf) oder MOTS (en: modified off-the-shelf) bezeichnet.

3.1.4

Kunde

(en: customer)

Beteiligter, der die Einheit bestellt oder diese spezifiziert, samt Zuverlässigkeitsanforderungen

Anmerkung 1 zum Begriff: Dies kann eine Organisation sein, ein Geldgeber, eine Abteilung, eine Gesellschaft oder ein Individuum und kann sich während des Lebenszyklus ändern.

3.1.5

Subsystem

(en: subsystem)

Teil eines Systems, das selbst ein System ist

3.1.6

Lieferant

(en: supplier)

Beteiligter, der die Einheit liefert, die die Zuverlässigkeitsanforderung erfüllt

Anmerkung 1 zum Begriff: Dies kann eine Organisation sein, eine Abteilung, eine Gesellschaft oder ein Individuum und kann sich während des Lebenszyklus ändern.

3.1.7

System (<im Sinne der Zuverlässigkeit>)

(en: system (<in dependability>))

definierte Menge von in Wechselbeziehung stehenden Einheiten, die zusammen eine Anforderung erfüllen

Anmerkung 1 zum Begriff: Von einem System wird angenommen, dass es eine definierte reale oder abstrakte Grenze hat.

Anmerkung 2 zum Begriff: Für den Betrieb des Systems können externe Ressourcen (von außerhalb der Systemgrenze) erforderlich sein.

Anmerkung 3 zum Begriff: Eine Systemstruktur kann hierarchischer Art sein, beispielsweise System, Subsystem, Bauelement, usw.

Anmerkung 4 zum Begriff: Anwendungs- und Instandhaltungsbedingungen sollten im Rahmen der Anforderung beschrieben oder impliziert sein.

3.2 Abkürzungen

COTS handelsüblich (en: commercial-off-the-shelf)

FEM Modellierung finiter Elemente (en: finite element modelling)

FMECA Ausfalleffekt- und Kritizitätsanalyse (en: failure mode, effects and criticality analysis)

FTA Fehlzustandsbaumanalyse, Störungsbaumanalyse (en: fault tree analysis)

MOTS modifiziert handelsüblich (en: modified off-the-shelf)

OTS handelsüblich (en: off-the-shelf)

4 Grundlagen des Zuverlässigkeitsnachweises

4.1 Grundsätze und Zweck

Ein Zuverlässigkeitsnachweis stellt eine logisch aufgebaute und nachvollziehbare, nachweisbasierte Argumentation bereit, dass ein System die Anforderungen erfüllt und diese auch in Zukunft erfüllen wird. Der Zuverlässigkeitsnachweis legt dar, warum bestimmte Tätigkeiten durchgeführt worden sind und inwiefern diese als erfolgreich angesehen werden können. Für eine maximale Wirksamkeit sollte der Nachweis bereits in der Konzeptionsstufe begonnen und in der Folge fortschreitend mit dem Systemlebenszyklus aktualisiert werden; er wird üblicherweise in Zuverlässigkeitsnachweisberichten zu vorher festgelegten Meilensteinen zusammengefasst. Er erfasst den Fortschritt, inwieweit Zuverlässigkeitsanforderungen bereits erreicht wurden, und begleitet das System den gesamten Lebenszyklus über bis zu dessen Stilllegung.

Der Zuverlässigkeitsnachweis ist besonders bei hochwertigen, in geringer Anzahl eingesetzten Systemen von größtem Vorteil, bei denen ein direkter Nachweis der Zuverlässigkeit möglicherweise schwierig oder nur zu hohen Kosten erhältlich sein könnte. Da solche Systeme häufig sehr komplex sind, neuartige Technologien verwenden und in weitreichender Weise verschiedenartige Interessenträger betreffen, wird ein explizites Argument zur beweiskräftigen Darlegung ihrer detaillierten Zuverlässigkeitsansprüche (en: dependability claim) benötigt.

4.2 Beziehung zwischen dem Zuverlässigkeitsnachweis und Zuverlässigkeitsplänen

Ein wirkungsvolles Management der Zuverlässigkeit erfordert organisatorische Vorkehrungen, damit die Grundsätze, die in Zuverlässigkeitsprogrammen und Plänen benannten Tätigkeiten und die Prozesse zur Leistungsbeurteilung und Überprüfung richtig umgesetzt werden können.

Ein Zuverlässigkeitsprogramm umfasst:

- a) Zuverlässigkeitspläne, in denen die für das Erreichen der Zuverlässigkeit benötigten Tätigkeiten, Techniken und Ressourcen definiert und festgelegt werden;
- b) Messmethoden und Beurteilungskriterien;
- c) Zusicherung und Überprüfung bzw. Bewertung.

Zu den Zielsetzungen eines Zuverlässigkeitsplanes gehören neben anderen Aufgaben die Sicherstellung, dass:

- 1) die Zuverlässigkeitsanforderungen des Kunden bestimmt und benannt wurden und dargelegt wurde, dass diese Anforderungen sowohl vom Kunden als auch vom Lieferanten verstanden wurden;
- 2) Tätigkeiten geplant, vereinbart und durchgeführt wurden, dergestalt, dass den Anforderungen genügt wird und dass deren Erfüllung nachgewiesen wird und die Risiken einer Nichterfüllung behandelt wurden;
- 3) dem Kunden glaubhaft zugesichert wird, dass die Zuverlässigkeitsanforderungen bereits erfüllt wurden oder diese in Zukunft erfüllt werden und dass Ungewissheiten im Zusammenhang mit der Zuverlässigkeit im Verlauf des Planes abnehmen werden.

Der Zuverlässigkeitsnachweis liefert die fortlaufende Zusicherung, dass die Zuverlässigkeitsanforderungen bereits erfüllt wurden oder diese in Zukunft erfüllt werden und dass Ungewissheiten im Zusammenhang mit der Zuverlässigkeit abnehmen. Zusätzlich wird durch den Nachweis dargelegt, dass durch die im Plan genannten Maßnahmen die Anforderungen erreicht und die Risiken behandelt werden. Dies ist Teil des Arguments und ein Indiz dafür, dass das System zuverlässig ist oder dies sein wird. Der Plan beruht üblicherweise auf Normen und auf der Erfahrung der Organisation in der Lenkung der Zuverlässigkeit. Er ist auf die jeweils zu beachtenden Faktoren zugeschnitten, wie beispielsweise relevante Lebenszyklusstufen, die besonderen Gegebenheiten der Organisation, verfügbare Ressourcen und die zu beherrschenden Risiken.

Der Zuverlässigkeitsplan und der Zuverlässigkeitsnachweis werden meist parallel zueinander aufgestellt, da in beiden die Risiken des Nichterfüllens der Anforderungen behandelt werden. Es kann jedoch sein, dass das System zwar tatsächlich die Zuverlässigkeitsanforderungen erfüllt, aber möglicherweise die Erfüllung dieser Anforderungen nicht nachgewiesen werden könnte. Dies könnte einerseits daran liegen, dass es keine

geeignete Tätigkeit gibt, mit der man die Erfüllung der Anforderungen nachweisen kann, oder die Kosten oder der Zeitaufwand hierfür viel zu hoch sein könnten. Daher kann der Zuverlässigkeitsplan auch solche Tätigkeiten benennen, die speziell darauf ausgelegt sind, die Risiken einer Nichtnachweisbarkeit zu behandeln; auch diese Tätigkeiten liefern ein Indiz im Zuverlässigkeitsnachweis.

Ein Risikoregister sollte als Teil des Zuverlässigkeitsnachweises aufgestellt und mit den anderen Risiken, die im Rahmen der Planung des Zuverlässigkeitsprogrammes ermittelt wurden, koordiniert werden; beide sollten mit dem allgemeinen Projektrisikoregister abgestimmt werden. Tätigkeiten, die zur Behandlung der Risiken vorgeschlagen wurden, werden in den Zuverlässigkeitsplan mit aufgenommen und daraufhin untersucht, ob sie als Indiz für eine erfolgreiche Risikobehandlung gewertet werden können. Im Verlauf der Umsetzung des Zuverlässigkeitsplans wird der Zuverlässigkeitsnachweis mit weiteren Indizien für eine erfolgreiche Umsetzung des Planes versehen. Dadurch erhält man eine fortlaufende Zusicherung, dass die Anforderungen erfüllt werden. Können ausreichende Belege oder Nachweise nicht beigebracht werden, dann sollte der Zuverlässigkeitsplan entsprechend geändert werden.

In einem gut geführten Projekt sind der Zuverlässigkeitsplan und der Zuverlässigkeitsnachweis vollständig in das allgemeine Projektmanagement integriert. In solch einem Projekt führt die Durchführung eines Zuverlässigkeitsnachweises zu keiner Zunahme der insgesamten Arbeitsbelastung, da die Kosten für das Aufstellen des Nachweises durch die Einsparungen ausgeglichen werden, die sich durch vermiedene Missverständnisse, vermiedene Nacharbeiten aufgrund spät erkannter Fehlzustände, vermiedene Tätigkeiten ohne erkennbaren Nutzen und so weiter ergeben.

Des Weiteren unterstützt die Ausarbeitung eines Zuverlässigkeitsnachweises die Entwicklung eines kostengünstigen Zuverlässigkeitsplanes, da bei der Suche nach Indizien zur Unterstützung des Arguments im Zuverlässigkeitsnachweis solche Tätigkeiten gefunden werden könnten, die den Zuverlässigkeitsplan verbessern können. Sofern eine im Plan benannte Tätigkeit nicht Teil des Arguments im Zuverlässigkeitsnachweis ist, sollte überprüft werden, ob dieser Tätigkeit eine andere nützliche Funktion im Plan zukommt. (Es wird darauf hingewiesen, dass einige im Zuverlässigkeitsplan benannte Tätigkeiten auch deswegen aufgenommen wurden, weil sie andere Disziplinen wie beispielsweise die Sicherheit unterstützen, die normalerweise nicht Bestandteil des Zuverlässigkeitsnachweises sind.)

Falls sich bei den folgenden Punkten wesentliche Änderungen ergeben, sollten der Zuverlässigkeitsplan und der Zuverlässigkeitsnachweis überprüft und aktualisiert werden:

- Kundenanforderungen oder Erwartungen;
- Umwelt oder Schnittstellensysteme;
- Einsatzbedingungen oder beabsichtigte Verwendung;
- Entwurf beziehungsweise Konstruktion;
- tatsächliche Leistung.

4.3 Fortlaufende Zusicherung der Zuverlässigkeit

Der Zuverlässigkeitsnachweis liefert eine wachsende Sammlung von Indizien dafür, dass die Ungewissheit über das Erreichen der Zuverlässigkeitsanforderungen fortlaufend abnimmt. Jedoch ist es eher der Normalfall als die Ausnahme, dass sich Anforderungen, Umfeld etc. im Systemlebenszyklus ändern können. Daher braucht die Ungewissheit nicht zwangsweise immer abzunehmen. Es könnten sich Umstände ergeben, falls beispielsweise durch eine andersartige Entwurfsoption ein Teil der Indizien obsolet wird, durch die es zu einer Zunahme der Ungewissheit kommen kann. Es könnte auch Zeitabschnitte geben, in denen keine Indizien beigebracht werden, beispielsweise während der Prüfung kurz vor Herausgabe der Prüfergebnisse, wobei sich die Ungewissheit nicht ändert. Außerdem kann es sein, dass neu aufgetauchte Indizien bereits vorliegenden Indizien entgegenstehen, dadurch könnte die Ungewissheit ebenfalls zunehmen.

Bild 1 zeigt zwei Arten von Produktentwicklungen: Neu-Entwicklung und Modifizierung handelsüblicher Produkte (MOTS). Die senkrechte Achse steht für das festgestellte Niveau der Ungewissheit zu einem beliebigen Zeitpunkt des Projektes. Da der Umfang der Zuverlässigkeitsindizien zunimmt, nimmt die Ungewissheit im Allgemeinen ab, und damit ergibt sich zunehmende Gewissheit.

Die waagerechte Achse steht für die Zeit im Projektablauf: Zeiträume beginnend mit der Konzeptionsstufe „a“ über den Entwicklungsbeginn „b“ bis zum Abschluss der Realisierungsstufe, „c“, über die Aufnahme der Nutzung beziehungsweise des Betriebs zum Zeitpunkt „d“ und über mögliche Erweiterungen zum Zeitpunkt „e“, sowie die Zeit darüber hinaus.

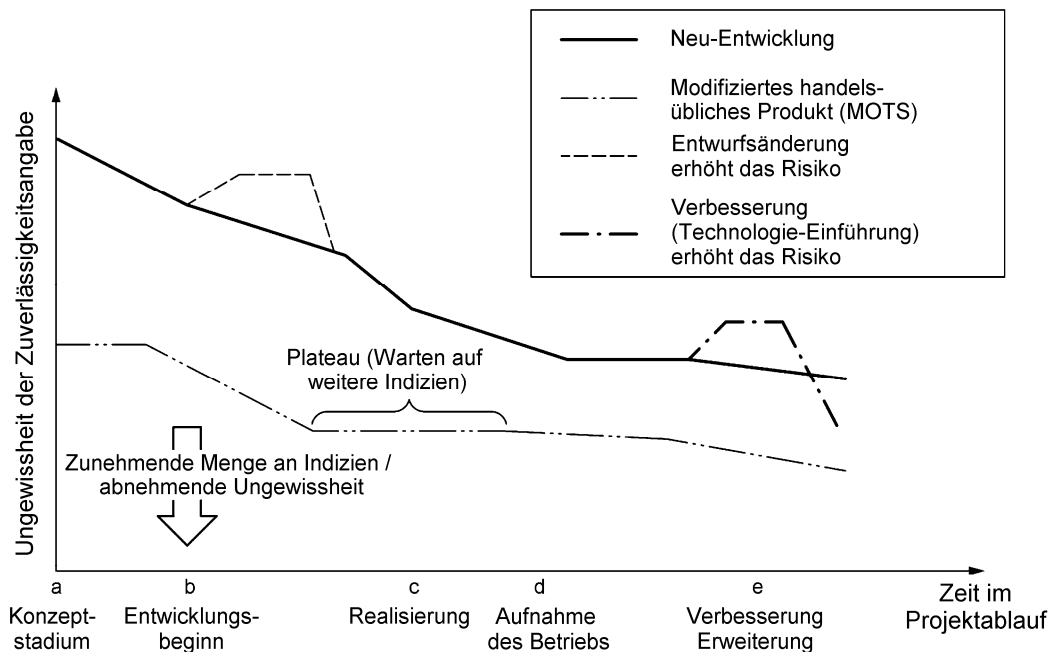


Bild 1 – Veranschaulichung des fortlaufenden Zusicherungs-Prozesses

Zur Zeit „a“ (Beginn der Konzeptionsstufe) ist das Niveau der Ungewissheit relativ hoch, aber mit fortschreitendem Projekt nimmt diese Ungewissheit ab. Zur Zeit „c“ (Realisierung), insbesondere am Übergang von der Realisierungsstufe zur Nutzungsstufe, reicht die Menge an Indizien (Belegen, Beweismittel) aus, dass die Zuverlässigkeit soweit als gesichert angesehen werden kann, dass der Übergang zur nächsten Stufe verantwortet werden kann. Die Menge an Indizien (und damit die Gewissheit) sollte auch während der Nutzung weiter zunehmen, indem Informationen aus erfolgreichen Versuchen und dem Einsatz erfasst werden und sich die verbliebenen Risiken offensichtlich weiter verringern.

Sofern eine modifizierte handelsübliche (MOTS) Lösung ihre eigene Entwicklungsperiode durchlaufen hat, wird solch eine Lösung im Vergleich zu einer kompletten Neuentwicklung (wie in Bild 1 dargestellt) häufig als weniger ungewiss angesehen, vorausgesetzt, alle anderen Dinge bleiben sonst gleich. Dies trifft bei Neuanwendungen für eine handelsübliche (OTS) Lösung oder in einer neuen Umgebung nicht zu; in solchen Fällen bedarf es einer sorgfältigen Neubeurteilung.

Abschließend muss beachtet werden, dass viele Änderungen bei der Ungewissheit schrittweise und nicht fortlaufend erfolgen.

5 Grundsätze des Zuverlässigkeitsnachweises

5.1 Beschreibung des Zuverlässigkeitsnachweises

Ein Zuverlässigkeitsnachweis beginnt zunächst mit der Angabe der Zuverlässigkeitsanforderungen. Diese Anforderungen können interne Zielvorgaben des Kunden und des Lieferanten, Marktstrategien, behördliche Vorgaben usw. enthalten, wie auch seitens des Kunden explizit genannte Anforderungen.

Der Zuverlässigkeitsnachweis stellt dann auf höchster Ebene einen Anspruch auf, in dem behauptet wird, dass das System die Anforderungen erfüllt (siehe 5.2). Der Zuverlässigkeitsnachweis liefert dann eine mehrschichtige Struktur von Behauptungen, Nebenbehauptungen und damit verbundenen Nebenargumenten, die letztendlich auf Indizien (siehe 5.3) sowie Annahmen beruhen.

Indizien werden in dem Nachweisrahmen (siehe 5.4) präsentiert und zusammengefasst; in dem im Zuverlässigkeitsnachweisbericht enthaltenen und dort vorgestellten Argument (siehe 5.5) wird auf diese Indizien verwiesen.

5.2 Ansprüche im Zuverlässigkeitsnachweis aufstellen und darlegen

Der Zuverlässigkeitsnachweis verwendet Indizien (Beweise, Hinweise oder Belege und Ähnliches), um ein Argument für den Anspruch (die Behauptung) beizubringen, dass die Zuverlässigkeitsanforderungen erfüllt wurden oder diese erfüllt werden.

Bild 2 verdeutlicht den Prozess, Ansprüche beim Zuverlässigkeitsnachweis unter Verwendung der Indizienquellen aufzustellen und diese darzulegen.

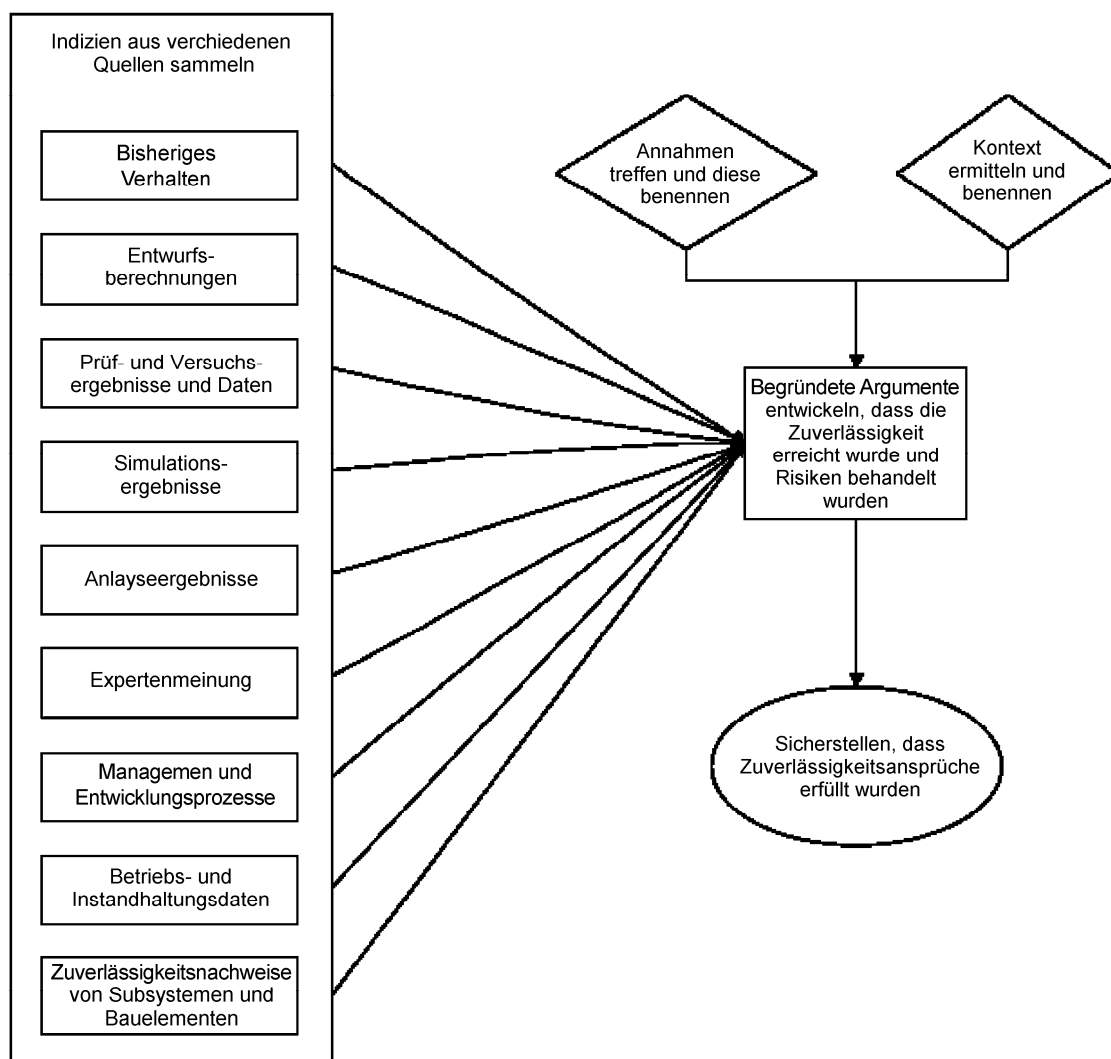


Bild 2 – Ansprüche aufstellen

Für das Aufstellen eines Argumentes erforderliche Annahmen sollten benannt und explizit dargelegt werden, zusammen mit den für deren Validierung geplanten Tätigkeiten. Dies könnten Annahmen sein hinsichtlich der Einsatz- und Anwendungsbedingungen, der Umgebung in der das System verwendet werden soll oder die Art der Instandhaltung.

Argumente können in zwei Kategorien aufgeteilt werden:

- a) Argumente dafür, dass alle den Anspruch gefährdende Risiken ermittelt und benannt und diese Risiken eliminiert oder ausreichend genug behandelt wurden, begleitet und unterstützt durch entsprechende Indizien;
- b) Argumente dafür, dass der Anspruch ausreichend begründet ist, unterstützt durch entsprechende Indizien für die Richtigkeit dieser Aussage.

Die erste Kategorie bedarf der Betrachtung aller maßgeblichen Risikoquellen, Angriffsflächen, möglichen Ereignisse (einschließlich sich ändernder Umstände) und deren Ursachen und deren potenziellen Konsequenzen. Letzteres erfordert, dass die durch die Indizien aufgebrachten Aspekte ausreichen, um den Anspruch abzusichern.

Des Weiteren müssen der Kontext und der Hintergrund ermittelt und benannt werden, für die das Argument aufgestellt wird, da sich daraus die Grenzen des Zuverlässigkeitsnachweises ergeben. Zu dem Kontext gehören die Interessenträger an dem System, die Zielsetzungen und Leistungsanforderungen, das betrachtete System und gegebenenfalls vorgeschlagenen Einschränkungen für die Verwendung des Systems.

Sollten gewisse Annahmen oder der Kontext sich ändern, dann müssen das Argument und die Ansprüche und Behauptungen im Zuverlässigkeitsnachweis neu überprüft werden.

Während der Umsetzung des Zuverlässigkeitsplanes sollten die Schlüsselannahmen validiert und, wo möglich, durch substantielle Indizien und Beweise ersetzt werden. In ähnlicher Weise sollte der Kontext, in dem das Argument aufgestellt wird, daraufhin validiert werden, ob er zu der beabsichtigten Anwendung des Systems und zu dem Zuverlässigkeitsnachweis passt.

Anhand dieser Indizienquellen und den explizit vorgestellten Annahmen legt ein begründetes Argument dar, wie die Zuverlässigkeitsansprüche substantiiert, also durch Tatsachen belegt und begründet werden können. Dokumente und Daten, die sich auf all diese Indizien und Annahmen beziehen, bilden zusammen den Zuverlässigkeitsnachweis.

5.3 Verwendung von Indizien im Zuverlässigkeitsnachweis

Es gibt zwei Arten von Indizien im Zuverlässigkeitsnachweis. Dies sind einerseits direkte Beweise oder Belege, dass die Zuverlässigkeitsanforderungen erfüllt und nachgewiesen wurden. Andererseits gibt es Indizien dafür, dass Tätigkeiten, die zur Behandlung der Risiken einer etwaigen Nichterfüllung der Zuverlässigkeitsanforderungen entworfen worden waren, auch erfolgreich ausgeführt wurden.

Ein breiter Bereich von Indizien (also Beweise, Hinweise oder Belege und Ähnliches) sollte verwendet werden. Hierzu können gehören:

- a) Leistung und Verhalten des betrachteten Systems bei früheren Einsätzen;
- b) Entwurfs- und sonstige Berechnungen;
- c) Prüfergebnisse und Versuchsdaten;
- d) Simulationsergebnisse (z. B. FEM oder Monte Carlo);
- e) Analyseergebnisse (z. B. FMECA und FTA) einschließlich Vorhersagen und Modellierung;
- f) Expertenmeinung einschließlich früher dokumentierter Erfolge des Lieferanten;
- g) Management und Entwicklungsprozesse einschließlich
 - korrekte Umsetzung bewährter Methoden,
 - Befolgung vorgegebener Managementtätigkeiten und Systemprozesse;
- h) Daten aus Betrieb und Instandhaltung;
- i) Zuverlässigkeitsnachweise über Bauelemente/Subsysteme, die von deren Lieferanten beigebracht wurden.

Es können auch Indizien aus anderen Tätigkeiten und Aufgaben berücksichtigt werden, die aus anderen Gründen als der Umsetzung des Zuverlässigkeitsplanes durchgeführt wurden, wie beispielsweise Hinweise, die aus Sicherheitsbetrachtungen oder aus Analysen der logistischen Unterstützung stammen.

Bevor man eine Zuverlässigkeitstätigkeit beginnt, sollte deren Zielsetzung zweifelsfrei verstanden worden sein; d. h. in welcher Weise hilft die beabsichtigte Tätigkeit dabei, die geforderte Zuverlässigkeit zu erreichen, wie steuert sie Indizien zum Zuverlässigkeitsnachweis bei und welche Kriterien gibt es für die Beurteilung einer erfolgreich durchgeführte Tätigkeit. Die Erfolgskriterien werden auf die Aufzeichnungen und die Ergebnisse der Tätigkeit angewendet, um zu beurteilen, ob die Zielsetzungen erreicht wurden. Indizien für eine Erfüllung der Kriterien (einschließlich Aufzeichnungen und Ergebnisse) substantiieren die Ansprüche und Behauptungen, dass die Zielsetzungen erreicht wurden. Soweit zutreffend gehört zu den Erfolgskriterien eine nachgewiesene angemessene Behandlung der Risiken.

Quantifizierte Erfolgskriterien sollten bevorzugt werden, da damit ein Erfolg einfacher bestimmt werden kann und es weniger Raum für Interpretationen gibt.

Es können jedoch nicht für alle Tätigkeiten quantifizierte Erfolgskriterien beigebracht werden. In solchen Fällen sollten qualitative Kriterien auf der Grundlage der Zielsetzungen der Tätigkeit definiert werden, diese Definitionen sollten Beweise dafür enthalten, dass die Tätigkeit selbst und auch deren Ergebnis geeignet und korrekt sind. Beispielsweise bestehen die Erfolgskriterien der Modellierung nicht einfach aus dem Nachweis, dass die Vorhersagen und die Modellierung die Erfüllung der Anforderungen darlegen, sondern darin, dass das Modell selbst eine adäquate Darstellung des Systems ist und dass alle Elemente des Systems (z. B. Software) in der Modellierung berücksichtigt wurden. Das Modell sollte auch die Robustheit des Entwurfs gegen Variationen der Nutzungsbedingungen und Fertigungsbedingungen und Fertigungstoleranzen ansprechen.

Zusicherung und Indizien ergeben sich nicht bloß aus den Ergebnissen einer Zuverlässigkeitstätigkeit, sondern auch aus dem richtigen Zeitpunkt der Durchführung der Tätigkeit und daraus etwaig folgender weiterer Aktionen. Es ist sehr wichtig, eine Tätigkeit zum richtigen Zeitpunkt durchzuführen, damit der Systementwurf noch beeinflusst werden kann; Tätigkeiten sollten daher gegebenenfalls parallel zum Entwicklungs- und Entwurfsprozess durchgeführt werden. Daher sollte zu den aus einer Analysetätigkeit stammenden Belegen auch eine Dokumentation gehören, in der aufgezeigt wird, dass die Tätigkeiten und Aktionen rechtzeitig ausgeführt wurden.

5.4 Nachweisrahmen

Der Nachweisrahmen präsentiert die Indizien, die zur Veranschaulichung der Ansprüche und Behauptungen verwendet werden, und untermauert das Argument; er wird üblicherweise in Form einer Tabelle dargestellt. Der Nachweisrahmen fasst den gegenwärtigen Satz der Übereinstimmung und der Sicherungstätigkeiten (und deren Erfolgs- oder Annahmekriterien) zusammen, mittels derer nachgewiesen werden kann, dass die Zuverlässigkeit erreicht wurde und dass Zuverlässigkeitsrisiken adäquat behandelt wurden.

Bild 3 veranschaulicht die Schritte hin zur Entwicklung des Nachweisrahmens. Jeder Zuverlässigkeitsnachweisbericht sollte seine Ansprüche und Behauptungen und Argumente auf dem neuesten Status des Nachweisrahmens aufbauen.